NPCC, Inc.

1040 Avenue of the Americas - 10th Floor
New York, New York 10018-3703

NPCC Regional Standards Committee
Preliminary Agenda--Draft
Meeting # 11-6

December 1, 2011 8:00 a.m. - 5:00 p.m.
December 2, 2011 8:00 a.m. - 3:00 p.m. (joint meeting with the CC 10:00 - noon)

Toronto Marriott Bloor Yorkville
90 Bloor Street East, Toronto, Ontario

Dress Business Casual

RSC@npcc.org

Call in 719-785-1707, Guest Code 8287#

Web Conference

Note: Glossary of Terms Used in NERC Reliability Standards dated October 26, 2011 included in the Meeting Materials.

1. **Introductions-Agenda Review-Roster**
   a. RSC membership changes.

2. **RSC October, 2011 Meeting Minute Approval and Antitrust Guidelines** (in Meeting Materials Package)
   a. Discussion of the October, 2011 RSC Meeting minutes.

3. **Action Item Assignment List and Ongoing Assignments** (in Meeting Materials Package), (Refer to Action Item Table [Item 65] at the back of Agenda)
   a. NPCC Members on NERC Drafting Teams

4. **Items Requiring RSC Approval**

5. **Executive Tracking Summary** (in Meeting Materials Package)
   a. Review entries.

6. **FERC** (in Meeting Materials Package)

   a. FERC Public Meeting--November 17, 2011.

.

NOPRs					
Item	NOPR	Docket No.	Posted	End Date	When Effective
6-1	Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards	RM11–20–000	10/26/11	12/27/11	
6-2	Transmission Planning Reliability Standards	RM11-18-000	10/26/11	12/27/11	

Letters of Approval			
Item	Docket No.	Posted	Summary
6-11	RD11-10-000		FERC approved Reliability Standard FAC-008-3 and the retirement of FAC-008-1 and FAC-009-1. Also approved the associated VRFs with one modification, and the associated VSLs. The new Reliability Standard, FAC-008-3 will be effective, and Reliability Standards FAC-008-1 and FAC-009-1 will be retired on the first day of the first calendar quarter that is twelve months after issuance of this order, as requested by NERC.
6-22	RD11-3-000	11/22/11	FERC found revised Reliability Standard FAC-013-2 (including the associated new Glossary terms and implementation plan) just, reasonable, not unduly discriminatory or preferential and in the public interest. FERC also accepted the violation risk

			factors and violation severity levels associated with the standard as proposed by NERC three exceptions. FERC denied a request by the Electric Reliability Council of Texas (ERCOT) for an exemption from Reliability Standard FAC-013-2.
6-33	RR11-5-000		NERC filed a petition requesting approval of proposed amendments to the NERC Rules of Procedure. FERC approved the proposed Amendments.

Petitions			
Item	Docket No.	Posted	Title
6-111	RR11-2-000	11/15/11	Petition for Approval of Compliance Monitoring and Enforcement Agreement Between Northeast Power Coordinating Council, Inc. and Western Electricity Coordinating Council and Related Amendments to Delegation Agreements

Motion To Defer Further Action			
Item	Docket No.	Posted	Summary

Compliance Filing			
Item	Docket No.	Posted	Summary

Final Rule			
Item	Docket No.	Posted	Summary

Other			
Item	Docket No.	Posted	Summary
6-O1	AD12-1-000 RC11-6-000 EL11-62-000	11/14/11	Request For Evidence Of Commissioner Philip D. Moeller On EPA Issues For The November 2011 Reliability
6-O2	RM11-11-000	11/21/11	Comments Of The North American Electric Reliability Corporation In Response To Notice Of Proposed Rulemaking Regarding Version 4 CIP Reliability Standards
6-O3	RM11-16-000	11/21/11	Comments Of The North American Electric Reliability Corporation In Response To Notice Of Proposed Rulemaking Regarding The Transmission Relay Loadability Standard PRC-023-2.
6-O4	AD12–5–000	11/22/11	Voltage Coordination on High Voltage Grids; Notice of Reliability Workshop Agenda. Workshop Dec. 1, 2011.
6-05	RM06-16-000	11/23/11	Third Quarter 2011 Compliance Filing Of The North American Electric Reliability Corporation In Response To Paragraph 629 Of Order No. 693
6-06	RM08-13-001	11/22/11	Motion For An Extension Of Time Of The North American Electric Reliability Corporation To Submit A Filing PRC-023-1
6-07	RM09-25-000	11/22/11	Motion For An Extension Of Time Of The North American Electric Reliability Corporation To Submit A Filing for Personnel Performance, Training, and Qualifications ("PER") Reliability Standards

7. Current and Pending Ballots:

a.	Project 2007-12 - Frequency Response	Initial Ballot and Non-Binding Poll	11/30/11	12/8/11
b.	Project 2009-01 - Disturbance and Sabotage Reporting - CIP-001 and EOP-004	Initial Ballot and Non-Binding Poll	12/2/11	12/12/11
c.	Project 2008-06 - Cyber Security - Order 706 - CIP-002 through CIP)-009 (Version 5 CIP Standards)	Initial Ballots Please Vote for each of the 10 CIP Standards Separately	12/16/11	1/6/12

8. Overlapping Postings (in Meeting Materials Package)

a.				

9. Join Ballot Pools:

a.	Project 2008-06 - Cyber Security - Order 706 - CIP-002 through CIP)-009 (Version 5 CIP Standards)	Join Ballot Pool	11/7/11	12/15/11

10. Posted for Comment: (in Meeting Materials Package)

a.	Project 2007-12 - Frequency Response BAL-003-1 - Redline to last posting Attachment A - Clean Attachment B - Clean Implementation Plan - Redline to last posting Background Document BAL-003-0.1b Mapping Document FRS Form 1 (Excel files--not in Meeting Materials Package):	Submit Comments (Word version--ctrl+click here)	10/25/11	12/8/11

	Eastern Interconnection ERCOT Quebec Interconnection Western Interconnection FRS Form 2 for Interconnection with Multiple BAs (Excel files--not in Meeting Materials Package): Two-second Sample Data Three-second Sample Data Four-second Sample Data Five-second Sample Data Six-second Sample Data FRS Form 2 for Interconnection with One BA (Excel files--not in Meeting Materials Package): Two-second Sample Data Three-second Sample Data Announcement Comments, RSAR--Mike Potishnak (in Meeting Materials)			
b.	Project 2009-01 - Disturbance and Sabotage Reporting - CIP-001 and EOP-004 EOP-004-2 - Redline to last posted Implementation Plan - Redline to Last Posted Mapping Document VRF/VSL Justification CIP-001-1 EOP-004-1 Announcement	Submit Comments (Word version--ctrl+click here)	10/28/11	12/12/11

c.	Project 2008-06 - Cyber Security - Order 706 - CIP-002 through CIP-009 (Version 5 CIP Standards) CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions Mapping Document CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period Draft Consideration of Issues and Directives Announcement CIP Standard Version 5 Webinar Slides Webinar--Dec. 13, 2011 1:00-2:00 p.m.	Submit Comments (Word version--ctrl+click here)	11/7/11	1/6/12
d.	Proposed Changes to the NERC Rules of Procedure and Associated Appendices	Comments to be Submitted Electronically to ROPcomments@nerc.net	11/7/11	12/22/11
e.	Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011	Comments to be Submitted Electronically to ROPcomments@nerc.net	11/22/11	12/22/11
f.	Regional Reliability Standard PRC-006-NPCC-1 — Automatic Underfrequency Load Shedding (NPCC Website Link)	Submit Comments (Word version--ctrl+click here)	11/22/11	12/22/11

	PRC-006-NPCC-01 Implementation Plan			
g.	Draft CAN-0027: TOP-003 R2 Coordination of Scheduled Outages	Comment Form To Be Sent To cancomments@nerc.net	11/22/11	12/14/11

a-beneath--PRC-024 variance--Hydro-Quebec.

11. Reference Documents Posted For Comment

a.				

12. Concluded Ballots (in Meeting Materials Package)

https://standards.nerc.net/Ballots.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)					Results of Ballot	RSC Recommend/Date
a.	Project 2010-11 - TPL Table 1, Footnote B	Recirculation Ballot	1/26/11	2/5/11	Quorum: 93.61% Approval: 86.54%	Yes 1/5/11
b.	Project 2007-07 - Vegetation Management - FAC-003	Successive Ballot and Non-Binding Poll	2/18/11	2/28/11	Quorum: 79.28% Approval: 79.34%	Yes 2/22/11
c.	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Initial Ballot	2/25/11	3/7/11	Quorum: 87.10% Approval: 49.54%	Yes 3/2/11
d.	Project 2007-23 - Violation Severity Levels	Non-binding Poll	2/9/11	2/18/11	Ballot Pool: 310 Opinions: 141 72% Support	Yes 10/28/10
e.	Project 2010-13 - Relay Loadability Order - PRC-023	Successive Ballot and Non-Binding Poll	1/24/11	2/13/11	Quorum: 83.95% Approval: 65.71%	Yes 2/11/11

f.	Project 2010-13 - Relay Loadability Order - PRC-023	Recirculation Ballot	2/24/11	3/6/11	Quorum: 87.35% Approval: 68.83%	Yes 2/11/11
g.	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Successive Ballot and Non-Binding Poll	4/19/11	4/28/11	Quorum: 79.66% Approval: 38.00%	No 4/19/11
h.	Project 2009-06 - Facility Ratings	Cast Ballot	4/21/11	5/2/11	Quorum: 86.01% Approval: 48.74%	Abstain 4/26/11
i.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Successive Ballot and Non-Binding Poll	5/3/11	5/12/11	Quorum: 78.33% Approval: 67.00%	No Recommendation
j.	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	Recirculation Ballot	5/12/11	5/23/11	Quorum: 91.25% Approval: 78.92%	Yes 5/12/11
k.	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Successive Ballot and Non-Binding Poll	5/18/11	5/31/11	Quorum: 92.07% Approval: 73.99	----
l.	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	Initial Ballot and Non-Binding Poll	5/31/11	6/9/11	Quorum: 88.47% Approval: 48.64%	Reject 5/31/11
m.	Project 2007-09 – Generator Verification – MOD-026-1 Ballot Results Revised because of NERC IT problem	Cast Ballot	7/22/11	8/1/11	Quorum: 90.25% Approval: 46.53%	No Consensus 7/28/11
n.	Project 2007-09 – Generator Verification – MOD-026-1	Cast Non-Binding Poll Opinion	7/22/11	8/1/11	Quorum: 88.75% Approval: 56.00%	----
o.	Project 2007-09 – Generator Verification – PRC-024-1 Ballot Results Revised because of NERC IT problem	Cast Ballot	7/22/11	8/1/11	Quorum: 90.82% Approval: 18.23%	No Consensus 7/28/11
p.	Project 2007-09 – Generator Verification – PRC-024-1	Cast Non-Binding Poll Opinion	7/22/11	8/1/11	Quorum: 88.35% Approval: 20.79%	----

q.	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Recirculation Ballot and Non-Binding Poll	6/20/11	6/30/11	Quorum: 82.97% Approval: 64.76%	Yes 6/28/11
r.	Project 2006-02 - Assess Transmission and Future Needs	Cast Ballot	7/13/11	7/22/11	Quorum: 94.33% Approval: 75.37%	----
s.	Project 2006-06 - Reliability Coordination - IRO-002-3	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 76.99%	Yes 7/22/11
t.	Project 2006-06 - Reliability Coordination - IRO-005-4	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 75.17%	Yes 7/22/11
u.	Project 2006-06 - Reliability Coordination - IRO-014-2	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 76.27%	Yes 7/22/11
v.	Project 2006-06 - Reliability Coordination - IRO-002-3	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.37% Approval: 93%	----
w.	Project 2006-06 - Reliability Coordination - IRO-005-4	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.66% Approval: 93%	----
x.	Project 2006-06 - Reliability Coordination - IRO-014-2	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.37% Approval: 89%	-----
y.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Initial Ballot	9/19/11	9/28/11 9/29/11-- Technical Difficulties	Quorum: 84.86% Approval: 61.10%	Yes 9/21/11
z.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Non-Binding Poll VRFs and VSLs	9/19/11	9/28/11 9/29/11-- Technical Difficulties	Quorum: 83.13% Approval: 68.68%	----
aa.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	Initial Ballot	9/30/11	10/10/11	Quorum: 92.97% Approval: 71.68%	No Consensus 10/3/11

bb.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Detailed Information to Support BES Exceptions Request	Initial Ballot	9/30/11	10/10/11	Quorum: 89.53% Approval: 64.03%	No Consensus 10/7/11
cc.	Project 2007-07 - Vegetation Management	Recirculation Ballot	10/4/11	10/13/11	Quorum: 87.17% Approval: 86.25%	Yes 2/22/11
dd.	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Initial Ballot	11/7/11	11/16/11	Quorum: 91.2% Approval: 95.05%	Yes 11/8/11
ee.	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Initial Ballot	11/8/11	11/18/11	Quorum: 91.2% Approval: 95.05%	Yes 11/8/11
ff.	Project 2010-07 - Generator Requirements at the Transmission Interface FAC-001-1 FAC-003-3 FAC-003-x PRC-004-2.1	Initial Ballot	11/9/11	11/18/11	Quorum: 88.22% Approval: 86.94% Quorum: 85.08% Approval: 85.71% Quorum: 84.82% Approval: 85.71% Quorum: 84.29% Approval: 96.09%	Yes 11/10/11
gg.	Project 2010-17 - Definition of Bulk Electric System and Implementation Plan	Recirculation Ballot	11/10/11	11/21/11	Quorum: 95.92% Approval: 81.32%	Yes 10/3/11
hh.	Project 2010-17 - Detailed Information to Support an Exception Request	Recirculation Ballot	11/10/11	11/21/11	Quorum: 93.02% Approval: 81.48%	

ii.	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Successive Ballot	11/11/11	11/21/11	Quorum: 83.53% Approval: 95.99%	Yes 11/14/11

13. Posted For 30-Day Pre-Ballot Review (Open Ballot Pools) Between RSC Meetings:

a.				

14. Comment Forms Submitted (in Meeting Materials Package)

a.	Standards Project Prioritization Reference Document and Tool	Comment Form	1/21/11	2/10/11
b.	Project 2007-12 - Frequency Response	Comment Form	2/4/11	3/7/11
c.	Project 2007-07 - Vegetation Management - FAC-003	Comment Form	1/27/11	2/28/11
d.	Project 2007-23 - Violation Severity Levels	Comment Form	1/20/11	2/18/11
e.	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Comment Form	1/18/11	3/7/11
f.	Regional Reliability Standards - PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding	Comment Form (no comments submitted)	1/10/11	2/24/11
g.	CAN-0015--Draft CAN-0015 Unavailability of NERC Tools	Comments	2/4/11	2/18/11
h.	CAN-0016--Draft CAN-0016 CIP-001-1 R1 - Applicability to Non-BES	Comments	2/4/11	2/18/11
i.	CAN-0017--Draft CAN-0017 CIP-007 R5 System Access and Password Controls	Comments	2/11/11	3/4/11
j.	CAN-0018--Draft CAN-0018 FAC-008 R.1.2.1 - Terminal Equipment	Comments	2/4/11	2/18/11
k.	Proposed Changes to Rules of Procedure to Add Section 1700 - Challenges to Determinations	Comments	2/14/11	3/7/11
l.	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	Comment Form	3/17/11	5/2/11
m.	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	Comment Form	3/29/11	4/28/11
n.	Project 2009-02 - Real-time Reliability Monitoring and Analysis Capabilities	Comment Form	2/16/11	4/4/11

o.	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments	Comments (No comments submitted)	3/1/11	4/15/11
p.	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Comments	3/1/11	4/15/11
q.	Project 2010-07 - Generator Requirements at the Transmission Interface	Informal Comment Period	3/4/11	4/4/11
r.	Project 2009-01 - Disturbance and Sabotage Reporting	Comment Form	3/9/11	4/8/11
s.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Comment Form	4/13/11	5/12/11
t.	Project 2010-17 - Definition of Bulk Electric System	Comment Form	4/28/11	5/27/11
u.	Project 2006-02 - Assess Transmission and Future Needs	Comment Form	4/18/11	5/31/11
v.	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	Comment Form	4/26/11	6/9/11
w.	Project 2010-17 - Definition of Bulk Electric System	Comment Form	5/11/11	6/10/11
x.	Rules of Procedure Development Team: BES Definition Exception Process	Comment Form	5/11/11	6/10/11
y.	CAN-0024--Draft CAN-0024 CIP-002 through CIP-009 Routable Protocols and Data Diodes	Comments	5/20/11	6/10/11
z.	CAN-0029--Draft CAN-0029 PRC-004-1 R1, R2 and R3 Misoperations	Comments	5/20/11	6/10/11
aa.	CAN-0030--Draft CAN-0030 Attestations	Comments	5/20/11	6/10/11
bb.	CAN-0039--Draft CAN-0039 DOE Form 407	Comments	5/20/11	6/10/11
cc.	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)	Comment Form	6/10/11	7/11/11
dd.	Project 2007-09 – Generator Verification – MOD-025-2, MOD-027-1, PRC-019-1	Comment Form	6/15/11	7/15/11
ee.	Project 2007-09 – Generator Verification – MOD-026-1 and PRC-024-1	Comment Form	6/15/11	8/1/11
ff.	Project 2010-07 – Generator Requirements at the Transmission Interface – Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards	Comment Form	6/17/11	7/17/11
gg.	Proposed Changes to NERC Rules of Procedure and associated Appendices (Appendix 4B – Sanction Guidelines; and Appendix 4C – Compliance Monitoring and Enforcement Program)	Sent Comments to ROPcomments@nerc.net	6/30/11	8/15/11

hh.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Comment Form	8/15/11	9/29/11 (Extended from 9/28/11 because of NERC network problems)
ii.	Compliance Application Notice (CAN) Process	Comment Form	8/15/11	9/6/11
jj.	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	Comment Form	8/15/11	9/6/11
kk.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	Comment Form	8/26/11	10/10/11
ll.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Detailed Information to Support BES Exception Request	Comment Form	8/26/11	10/10/11
mm.	Proposed Changes to NERC Rules of Procedure and All Appendices	Sent Comments to cancomments@nerc.net No Comments Submitted	9/2/11	10/17/11
nn.	NERC 2012-2014 Reliability Standards Development Plan	Comment Form	9/12/11	9/26/11
oo.	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004 (See note below table)	Sent Comments to cancomments@nerc.net	8/31/11	9/21/11
pp.	New CAN Template, five DRAFT CANs for Industry review, and CANs Status posted to NERC Compliance's Web site.	Sent Comments to cancomments@nerc.net	9/23/11	10/14/11
qq.	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests	Comment Form	9/13/11	10/27/11
rr.	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Comment Form	10/3/11	11/16/11
ss.	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Comment Form	10/4/11	11/17/11
tt.	Project 2010-07 - Generator Requirements at the Transmission Interface * See Item below this table	Comment Form	10/5/11	11/18/11
uu.	CAN-0020--TPL-002, TPL-003, TPL-004 and TOP-002 Equipment Maintenance Outages	Sent Comment Form to cancomments@nerc.net	10/19/11	11/9/11

vv.	CAN-0030--Attestations	No Comments	10/19/11	11/9/11
ww.	Project 2008-10 - Interpretation of CIP-006-1 R1.1 by Progress Energy	Comment Form	10/12/11	11/21/11
xx.	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
yy.	CAN-0011--PRC-005-1 R2: New Equipment	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
zz.	CAN-0012--Completion of Periodic Activity Requirements During Implementation Plan	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
aaa.	CAN-0013--PRC-023 R1 and R2 Effective Dates for Switch-on-to-Fault Schemes	No Comments	10/10/11	10/31/11
bbb.	CAN-0015--Unavailability of NERC Software Tools	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
ccc.	CAN-0022--VAR-002-1.1b R1 and R3 Generator Operation in Manual Mode	No Comments	10/10/11	10/31/11
ddd.	CAN-0024--CIP-002 R3 Routable Protocols and Data Diode Devices	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
eee.	CAN-0026--TOP-006 R3 Protection Relays	Sent Comment Form to cancomments@nerc.net	10/10/11	10/31/11
fff.	CAN-0028--TOP-006-1 R1.2 Reporting Responsibilities	No Comments	10/10/11	10/31/11
ggg.	Draft Directive Regarding Generator Transmission Leads (comments also submitted by CC)	Comments forwarded to NERC Staff: Jim Hughes, Jack Wiseman, Stacia Ann-Chambers	10/17/11	11/18/11 (originally 11/15/11)
hhh.	CAN-000040 - BAL-003 Frequency Bias Calculation	No Comments	11/2/11	11/23/11
iii.	CAN-0043 - PRC-005 Protection System Maintenance and Testing Evidence	Comment Form (submitted to cancomments@nerc.net)	11/2/11	11/23/11

* Item 14tt--FAC Alert Recommendation Webinar Participant Q&A.

15. Reference Documents Posted For Comment Between RSC Meetings

a.				

16. Drafting Team Nominations Open (Current and between RSC Meetings)

a.				

17. NERC Meetings (in Meeting Materials Package)

a. Board of Trustees, Member Representatives Committee, and Board Committees' Meetings--Nov. 2-3, 2011.
   1. Policy input.
   2. Schedule of events.
   3. Presentations.
      a. Standards Oversight and Technology Committee
      b. Compliance Committee Open Session
      c. Member Representatives Committee
      d. Board of Trustees
      e. Chairman's Notes.

b. MRC Nov. 2, 2011 Meeting notes.

c. NERC Board of Trustees Meeting Nov. 3, 2011-- NERC Board Approves Vegetation Management Standard; Focuses on Four Pillars of Success.

d. NERC--Board of Trustees Conference Call Agenda--Nov. 22, 2011.

.

18. NERC RSG (in Meeting Materials Package)

a. Whitepaper on Regional Standards and Variances.

19. NERC Standards Committee Report (in Meeting Materials Package)

a. 2012-2013 Nov. 8-18, 2011 2012-2013 election results, special election.

b. Nov. 10, 2011 teleconference--notes.

20. NERC SPCS Meeting (in Meeting Materials Package)

a.

21. NERC Compliance Application Notices (CANs), Other (refer to Meeting Materials Package--see section 13 above)

a. CO-11 NPCC Restoration Working Group letter to Michael Moon regarding CAN-0006.

b. CAN Status spreadsheet.

	CAN Final Version --Table 1	Industry Comment Analysis Spreadsheet (ctrl+click)	Comment Analysis Summary (ctrl+click)	Industry Comment Redline (ctrl+click)
1.	CAN-0006: EOP-005 R7 Verification of Restoration Procedure (Revised)	AA1	BB1	CC1
2.	CAN-0009: FAC-008 and FAC-009 Facility Rating and Design Specifications (Revised)	DD1	EE1	FF1
3.	CAN-0017: CIP-007 R5 Technical and Procedural System Access and Password Controls	GG1	HH1	II1
4.	CAN-0018: FAC-008 R1.2.1 Terminal Equipment (Revised)	JJ1	KK1	LL1
5.	CAN-0008: PRC-005 R2 Basis for First Maintenance and Testing Date (Revised)	MM1	NN1	OO1
6.	CAN-0010: Implementation of Annual in Reliability Standard Requirements (Revised)	PP1	QQ1	RR1
7.	CAN-0011: PRC-005 R2 Interval Start Date for New Equipment (Revised)	SS1	TT1	UU1
8.	CAN-0012: Completion of Periodic Activity Requirements During Implementation Plan (Revised)	VV1	WW1	XX1
9.	CAN-0013: PRC-023 R1 And R2 Effective Dates for Switch-On-To-Fault Schemes (Revised)	YY1	ZZ1	AAA1
10.	CAN-0028: TOP-006 R1.2 Reporting Responsibilities (Revised)	BBB1	CCC1	DDD1

	Draft CANs--Table 2	Industry Comment Analysis Spreadsheet (ctrl+click)	Comment Analysis Summary (ctrl+click)	Industry Comments Received (ctrl+click)
1.	DRAFT CAN-0029: PRC-004 R1, R2 and R3 Protection System Misoperations	AA2	BB2	
2.	DRAFT CAN-0039: EOP-004-1 Filing DOE Form OE-417 Event Reports	CC2	DD2	
3.	DRAFT CAN-0031: CIP-006 R1 Acceptable Opening Dimensions	EE2	FF2	
4.	DRAFT CAN-0030: Attestations	GG2	HH2	II2

22. NERC Bulk Electric System Definition (in Meeting Materials Package)

a.

23. NERC Standards Bulletin

a. Nov. 7-13, 2011 edition.
b. Nov. 14-20, 2011 edition.
c. Nov. 21-27, 2011 edition.
d. Nov. 28 - Dec. 4, 2011 edition.

24. NPCC Regional Standards, and More--Update (in Meeting Materials Package)

a. Disturbance Monitoring (PRC-002-NPCC-01)
   1. FERC approved October 20, 2011.
b. Underfrequency Load Shedding
   1. CEAP report.
   2. Approved by Member Ballot--Nov. 18, 2011. Scheduled for submission to the NPCC Board of Directors Nov. 30, 2012.
c. Regional Reserve Sharing Groups
   1. Draft RSAR developed
   2. TFCO will oversee the Drafting Team.
   3. Drafting Team members.

25. NY adoption of more stringent/specific NPCC Criteria

a. The New York filing (as well as an update to the applicable NPCC Criteria in Nova Scotia that were approved by the Nova Scotia Utility and Review Board earlier this year), will be filed by the end of October, 2011.

26. Directory and Regional Work Plan Status

a.

Directory Number	Title	Lead Group, Status	Current Activity
#1 (A-2)	Design and Operation of the Bulk Power System	Approved on 12/1/2009	TFCP has charged CP11 with a comprehensive review of Directory #1 to include the triennial document review, an examination of the NERC TPL standards, the existing NPCC planning criteria, and the implementation of Phase 2 of the Directory Project which will reformat the existing Directory criteria into NERC style requirements. TFCO has assigned CO-8 to review the TO requirements within the Directory #1 criteria. CP-11 has completed its review and returned the document to TFCP. TFSS and TFCO (CO-8) are also reviewing the draft and it is expected that the TFCO and TFSS will return the draft document to TFCP in early 2012 in order for the TFCP to post the initial draft to the Open Process.
#2 (A-3)	Emergency Operation	Approved on 10/21/08.	Automatic UFLS language transferred to Directory #12. Next TFCO review Oct. 21, 2011.
#3 (A-4)	Maintenance Criteria for BPS Protection.	Approved on 7/11/08.	Phase 2 reformatting pending.
#4 (A-5)	Bulk Power System Protection Criteria	Approved on 12/1/09.	TFSP expects to begin Phase 2 review of Directory #4 in early 2012.
#5 (A-6)	Operating Reserve	TFCO	Directory#5 was approved by the Full Members on December 2, 2010. TFCO is working to resolve several open issues including how imports from HQ are wheeled within the Region. A TFCO special meeting is scheduled for Dec. 6, 2011 to finalize proposed revisions to Directory #5 in advance of an Open Process posting.
#6 New	Reserve Sharing	TFCO	TFCO has posted a draft of a new Directory#6 on Regional Reserve Sharing which would replace C-38 until a Regional Standard is developed. An Open Process posting for Directory #6 concluded on Oct. 24, 2011, and awaiting the TFCO response to comments.
#7 (A-11)	Special Protection Systems	Approved on 12/27/07.	TFSP, TFSS, and TFCP are revising Directory #7. TFSP to incorporate current NRAP revisions (including Appendix A) of the document into a Phase 2 version and post for member comment after the November, 2011 TFSP Meeting.
#8 (A-12)	System Restoration	Approved on 10/21/08.	CO-11 has recently made revisions to the Directory #8 criteria. These revisions will be incorporated into the draft Phase 2 reformatting of Directory #8 which will be addressed by CO-8 early next year.

#9 (A-13)	Verification of Generator Real Power Capability	Approved on 12/22/08.	TFCO has posted the initial Phase 2 drafts of both Directories #9 and #10 to the Open Process. The initial open process concluded on June 14, 2011. TFCO reviewed comments and posted the revised Directories for a second posting which concluded on 10/24/2011. TFCO expects to present Directories #9 and #10 to the RCC in November, 2011, and anticipates a Full Member ballot of both Directories #9 and #10 in December, 2011.
#10(A14)	Verification of Generator Reactive Power Capability	Approved on 12/22/08.	Refer to Directory #9 preceding.
#12	UFLS Program Requirements	Approved on 6/26/09.	

27. Review RFC, MRO Standards Relevant to NPCC (in Meeting Materials Package)

a. RFC Standards Under Development webpage
https://rsvp.rfirst.org/default.aspx

b. RFC Standard Voting Process (RSVP) webpage
ReliabilityFirst Corporation - Reliability Standards Voting Process

	Standard Under Development	Status	Start Date	End Date
1.	PRC-006-RFC-01 (Automatic Underfrequency Load Shedding)	Comment Period	9/28/11	10/27/11
	NERC Posting PRC-006-RFC-01	Comment Form	10/3/11	11/2/11

c. Midwest Reliability Organization Approved Standards
http://www.midwestreliability.org/STA_approved_mro_standards.html
(click on RSVP under the MRO header)

d. Midwest Reliability Organization Reliability Standard Voting Process webpage (table lists standards under development)
Midwest Reliability Organization - Reliability Standards Voting Process

	Standard Under Development	Status	Start Date	End Date
1.				
2.				

e. As of June 14, 2010 MRO suspended its regional standards development.

28. Report on NERC, NAESB and Regional Activities (in Meeting Materials Package)

a. Report on NERC, NAESB and Regional Activities
   1. October, 2011.

29. Task Force Assignments, et al. (in Meeting Materials Package)

a.

30. Future Meetings and Other Issues (in Meeting Materials Package)

a. NERC News
   1. October, 2011 Edition.
b. NERC Analysis of NERC Standard Process Results Third Quarter 2011 filed in Docket Nos. RR06-1-000, RR09-7-000.
c. NERC Reliability Standards and Compliance Workshop - October 26-28, 2011.
d. SNL Energy Power Daily--Senators see electric power system reliability declining. (see page 3).
e. TFCO Review of the of the Proposed Modification to the Maxcys-Bucksport Special Protection System.
f. Project 2007-12 Frequency Response and Frequency Bias Setting Webinar--Nov. 14, 2011.
g. NERC Standards 101 Webinar--slides.
h. NPCC Board of Directors Meeting Nov. 30, 2011--Agenda. Changes to RSC membership.
i. NERC Completes First Grid Security Exercise.
j. NERC Standards Prioritization.
k. Project 2008-06 Cyber Security Order 706 Industry Webinar – November 15, 2011--slides.
l. Project 2007-12 Frequency Response Industry Webinar – November 14, 2011--slides.
m. ISO - New England--October 2011 Snowstorm.
n. NERC Hires New Enforcement Director.
o. NERC Media Release--Reserve Margins Down in Some Areas; NERC Integrated Analysis Shows Impact of Environmental Assessment.
p. SERC Regional Standards Development Plan--requested SERC Board of Director actions.
   1. Link to supporting documents.

q. NERC Participates in FERC Technical Conference.

RSC 2012 Meeting Dates

February 22-23, 2012 NPCC Offices	May 2-3, 2012 Dominion Resources Services Tredegar Facility
July 18-19, 2012 New England Location	September 5-6, 2012 Hydro-Quebec Offices, Montreal
October 24-25, 2012 Toronto	December--coincide with General Meeting

2011 RSC Conference Call Schedule

(call 719-785-1707, Guest Code 8287#)

Dec. 16, 2011
Dec. 30, 2011

BOD 2012 Meeting Dates

January 31, 2012--NPCC Offices
February 1, 2012--NPCC Offices
March 13, 2012 (BES Special Teleconference)
May 1, 2012 (Teleconference)
June 26, 2012--NPCC Offices
August 7, 2012 (Teleconference)
September 19, 2012--NPCC Offices
October 30, 2012 (Teleconference)
November 28, 2012--Montreal, Quebec

RCC, CC, and Task Force Meeting Dates--2011/2012

RCC	Nov. 29, 2011
	2012-- March 1, June 6, Sept. 6, Nov. 27
CC	Nov. 16, Dec. 13-15
TFSS	
TFCP	Feb. 8, May 9, August 15, Nov. 7
TFCO	
TFIST	
TFSP	Nov. 15-17

Respectfully Submitted,

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

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

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

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment. Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

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

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's Secretary, Andrianne S. Payson at 212-259-8218.

Action Item List

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
August 20-21, 2008					
Feb. 17-18, 2009					
June 17-18, 2009					
August 6-7, 2009					
60	3a	NPCC representatives from NERC drafting teams that have documents posted for comments report at RSC Meetings	Lee Pedowicz	RSC Meeting	Ongoing.
Sept. 24-25, 2009					
Nov. 4-5, 2009					
April 21-22, 2010					
63	----	Coordination with the Compliance Committee to develop Joint Activity Action List	Greg Campoli	RSC Meeting	Outgrowth of RSC/CC joint session April 21, 2010. Ongoing. Joint RSC/CC Meeting this meeting. Ralph Rufrano rejoined the RSC in the capacity of NPCC Compliance liaison. Comments not to be

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
					submitted on the CCEP.
June 29-30, 2010					
65	----	RSC to review the NPCC Members on NERC Drafting Teams list. Saurabh Saksena to maintain. Will get input from Carol Sedewitz.	RSC	RSC Meeting	Ongoing.
August 18-19, 2010					
66	----	Status of Memorandum of Understanding	Sylvain Clermont	RSC Meeting	Provide update. (MOU in Meeting Materials Package)
Nov. 30, 2010,					
Dec. 2, 2010					
69	----	Revise RSC Scope	Guy Zito	RSC Meeting	Approved at the August 3, 2011 RSC Meeting. To be presented to the NPCC Board of Directors.

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
Feb. 2-3, 2011					
71	----	Talk to Compliance about Regional Reliability Standard RSAWs. There should be a Compliance Committee representative on the Drafting Team.	Guy Zito	RSC Meeting	Ongoing.
73	----	Discuss consistency with the RSG.	Guy Zito	RSC Meeting	Ongoing.
March 16-17, 2011					
75	11f	Non-convergent contingencies enumerated in Project 2010-13 - Relay Loadability Order - PRC-023 Attachment B4a.	Guy Zito	RSC Meeting	To be discussed with Sal Buffamante.
August 3-4, 2011					
October 26-27, 2011					
77	22d	If a term defined in one document, should it be included in the NPCC Glossary?	Guy Zito/Gerry Dunbar	RSC Meeting	Ongoing.

November 2011
Meeting Summaries

These are summaries of orders voted by the Federal Energy Regulatory Commission at its November 17, 2011 public meeting. The summaries are produced by FERC's Office of External Affairs and are intended to provide only a general synopsis of the orders. These are not intended as a substitute for the Commission's official orders. To determine the specific actions and the Commission's reasoning, please consult the individual orders when they are posted to FERC's eLibrary found at www.ferc.gov.

G-1, Press Release

G-2, 3, 4, Press Release

H-1, Press Release

FERC accepts filing

E-1, *PJM Interconnection, L.L.C.; Trans-Allegheny Interstate Line Company*, Docket No. ER11-4574-000. This order accepts Trans-Allegheny Interstate Line Company's (TrAILCo) proposed modifications to TrAILCo's Attachment H-18 to the PJM OATT. As a result of the merger between Allegheny Energy, Inc. and FirstEnergy Corp., TrAILCo is now affiliated with FirstEnergy's operating companies (FirstEnergy affiliates). The proposed changes reflect the additional PJM transmission zones of the FirstEnergy affiliates in which TrAILCo may construct facilities.

FERC denies request for rehearing

E-2, *Nebraska Public Power District, Southwest Power Pool Regional Entity*, Docket No. RR11-1-002. This order denies Nebraska Public Power District's (NPPD) and Southwest Power Pool Regional Entity's (SPP RE) requests for rehearing of a Commission order upholding the North American Electric Reliability Corporation's denial of the request to transfer the compliance registrations of NPPD and several other registered entities located within Nebraska (together the "Nebraska Entities") from Midwest Reliability Organization to SPP RE. The order reaffirms that the transfer of the Nebraska Entities' compliance registration to SPP RE would likely result in compliance auditing inefficiencies and the need for increased coordination between Regional Entities.

FERC approves reliability standard, denies request for an exemption

E-4, *North American Electric Reliability Corporation,* Docket No. RD11-3-000. This order approves a revised Reliability Standard (FAC-013-2), which was developed in response to prior Commission directives regarding the need for transparency and consistency in assessing Transfer Capability. The proposed standard requires Planning Coordinators to have a transparent methodology for, and to annually perform, an assessment of transmission Transfer Capability over the near-term planning horizon. The order also denies ERCOT's request for an exemption from the requirements of the revised Reliability Standard, and requests further support for, or a modification of, certain Violation Risk Factors assigned to the revised Standard.

FERC approves reliability standard

E-5, *North American Electric Reliability Corp.*, Docket No. RD11-10-000. The order approves Reliability Standard FAC-008-3 (Facility Ratings) and the retirement of Reliability Standards FAC-008-1 (Facility Ratings Methodology) and FAC-009-1 (Establish and Communicate Facility Ratings). The order finds that FAC-008-3 presents measurable and enforceable requirements that obligate transmission owners and generator owners to develop facility ratings methodologies for its facilities. The order also approves the assigned Violation Severity Levels and the associated Violation Risk Factors (VRFs) with one modification. Specifically, the order directs NERC to change the VRF assigned to FAC-008-3, Requirement R2, from "Lower" to "Medium."

FERC denies rehearing; clarifies prior order

E-6, *Cedar Creek Wind Energy, LLC, Milford Wind Corridor Phase I, LLC*, Docket Nos. RC11-1-001 and RC11-2-001. This order denies rehearing and provides clarification of the Commission's order denying the appeals of two NERC registry decisions in which NERC found that Cedar Creek Wind Energy, LLC and Milford Wind Corridor Phase I, LLC were properly included on the NERC Compliance Registry as transmission owners and transmission operators.

FERC denies, in part, and grants, in part, request for clarification

E-7, *Northeast Transmission Development, LLC*, Docket No. EL11-33-001. This order denies in part and grants in part the Designated PJM Transmission Owners' request for clarification of the Commission's June 16, 2011 order on Northeast Transmission's petition for transmission rate incentives.

FERC grants petition seeking a declaratory order

E-8, *Duke Energy Ohio, Inc.*, Docket No. EL11-58-000 *et al.* The order grants the petition of Duke Energy Ohio, Inc. seeking a declaratory order finding that its proposed payment of dividends from equity accounts will not violate section 305(a) of the Federal Power Act.

FERC grants, in part, and denies, in part, request for rehearing and directs further revision

E-10, *Westar Energy, Inc.*, Docket No. ER09-1273-002 *et al.* This order grants in part and denies in part American Wind Energy Association's and the Wind Coalition's request for rehearing of the Commission's March 18, 2010 order in this proceeding. The March 18, 2010 order accepted Westar Energy, Inc.'s proposed *pro forma* Balancing Area Services Agreement and Schedule 3A, Generator Regulation and Frequency Response Service, which enabled Westar to charge for and provide generation regulation and frequency response services to generators located in Westar's balancing area whose output is delivered outside Westar's balancing area or to Southwest Power Pool, Inc.'s energy imbalance market. The order also institutes a proceeding under section 206 of the FPA, establishes a refund effective date, and directs Westar to submit a compliance filing within thirty days that would require Westar to aggregate certain data in calculating the Schedule 3A regulation requirements.

FERC acts on rehearing requests, technical conference, and compliance filing

E-11, *PJM Interconnection, L.L.C.*, Docket No. ER11-2875-001, *et al*. The order addresses PJM's Minimum Offer Price Rule (MOPR) - a mechanism that seeks to prevent the exercise of buyer market power in the forward capacity market by ensuring that all new resources are offered into PJM's Reliability Pricing Model (RPM) on a competitive basis. The order addresses requests for rehearing and clarification of an earlier order, issued April 12, 2011, a technical conference established to consider a rehearing issue relating to self-supply, and a PJM compliance filing. The Commission generally affirms its acceptance of PJM's proposed revisions to the MOPR, finding that the MOPR helps ensure that wholesale prices are just and reasonable and should elicit new entry when new capacity is needed. The Commission finds that PJM's proposal to permit suppliers to justify their costs on a project-specific basis will allow reasonable consideration of the cost and revenue characteristics and business models of individual projects.

FERC denies request for rehearing; conditionally accepts compliance filing and directs Commission staff to commence a technical conference

E-12, *California Independent System Operator Corporation*, Docket Nos. ER10-1706-001 and ER10-1706-002. This order denies the California Independent System Operator Corporation's (CAISO) request for rehearing of the Commission's August 31, 2010 order accepting, in part, and rejecting, in part, certain tariff revisions proposed by CAISO relating to interconnection requirements applicable to large asynchronous generators, primarily wind and solar photovoltaic resources. The order finds that CAISO did not provide sufficient evidence to justify its requested tariff revisions, and that the August 31, 2010 order was not in conflict with the Commission's order approving the North American Electric Reliability Corporation's interpretation of the Commission-approved Voltage and Reliability Standard designated VAR-002-1.1b, and does not arbitrarily discriminate against existing conventional generators. The order conditionally accepts CAISO's September 30, 2011 compliance filing, subject to a subsequent compliance filing. The order also directs Commission staff to commence a technical conference to consider the reactive power provisions of Order No. 661-A and the evidentiary requirements necessary to make a showing under that order.

FERC approves proposed amendments to NERC's Rules of Procedure

E-13, *North American Electric Reliability Corporation*, Docket No. RR11-5-000. This order approves NERC's proposed amendments to the NERC Rules of Procedure. The amendments modify the Election Procedure for Members of NERC Standards Committee and the Registered Ballot Body Criteria.

FERC accepts and suspends a request

E-14, *Nevada Power Company*, Docket No. EL11-4215-000. The order accepts and suspends a request for cancellation of rate schedule, and sets the matter for hearing and settlement procedures.

FERC rejects motion for clarification and request for rehearing

H-2, *FirstLight Hydro Generating Company*, Project No. 2576-151. This order rejects the Candlewood Lake Authority's motion for clarification and request for rehearing of a September 23, 2011 Commission staff order approving the request of FirstLight Hydro Generating Company to modify the nuisance plant monitoring plan for its Housatonic Project No. 2576 located in Connecticut, because the Authority is not a party to the proceeding. For clarity, however, the order also addresses Candlewood's substantive concerns.

FERC denies rehearing

H-3, *Duke Energy Carolinas, LLC,* Project No. 2601-015. The order denies a request for rehearing by Paulette Smart of a September 20, 2011, notice denying her late motion to intervene in the relicensing proceeding for the Bryson Hydroelectric Project No. 2601 located in North Carolina. The order concludes that Ms. Smart has not provided good cause for intervening late and that she is not aggrieved by the underlying order, but, for clarity, addresses her substantive concerns.

FERC denies rehearing

H-4, *The Nevada Hydro Company, Inc.*, Project No. 11858-004. This order denies Nevada Hydro Company's request for rehearing of an order issued July 12, 2011, in which the Director of FERC's Office of Energy Projects dismissed the license application filed by Nevada Hydro and its co-applicant, Elsinore Valley Municipal Water District, for the proposed Lake Elsinore Advanced Pumped Storage Project, in California. The Director dismissed the application based on his conclusion that the co-applicants, which have had ongoing disagreements regarding the status of a transmission line included in the project description, would be unlikely to be able to work together as co-licensees.

In its order denying rehearing, the Commission finds the Director correctly concluded that the disagreements between the co-applicants were such that the Commission could not rely on them to be cooperating co-licensees, and that his dismissal of the application was within his discretion.

FERC authorizes revised protective buffer zone for a storage facility in NY

C-2, *Dominion Transmission Inc.*, Docket No. CP11-493-000. The order authorizes Dominion Transmission, Inc. to revise the active boundary and to establish a 2,000-foot buffer zone around its Woodhull Storage Pool located in Steuben County, New York. The order finds that the proposed protective buffer should protect the Woodhull Storage Pool from potential breaches that may be caused from the hydraulic fracturing used in the drilling of Marcellus Shale wells in the vicinity of the Pool.

FERC approves construction of certain natural gas facilities in PA

C-3, *Texas Eastern Transmission, LP,* Docket Nos. CP11-67-000 and 001.

The order authorizes, subject to conditions, a proposal by Texas Eastern to construct, operate, and abandon certain facilities on its mainline in Greene and Lancaster Counties, Pennsylvania.

FERC grants clarification and rehearing

C-4, *Tennessee Gas Pipeline Company*, Docket No. CP11-36-001. This order grants Tennessee Gas Pipeline Company's request for clarification and rehearing of the Commission's August 24, 2011 Order Issuing Certificate. This order clarifies that a provision in Tennessee's binding precedent agreement with The Berkshire Gas Company is not non-conforming, as originally determined in the August 24 Order. This order also grants Tennessee's request for rehearing to allow it until November 1, 2012 to place the Northampton Expansion Project into service. The project would be located in Southwick, Massachusetts.

From:	Philip A. Fedora
To:	grpStaff
Subject:	November FERC Open Meeting Summary
Date:	Thursday, November 17, 2011 12:18:20 PM
Attachments:	20111117104741-summaries.pdf E-5.pdf

Of Note:

FERC approves reliability standard, denies request for an exemption

E-4, *North American Electric Reliability Corporation*, Docket No. RD11-3-000. This order approves a revised Reliability Standard (FAC-013-2), which was developed in response to prior Commission directives regarding the need for transparency and consistency in assessing Transfer Capability. The proposed standard requires Planning Coordinators to have a transparent methodology for, and to annually perform, an assessment of transmission Transfer Capability over the near-term planning horizon. The order also denies ERCOT's request for an exemption from the requirements of the revised Reliability Standard, and requests further support for, or a modification of, certain Violation Risk Factors assigned to the revised Standard.

FERC approves reliability standard (attached)

E-5, *North American Electric Reliability Corp.*, Docket No. RD11-10-000. The order approves Reliability Standard FAC-008-3 (Facility Ratings) and the retirement of Reliability Standards FAC-008-1 (Facility Ratings Methodology) and FAC-009-1 (Establish and Communicate Facility Ratings). The order finds that FAC-008-3 presents measurable and enforceable requirements that obligate transmission owners and generator owners to develop facility ratings methodologies for its facilities. The order also approves the assigned Violation Severity Levels and the associated Violation Risk Factors (VRFs) with one modification. Specifically, the order directs NERC to change the VRF assigned to FAC-008-3, Requirement R2, from "Lower" to "Medium."

AGREEMENT
ON THE DEVELOPMENT OF ELECTRIC POWER TRANSMISSION RELIABILITY STANDARDS AND OF PROCEDURES AND A PROGRAM FOR THE MONITORING OF THE APPLICATION OF THESE STANDARDS FOR QUÉBEC

BETWEEN

Régie de l'énergie, a public body established under the *Act respecting the Régie de l'énergie* (R.S.Q., c. R-6.01) with headquarters at Tour de la Bourse, P.O. Box 001, 800 Place Victoria, 2nd floor, Suite 2.55, Montréal, Québec H4Z 1A2, acting through Jean-Paul Théorêt, Chairman, duly authorized pursuant to subsection 85.4 of the *Act respecting the Régie de l'énergie* (R.S.Q., c. R-6.01),

hereinafter referred to as "the Régie"

AND

North American Electric Reliability Corporation, a corporate body established under the *New Jersey Nonprofit Corporation Act*, New Jersey Statutes Title 15A, with headquarters at 116-390 Village Boulevard, Princeton, New Jersey, United States, 08540-5721, acting through Richard P. Sergel, President and Chief Executive Officer, duly authorized pursuant to Article VI, Section 1, of the Bylaws of the North American Electric Reliability Corporation,

hereinafter referred to as "NERC"

AND

Northeast Power Coordinating Council, Inc., a corporate body established under Section 402 of the *New York State Not-for-Profit Corporation Law*, with headquarters at 1515 Broadway, 43rd floor, New York, New York, United States, 10036, acting through Edward A. Schwerdt, President and Chief Executive Officer, duly authorized pursuant to the Amended and Restated Bylaws of the Northeast Power Coordinating Council, Inc.,

hereinafter referred to as "NPCC."

WHEREAS subsection 85.2 of the *Act respecting the Régie de l'énergie* (the "Act") provides for the Régie to ensure that electric power transmission in Québec is carried out in accordance with the reliability standards it adopts;

WHEREAS reliability refers to the degree of performance of an electric power transmission system that results in electricity being delivered to customers within accepted standards and in the amount desired and may be measured by the frequency, duration, and magnitude of adverse effects on the electric supply;

WHEREAS subsection 85.4 of the Act further provides that the Régie, with the authorization of the Government of Québec, may enter into an agreement with a body that proves it has the expertise to establish or monitor the application of electric power transmission reliability standards for the purpose of developing such standards for Québec, carrying out inspections and investigations as part of plans to monitor compliance with the reliability standards that the Régie adopts, and providing the Régie with opinions and recommendations;

WHEREAS NERC is a New Jersey, United States (U.S.), not-for-profit corporation sponsored by all sectors of the utility industry, including those in Québec, whose mission is the development and enforcement of reliability standards to protect the reliability, adequacy, and security of the bulk power system in North America. NERC is the successor to the North

American Electric Reliability Council. NERC coordinates its activities with eight (8) regional entities in North America, including NPCC;

WHEREAS NERC has established the *NERC Reliability Standards Development Procedure,* in which all Québec entities subject to the reliability standards referred to in subsection 85.3 of the Act may participate;

WHEREAS the American National Standards Institute ("ANSI") has accredited the *NERC Reliability Standards Development Procedure* as being consistent with ANSI's standards development principles;

WHEREAS the U.S. Federal Energy Regulatory Commission ("FERC") has certified NERC as the Electric Reliability Organization, in accordance with the *Electricity Modernization Act of 2005*, to develop, submit to it for approval and enforce reliability standards for the bulk power system in the United States, subject to certain delegation provisions for the eight (8) regional entities in North America, including the delegation provisions for NPCC described below;

WHEREAS by means of legislation or other provisions, Ontario, New Brunswick, Manitoba, British Columbia, Alberta, Saskatchewan and Nova Scotia, have made or will make mandatory the NERC reliability standards;

WHEREAS the Régie has concluded that NERC has proven that it has the expertise to develop and monitor the application of electric power transmission reliability standards;

WHEREAS NPCC is a not-for-profit corporation in New York State, United States, having the purpose of promoting and enhancing the reliable and efficient operation of the international, interconnected bulk power systems in northeastern North America through the development of regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards, coordination of system planning, design and operations, and assessment of reliability, pursuant to an agreement with NERC which designates NPCC as a cross-border regional entity for the northeastern United States and delegates authority from FERC. Additionally, NPCC establishes regionally specific, more stringent reliability criteria and monitors and enforces compliance with such criteria;

WHEREAS NPCC has developed the *NPCC Regional Reliability Standards Development Procedure*, approved by NERC on October 23, 2007 and adopted by FERC on March 21, 2008, for the purpose of developing specific reliability standards for interconnected networks in northeastern North America in which Québec entities subject to the reliability standards referred to in subsection 85.3 of the Act may participate;

WHEREAS the Régie has concluded from NPCC's more than four decades of international reliability assurance that NPCC has the expertise to develop, monitor the application of, and assess compliance with electric power transmission reliability standards and criteria;

WHEREAS the Régie has resolved, for the reasons set out above, to mandate NERC and NPCC to develop reliability standards that the Régie adopts for electric power transmission in Québec and the procedures and a program for the monitoring of the application of these standards, and provide the Régie with opinions and recommendations pursuant to the present agreement (the "Agreement");

WHEREAS pursuant to subsection 85.5 of the Act, the Régie designated a reliability coordinator for Québec in its Decision D-2007-95;

WHEREAS pursuant to subsection 85.6 of the Act, the said reliability coordinator must file with the Régie the reliability standards proposed by a body that has entered into an agreement with the Régie under subsection 85.4 of the Act, as well as any variant or other standard the reliability coordinator considers necessary, an evaluation of the relevance and impact of the standards filed and the identification of the entities that may be subject to the reliability standards;

WHEREAS pursuant to subsection 85.7 of the Act, the Régie may request the reliability coordinator to modify a standard filed or submit a new one;

WHEREAS pursuant to subsection 85.7 of the Act, the Régie shall adopt the reliability standards and set the date for their coming into force;

WHEREAS pursuant to subsection 85.7 of the Act, the reliability standards may provide for a schedule of sanctions, including financial penalties, that apply if standards are not complied with and refer to reliability standards set by a standardization agency that has entered into an agreement with the Régie;

WHEREAS pursuant to subsection 85.8 of the Act, the reliability coordinator shall submit to the Régie a guide describing criteria to be taken into account in determining the sanction for non-compliance with a reliability standard;

WHEREAS pursuant to subsection 85.9 of the Act, if an entity is the object of a violation allegation to a reliability standard, it has at least twenty (20) days to submit observations to the body mandated by the Régie for the monitoring of the application of the reliability standards before this body reports to the Régie and recommends the application of a sanction, if need be;

WHEREAS pursuant to subsection 85.13 of the Act, the reliability coordinator must submit to the Régie, for approval, a register identifying the entities subject to the reliability standards adopted by the Régie;

WHEREAS the parties to the Agreement recognize the need to coordinate and to cooperate for the enhancement of the reliability of the North American bulk power system, including Québec's electric power transmission system, and to facilitate the exchange of experience, information and data related to that system;

WHEREAS the Québec electric power transmission system is an asynchronous interconnection and NERC and NPCC have recognized it as an Interconnection, it may, therefore, require reliability standards or variants of such standards specific to this Interconnection;

NOW THEREFORE, the Régie, NERC and NPCC agree as follows:

1. INTERPRETATION

1.1 Exclusivity of Agreement

This Agreement constitutes the entire agreement between the parties with respect to the development of reliability standards applicable to Québec and of the procedures and a program for the monitoring of the application of such standards, and opinions and recommendations provided by NERC or NPCC with respect to such standards and the electric power transmission reliability in Québec. It supersedes all prior agreements and understandings, both written and oral, among the parties with respect to the subject matter of this Agreement.

1.2 Governing law and competent jurisdiction

This Agreement shall be governed by the laws of Québec, and the courts of Québec shall have exclusive jurisdiction to settle any disputes arising herefrom.

1.3 Headings

The headings of this Agreement are for convenience of reference only and shall not define, limit, or otherwise affect any of the terms or provisions hereof.

2. REPRESENTATIVES

For the purposes of the application of the Agreement, the Régie designates Gilbert Neveu, Executive Director, as its representative; NERC designates David Cook, Vice President, as its

representative; and NPCC designates Edward A. Schwerdt, President, as its representative. Each of the parties undertakes to expeditiously advise the other parties of any change in its representative.

3. PURPOSE OF AGREEMENT

3.1 The Régie hereby retains the services of NERC and NPCC as experts in the development of electric power transmission reliability standards. NERC and NPCC shall develop, in accordance with their standards development procedures, electric power transmission reliability standards applicable to Québec, and propose them to the reliability coordinator for adoption by the Régie. The services of NERC and NPCC are also required as technical experts to advise the Régie with respect to the review of the reliability standards and of the sanction guide which will be filed by the reliability coordinator, and to provide the Régie with opinions and recommendations.

3.2 The Régie also retains the services of NERC and NPCC as experts in the monitoring of the application of electric power transmission reliability standards. NERC and NPCC shall develop, taking into account Québec's legal and regulatory environment and in accordance with their applicable compliance monitoring procedures, specific procedures and a program for the monitoring of the application of electric power transmission reliability standards in Québec which they are able to implement. The Régie shall be responsible for the said procedures and program.

3.3 The said specific procedures and program for the monitoring of the application of electric power transmission reliability standards in Québec will be submitted to a consultation with the entities subject to the reliability standards.

3.4 Subsequent to the said consultation and upon authorization from the Government of Québec, a second agreement shall detail the mandates granted by the Régie to NERC and to NPCC with respect to the implementation of the said procedures and program for the monitoring of the application of electric power transmission reliability standards in Québec and the provision of opinions and recommendations to the Régie in this regard.

4. UNDERTAKINGS OF NERC AND NPCC

4.1 NERC and NPCC undertake to develop electric power transmission reliability standards applicable to Québec in accordance with their procedures, namely the *NERC Reliability Standards Development Procedure* and the *NPCC Regional Reliability Standards Development Procedure*. To this end, NERC and NPCC undertake, within the framework of their respective procedures, to take note of the comments and opinions submitted by the Québec reliability coordinator, the electric power carriers and users of electric power transmission services in Québec.

4.2 NERC and NPCC undertake to ascertain that any electric power transmission reliability standards specific to Québec, and/or any variant of such standards specific to Québec, which the reliability coordinator deems necessary to ensure the reliability of electric power transmission in Québec, is as stringent as the NERC reliability standards applicable in the rest of North America.

4.3 NERC and NPCC undertake to develop, in accordance with their compliance monitoring procedures, namely the *NERC Rules of Procedures,* the *NERC Uniform Compliance Monitoring and Enforcement Program* and the *NPCC Compliance Monitoring and Enforcement Program,* specific program and procedures for the monitoring of the application of electric power transmission reliability standards adapted to Québec's legal and regulatory environment.

4.4 NERC and NPCC undertake to have representatives present or, as necessary, to testify as technical experts at the hearings the Régie will hold, if need be, when filings regarding reliability standards are examined by the Régie pursuant to subsections 85.6 and 85.7 of the Act, and when the sanction guide filed by the reliability coordinator pursuant to subsection 85.8 of the Act is reviewed.

4.5 NERC and NPCC undertake to submit to the Régie, at the Régie's request, opinions or recommendations during the proceedings referred to in Article 4.4, including but not limited to opinions or recommendations respecting matters submitted to the Régie's consideration by the reliability coordinator.

4.6 NERC and NPCC undertake to inform the Régie promptly of potential threats to the reliability of the electric power transmission system in Québec.

4.7 NERC and NPCC undertake to submit to the Régie, at the Régie's request or on their own initiative, opinions or recommendations on all matters related to the reliability of electric power transmission in Québec.

4.8 NERC and NPCC undertake to collaborate closely with the Régie on the implementation of this Agreement and to take into consideration all instructions and recommendations from the Régie related to this Agreement.

4.9 NERC and NPCC undertake to develop the procedures and a program for the monitoring of the application of the electric power transmission reliability standards for Québec which they will be able to implement, and to provide the Régie with opinions and recommendations.

4.10 NERC and NPCC hereby represent and warrant that during the term of this Agreement each of them shall remain validly existing and in good standing pursuant to all applicable laws relevant to this Agreement.

5. REMUNERATION

5.1 The total remuneration received by NERC and NPCC for, among other things, developing and monitoring the application of electric power transmission reliability standards in the United States and Canada (and, in the case of NERC only, in Mexico) is allocated in accordance with the currently effective calculation method approved by the NERC Board of Trustees.

5.2 Québec's share of that total remuneration is currently paid by Hydro-Québec TransÉnergie, Québec's electric power carrier, as approved by the Régie in its decisions in which it fixes or modifies the electric power carrier's rates pursuant to section 49 of the Act.

5.3 Québec's share of the total remuneration approved by NERC's Board of Trustees in consideration of the monitoring of the application of electric power transmission reliability standards in Québec by NERC and NPCC will be paid by the Régie as of the date of signing the Agreement and shall cover all the services they undertake to provide to the Régie under this Agreement.

5.4 Québec's share of the total remuneration will continue to be paid by Hydro-Québec TransÉnergie, as approved by the Régie, with the exception of the portion of Québec's share, referred to in Article 5.3, which will be paid by the Régie as of the date of signing the Agreement.

5.5 NERC and NPCC agree that this remuneration shall cover all the services they undertake to provide under this Agreement.

5.6 NERC and NPCC shall provide the Régie with the draft versions of their respective annual Business Plans and Operating Budgets by May 31st of each year and with the final versions of the said documents by August 15th of each year.

5.7 By December 1st of each year, at the latest, NERC and NPCC shall provide the Régie with their final budgets for the coming calendar year for the portion of Québec's share that will be paid by the Régie, in order to allow the Régie to prepare its own budget.

5.8 If the Régie objects to the budgets or any invoice(s) submitted under this Agreement, it shall promptly notify NERC and/or NPCC in writing. The parties agree that, should the

Régie object to an invoice, payment shall be effected under protest and the objection resolved pursuant to Article 9.

6. DECLARATIONS

NERC and NPCC do hereby declare that no applicable law, contract or other legal obligation prevents them from executing this Agreement and fulfilling their obligations hereunder.

The Régie declares that it has been duly authorized by the Government of Québec to make this Agreement, pursuant to subsection 85.4 of the Act.

7. TERM OF AGREEMENT AND TERMINATION

This Agreement is effective as of the date of the last signing by the parties.

Either party may terminate this Agreement upon one year's notice to the other party.

8. DEFAULT AND CURE

Upon the failure of a party to perform or observe any material term, condition or covenant of the Agreement, the non-breaching party shall give written notice of such breach to the breaching party (the "Default Notice"). Subject to a suspension of the following deadlines as specified below, the breaching party shall have thirty (30) days from receipt of the Default Notice within which to cure such breach; provided however, that if such breach is not capable of cure within thirty (30) days, the breaching party shall commence such cure within thirty (30) days after notice and continuously and diligently complete such cure within ninety (90) days from receipt of the Default Notice; and, if cured within such time, the breach specified in such notice shall cease to exist. Subject to the limitation specified in the following sentence, if a breach is not cured as provided in this Article, or if a breach is not capable of being cured within the period provided for herein, the nonbreaching party shall have the right to declare a default and resiliate this Agreement by written notice at any time until cure occurs, and be relieved of any further obligation hereunder. The deadlines for cure and the right to declare a default and terminate this Agreement shall be suspended during the pendency of any efforts or proceedings in accordance with Article 9 of this Agreement to resolve a dispute as to whether a breach has occurred. Resiliation of this Agreement does not extinguish any obligation existing at the time of the resiliation.

9. DISPUTE RESOLUTION

In the event a dispute arises under this Agreement between the Régie, NERC and/or NPCC, representatives of the parties with authority to settle the dispute shall meet and confer in good faith in an effort to resolve the dispute in a timely manner. In the event the designated representatives are unable to resolve the dispute within thirty (30) days or such other period as the parties may agree upon, each party shall have all rights to pursue all remedies, except as expressly limited by the terms of this Agreement. Neither party shall have the right to pursue other remedies until the Dispute Resolution procedures of this Article 9 have been exhausted. This Article 9 shall not apply to enforcement actions against registered entities.

10. LIMITATION OF LIABILITY

The Régie agrees not to sue NERC or NPCC or their directors, officers, employees, and persons serving on their committees and subgroups based on any act or omission of any of the foregoing in the performance of duties pursuant to this Agreement or in conducting activities under the authority of the Act, except to the extent that NERC or NPCC is found liable for gross negligence or intentional misconduct.

11. ASSIGNMENT

NERC and NPCC may not assign their rights and obligations under this Agreement without the consent of the Régie. However, nothing in this provision shall prohibit NERC or NPCC from contracting with other entities to assist them in carrying out their responsibilities under

the Agreement. NERC and NPCC shall, however, remain responsible for their obligations under this Agreement.

12. CONFIDENTIALITY

The information contained in the opinions and recommendations of NERC or NPCC to the Régie may not be copied, disclosed or distributed without the prior written permission of the Régie. In their opinions and recommendations, NERC and NPCC may identify the information they deem to be confidential.

During the course of the parties' performance under this Agreement, a party may receive Confidential Information, as defined in Section 1500 of NERC's Rules of Procedure or information of the same nature considered confidential by the Régie. Except as set forth herein, the parties agree to keep in confidence and not to copy, disclose, or distribute any Confidential Information or any part thereof, without the prior written permission of the issuing party, unless disclosure is required by subpoena, law, or other directive of a court, administrative agency, or arbitration panel, in which event the recipient hereby agrees to provide the party that provided the Confidential Information with prompt notice of such request or requirement in order to enable such issuing party to (a) seek an appropriate protective order or other remedy, (b) consult with the recipient with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Article. In the event a protective order or other remedy is not obtained or the issuing party waives compliance with the provisions, the recipient agrees to furnish only that portion of the Confidential Information which the recipient's counsel advises is legally required and to exercise best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. In addition, each party shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein.

13. NO THIRD PARTY BENEFICIARIES

Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any third party.

14. NOTICE

Whether expressly so stated or not, all notices, demands, requests, and other communications required or permitted by or provided for in this Agreement shall be given in writing to a party at the address set forth below, or at such other address as a party shall designate for itself in writing in accordance with this Article, and shall be delivered by hand or reputable overnight courier.

The Régie: Mr. Gilbert Neveu, Executive Director
Fax: (514) 873-3037
Email: gilbert.neveu@regie-energie.qc.ca

NERC: Mr. David Cook, Vice President
Fax: (609) 452-9550
Email: david.cook@nerc.net

NPCC: Mr. Edward A. Schwerdt, President
Fax: (212) 302-2782
Email: eschwerdt@npcc.org

15. EXECUTION OF COUNTERPARTS

This Agreement is executed in four (4) counterparts in French and four (4) counterparts in English and each has the same force and effect as the original.

IN WITNESS WHEREOF, the parties have caused the Agreement, in French and in English, both versions being regarded as equally authentic and valid, to be executed by their duly authorized representatives.

Signed for and on behalf of the Régie

Jean-Paul Théorêt
President
Régie de l'énergie
(514) 873-2452, extension 281

Date : 8 mai 2009

Signed for and on behalf of NERC

Richard P. Sergel
President and Chief Executive Officer
North American Electric Reliability Corporation
(609) 452-8060

Date : 8 mai 2009

Signed for and on behalf of NPCC

Edward A. Schwerdt
President and Chief Executive Officer
Northeast Power Coordinating Council, Inc.
(212) 840-1070

Date : 8 mai 2009

NPCC, Inc.

1040 Avenue of the Americas - 10th Floor
New York, New York 10018-3703

NPCC Regional Standards Committee
Preliminary Minutes--Draft
Meeting # 11-5

October 26, 2011 10:00 a.m. - 5:00 p.m.
October 27, 2011 8:00 a.m. - 3:00 p.m.

Hyatt Harborside at Boston's Logan International Airport
101 Harborside Drive
Boston, Massachusetts

Dress Business Casual

RSC@npcc.org

Call in 719-785-1707, Guest Code 8287#

Note: Glossary of Terms Used in NERC Reliability Standards dated August 4, 2011 included in the Meeting Materials.

Items in red from the October 26, 2011 session.
Items in green from the October 27, 2011 session.

Meeting called to order at 10:02 a.m.
Meeting called to order at 8:02 a.m.

1. **Introductions-Agenda Review-Roster**
   a. RSC membership changes.

	Name	***Organization***	***Sector***
1.	David Kiguel	Hydro One Networks Inc.	1
2.	Michael Lombardi	Northeast Utilities	1
3.	David Ramkalawan	Ontario Power Generation, Inc.	4
4.	Howard Gugel	NERC	Guest

5.	Mike Garton	Dominion Resources Services, Inc.	4
6.	Ron Falsetti	AESI Acumen Engineered Solutions International Inc.	Guest
7.	Don Weaver	New Brunswick System Operator	2
8.	Sylvain Clermont	Hydro-Quebec TransEnergie	1
9.	Kathleen Goodman	ISO - New England	2
10.	Greg Campoli	New York Independent System Operator	2
11.	Ben Wu	Orange and Rockland Utilities	1
12.	Si-Truc Phan	Hydro-Quebec TransEnergie	2
13.	Bruce Metruck	New York Power Authority	5
14.	Don Nelson	Commonwealth of Massachusetts	Guest
15.	Randy MacDonald	New Brunswick Power Transmission	1
16.	Lee Pedowicz	Northeast Power Coordinating Council	
17.	Gerry Dunbar	Northeast Power Coordinating Council	
18.	Brian Evans-Mongeon	Utility Services	5
19.	Tina Teng	IESO	Guest

On the Phone

	Name	***Organization***	***Sector***
1.	Saurabh Saksena	National Grid	3
2.	Chris de Granffenried	Consolidated Edison Co. of New York, Inc.	1
3.	Jerry Mosier (10/27)	Northeast Power Coordinating Council	

2. RSC August, 2011 Meeting Minute Approval and Antitrust Guidelines
(in Meeting Materials Package)

a. Discussion of the August, 2011 RSC Meeting minutes.

Lee Pedowicz read the NPCC Antitrust Compliance Guidelines.
Item 2a--Guy Zito reviewed the Minutes of the August, 2011 RSC Meeting. A motion to approve the Minutes as read was made by Don Weaver, and seconded by Michael Lombardi. A vote was taken, and with the exception of two abstentions, all others were in favor of accepting the Minutes.

3. **Action Item Assignment List and Ongoing Assignments** (in Meeting Materials Package), (Refer to Action Item Table [Item 65] at the back of Agenda)
   a. NPCC Members on NERC Drafting Teams

4. **Review Executive Tracking Summary** (in Meeting Materials Package)
   a. Review entries.

Item 4a--Michael Lombardi reviewed. RSC Members commented that they found the Executive Tracking Summary very useful.

5. **FERC** (in Meeting Materials Package)

   a. FERC News--September 15, 2011. Items from FERC Sunshine Open Meeting.
      1. September 15, 2011 Meeting Summaries.
   b. October 2011 Meeting Summaries.

NOPRs					
Item	NOPR	Docket No.	Posted	End Date	When Effective
T1	Version 4 Critical Infrastructure Protection Reliability Standards	RM11-11-000	9/15/11		
T2	Transmission Relay Loadability Reliability Standard	RM11-16-000	9/15/11		
T3	Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards	RM11-20-000	10/20/11 (Federal Register 10-26-11)	60 days after publication in the Federal Register	Comments due 12/27/11
T4	Transmission Planning Reliability Standards	RM11-18-000	10/20/11 (Federal Register 10-26-11)	60 days after publication in the Federal Register	

Letters of Approval			
Item	Docket No.	Posted	Summary
U1	RR10-12-001	8/25/11	Letter Order Issued Approving NERC Standards Process

			Manual Modifications
U2	RD11-7-000	9/15/11	FERC approves Reliability Standard PER-003-1
U3	RD11-8-000	10/20/11 (Federal Register 10/25/11)	FERC approves NPCC Regional Reliability Standard PRC-002-NPCC-01, and NERC's requested implementation plan.

Petitions			
Item	Docket No.	Posted	Title
V1	RD11-6-000	8/2/11	Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity
V2	Docket No. RM11-__-000	9/9/11	Petition of the North American Electric Reliability Corporation For Approval of Interpretations to Requirements of Reliability Standards EOP-001-0 and EOP-001-2— Emergency Operations Planning
V3	Docket No. RM__-__-___	10/19/11	Petition of the North American Electric Reliability Corporation For Approval of a Revised Transmission Planning System Performance Requirements Reliability Standard and Five New Glossary Terms and for Retirement of Four Existing Reliability Standards

Motion To Defer Further Action			
Item	Docket No.	Posted	Summary
W1	RM09-13-000	8/11/11	NERC requests that FERC defer action on BAL-004-1 to allow further research and analysis to be performed by NERC.
W2	RM09-13-000	8/11/11	NERC requests that FERC continue to defer action regarding the BAL-004-1 Time Error Correction standard.

Compliance Filing			
Item	Docket No.	Posted	Summary
X1	RM06-16-000	8/31/11	Second Quarter 2011 Compliance Filing of NERC in Response to Paragraph 629 of Order No. 693--timeframe to restore power

			to the auxiliary power systems of U.S. nuclear power plants following a blackout.
Final Rule			
Item	Docket No.	Posted	Summary
Y1	RM10-29-000; Order No. 753	9/15/11	FERC approves NERC's proposed interpretation of Reliability Standard, TOP-001-1, Requirement R8, which pertains to the restoration of real and reactive power during a system emergency.
Y2	RM10-6-000; Order No. 754	9/15/11	FERC rejects the NOPR for an alternative interpretation of Requirement R1.3.10 of Reliability Standard TPL-002-0. FERC approves NERC's proposed interpretation.

Other			
Item	Docket No.	Posted	Summary
Z1	RM08-13-004	9/15/11	Order Denying Reconsideration And Granting Clarification In Part And Denying Clarification In Part (Order No. 733-B)
Z2	RD11-5-000	9/26/11	Order Approving Interpretation Of Reliability Standards
Z3	RR10-1-001	9/28/11	Annual Report Of The North American Electric Reliability Corporation On Wide-Area Analysis Of Technical Feasibility Exceptions
Z4	AD-12-1-000 Notice of Technical Conference	10/7/11	FERC will hold a Technical Conference on Tuesday, November 29, 2011, from 1:00 p.m. to 5:00 p.m. and Wednesday, November 30, 2011, the purpose of which will be to discuss policy issues

			related to reliability of the Bulk-Power System.
Z5	RR11-3-000	10/17/11	Petition for Approval of Amendments to Delegation Agreement with NPCC.
Z6	RD11-9-000	10/20/11 (Federal Register 10/25/11)	Order Approving Interpretation Of Reliability Standards. FERC approves NERC's proposed interpretation of Requirement R10 of Reliability Standard TOP-002-2a, and approves the interpretation, referred to as Reliability Standard TOP-002-2b.
Z7	RR11-7-000	10/20/11	Order Accepting 2012 Business Plan And Budget of the North American Electric Reliability Corporation

6. Current and Pending Ballots:

a.	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Initial Ballot	11/7/11	11/16/11
b.	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Initial Ballot	11/8/11	11/17/11
c.	Project 2010-07 - Generator Requirements at the Transmission Interface	Initial Ballot	11/9/11	11/18/11

7. Overlapping Postings (in Meeting Materials Package)

a.				

8. Join Ballot Pools:

a.	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Join Ballot Pool	10/4/11	11/2/11
b.	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Join Ballot Pool	10/4/11	11/3/11
c.	Project 2010-07 - Generator Requirements at the Transmission Interface	Join Ballot Pool	10/5/11	11/4/11

9. Posted for Comment: (in Meeting Materials Package)

a.	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests BES Exception Process (Appendix 5C to NERC Rules of Procedure)--Redline Section 509 of NERC Rules of Procedure: Exceptions to the Definition of BES Section 1703 of NERC Rules of Procedure: Challenges to NERC Determinations of BES Exception Requests Under 509 Flow Charts Sample Form: Request for Exception to BES Definition Announcement	Comment Form (Word version in Meeting Materials)	9/13/11	10/27/11
b.	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company Draft 1--SAR MOD-028-2--Redline to Last Approved Implementation Plan FPL Request for Interpretation Announcement	Comment Form (Word version in Meeting Materials)	10/3/11	11/16/11
c.	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Comment Form (Word version in Meeting Materials)	10/4/11	11/17/11

	Draft 2 Interpretation--Redline to Last Posting Announcement			
d.	Project 2010-07 - Generator Requirements at the Transmission Interface FAC-001-1--Redline to Last Posted Redline to Last Approved FAC-003-x--Redline to Last Posted Redline to Last Approved FAC-003-3--Redline to Last Posted PRC-004-2.1--Redline to Last Approved Implementation Plans: FAC-001-1--Redline FAC-003-3--Redline FAC-003-x--Redline PRC-004-2--Clean Technical Justification Technical Justification for FAC-001-1 Announcement	Comment Form (Word version in Meeting Materials)	10/5/11	11/18/11
e.	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
f.	CAN-0011--PRC-005-1 R2: New Equipment	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
g.	CAN-0012--Completion of Periodic Activity Requirements During Implementation Plan	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
h.	CAN-0013--PRC-023 R1 and R2 Effective Dates for Switch-on-to-Fault Schemes	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
i.	CAN-0015--Unavailability of NERC Software Tools	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
j.	CAN-0022--VAR-002-1.1b R1 and R3 Generator Operation in Manual Mode	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11

k.	CAN-0024--CIP-002 R3 Routable Protocols and Data Diode Devices	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
l.	CAN-0026--TOP-006 R3 Protection Relays	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
m.	CAN-0028--TOP-006-1 R1.2 Reporting Responsibilities	CAN Comment Form to be Sent to cancomments@nerc.net	10/10/11	10/31/11
n.	Project 2008-10 - Interpretation of CIP-006-1 R1.1 by Progress Energy Draft Interpretation--Redline to Last Posting Form CIP-006-3C Announcement	Comment Form (Word version in Meeting Materials)	10/12/11	11/21/11
o.	Draft Directive Regarding Generator Transmission Leads Draft Directive Attachment 1--Examples of Typical Generation Transmission Tie Lines Attachment 2--Pro Forma Memorandum of Understanding (MOU) Appendix 1 to the MOU--Application Standards	Comments to be forwarded to NERC Staff: Jim Hughes, Jack Wiseman, Stacia Ann-Chambers	10/17/11	11/15/11
p.	CAN-0020--TPL-002, TPL-003, TPL-004 and TOP-002 Equipment Maintenance Outages Redline	CAN Comment Form to be Sent to cancomments@nerc.net	10/19/11	11/9/11
q.	CAN-0030--Attestations Redline	CAN Comment Form to be Sent to cancomments@nerc.net	10/19/11	11/9/11

a-beneath--CIP 706 Drafting Team Meeting Notes, September, 2011.
b-beneath--PRC-024 variance--Hydro-Quebec.
c-beneath--Protection and Control Subcommittee Joint Meetings--materials.
Discussion of SPS and related items.
d-beneath--FERC Technical Conference--CIP-006-2, Oct. 25, 2011.
e-beneath--CAN Comment Form--template.

Item 9a--Brian Evans-Mongeon reported that for the comment period that closed Oct. 10, 2011 NERC received over 1000 pages of comments for both of the documents that were posted. The responses to the comments rest with the Standard Drafting Team members. Anticipate that the responses will be made public the week of Oct. 31, 2011. An updated definitions document was sent out. The NERC BOT is scheduled to meet Nov. 3, 2011, and this will be on the agenda. There will be a recirculation ballot, and the NERC Board of Trustees will give guidance to the NERC Staff. David Ramkalawan remarked that black start facilities were mentioned in many of the comments submitted. Brian Evans-Mongeon said that black start facilities are essential to the restoration of the power system, thus making them needed for overall reliability. Everyone who submitted a comment will receive a response. David Ramkalawan observed that non-retail load was not addressed, but was mentioned in comments. Comments will be addressed globally. Greg Campoli commented that UFLS relays are not considered BES. Brian Evans-Mongeon responded that equipment that deals with non-BES facilities is not considered BES. In addition to UFLS relays, this includes UVLS relays. Chris de Graffenried questioned the single-line radial transmission design depicted on BES SDT Figure 7 as being atypical and perhaps even non-conforming with respect to the TPL's. (It would not survive an N-1 event and as such is a poor representation of a typical transmission radial.) The BES Definition of Radial Systems should allow both single-line and parallel-line radials to serve a distribution substation from a single BES source which provides both improved reliability and maintenance flexibility.

The Standard Drafting Team is not anticipating another meeting until the next phase. Compliance developed a straw man transition plan to provide guidance on how to conform to a new BES definition. Transition plans were discussed. Looking for draft transition plans from New York Transmission Operators.

Are the Canadians included? The feeling was that the Canadian entities were being ignored.

Guy Zito explained why he cast an affirmative vote during the last ballot. There were no "deal breakers" that would justify a "No" vote. The NPCC Board of Directors had discussed the BES definition. The NPCC was restricted to only voting on the definitions in Order 743. If the Standard Drafting Team had met that, the ballot would be "Yes". Guy Zito explained he had a responsibility to the NPCC Board of Directors and the NPCC Executive Management to vote appropriately. Sylvain Clermont commented that he was only considering voting "No", and not abstaining. Everyone except the NYISO and NPCC voted "No". Guy Zito did not disagree with the NPCC Board of Directors. He had sent out a letter with the issues, and got no responses. At the RSC Executive Committee Meeting Sept. 14, 2011 there were no deal breakers identified. Kathleen Goodman commented that on the one hand NPCC should be able to vote as an individual entity, and on the other it is important for the RSC's feelings to be made known.

The assembled were asked why they cast "No" votes. David Ramkalawan indicated that it is known that the process will be going to a Phase 2, and the feeling was that the industry was being pushed. Phase 2 should have been completed before a ballot was conducted. Guy Zito replied that because of a tight time constraint that would not have been possible. Sylvain Clermont commented that even though the comments submitted

were agreeable to the members, the members viewed them as not being favorable to casting a "Yes" ballot. Kathleen Goodman commented that she disagreed with the implemented concurrent balloting and commenting. She cannot vote when she doesn't know how submitted comments will be addressed. Sylvain Clermont suggested that Guy Zito speak with Ed Schwerdt about this. Guy Zito agreed to that. Guy Zito commented that it is important to understand how each one of the member's votes, and how the voting positions are developed. The vote needs to be coordinated. Lee Pedowicz sent out the Comment Form (due Oct. 27, 2011) with the draft responses for a final review before submission.

Kathleen Goodman, the IESO, Saurabh Saksena, and Michael Schiavone asked that their names not be included on the final submission to NERC.

Item 9b--there were no comments at the time of the Meeting.

Item 9c--there were no comments at the time of the Meeting.

Item 9d--waiting for comments from the ISO/RTO Council. Per Sylvain Clermont and David Kiguel, wind farms will be tapping in. David Kiguel is concerned about loads tapping in because of the regulating governance where the tap is made. Kathleen Goodman to send Lee Pedowicz comments by Nov. 10, 2011.

Item 9e--Greg Campoli sent comments.

Item 9f--CAN-0011 appears to go beyond what the requirement says. Mike Garton commented that the Standard refers to the BES, yet the CAN changed it to BPS. Why?

Item 9g--A discussion took place over the meaning of "annual". The CAN raised the question of how can compliance be retroactive? David Kiguel offered to come up with a comment for the RSC to consider. There is an attempt being made to state when a Standard becomes effective.

Item 9h--there were no comments at the time of the Meeting.

Item 9i--Pertains to NERC software tools. Bullet 2 on page 3 of 5 of the CAN suggests accomplishing the availability objective of the Standard, but not the requirement.

Item 9j--Both Ron Falsetti and Kathleen Goodman commented that the CAN had no apparent value. There were no comments from the RSC as a group. The question was asked if the CAN expanded the scope or changed the Standard, and the answer was no that it didn't. Michael Lombardi reported that Northeast Utilities will comment individually.

Item 9k--the comments submitted by TFIST were looked at. It was explained by Howard Gugel that a data diode takes available material, and converts it to one way serial data. It does involve routable protocol. It was agreed that the comments submitted by RSC would be those provided by TFIST.

Item 9l--the CAN, by the way it is written, says that the RC, etc. should communicate relay characteristics to operating personnel. Lee Pedowicz to generate comments to this CAN.

Item 9m--there were no comments at the time of the meeting.

Item 9n--TFIST to provide comments.

Item 9o--Kathleen Goodman to provide comments.

Item 9p--it was questioned whether or not this CAN is expanding a requirement. Randy MacDonald to review.

Item 9q-- were no comments at the time of the meeting.

Note: for CAN Items 9e through 9m, RSC members reviewed and were given the opportunity to send to Lee Pedowicz. Lee Pedowicz reviewed the comments and submitted to NERC Oct. 31, 2011.

Item 9b-beneath--Hydro-Quebec has a variance for PRC-006. PRC-024 should have the curve from PRC-006. Guy Zito commented that NERC Staff should be able to coordinate getting this done. Guy Zito gave it to Howard Gugel. Si-Truc Phan to send E-mail with the specific information to Howard Gugel. Howard Gugel commented that the change should be easy to implement because the Standard is in development.

10. Reference Documents Posted For Comment

a.				

11. Concluded Ballots (in Meeting Materials Package)

https://standards.nerc.net/Ballots.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)					Results of Ballot	RSC Recommend/Date
a.	Project 2010-11 - TPL Table 1, Footnote B	Recirculation Ballot	1/26/11	2/5/11	Quorum: 93.61% Approval: 86.54%	Yes 1/5/11
b.	Project 2007-07 - Vegetation Management - FAC-003	Successive Ballot and Non-Binding Poll	2/18/11	2/28/11	Quorum: 79.28% Approval: 79.34%	Yes 2/22/11
c.	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Initial Ballot	2/25/11	3/7/11	Quorum: 87.10% Approval: 49.54%	Yes 3/2/11

d.	Project 2007-23 - Violation Severity Levels	Non-binding Poll	2/9/11	2/18/11	Ballot Pool: 310 Opinions: 141 72% Support	Yes 10/28/10
e.	Project 2010-13 - Relay Loadability Order - PRC-023	Successive Ballot and Non-Binding Poll	1/24/11	2/13/11	Quorum: 83.95% Approval: 65.71%	Yes 2/11/11
f.	Project 2010-13 - Relay Loadability Order - PRC-023	Recirculation Ballot	2/24/11	3/6/11	Quorum: 87.35% Approval: 68.83%	Yes 2/11/11
g.	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Successive Ballot and Non-Binding Poll	4/19/11	4/28/11	Quorum: 79.66% Approval: 38.00%	No 4/19/11
h.	Project 2009-06 - Facility Ratings	Cast Ballot	4/21/11	5/2/11	Quorum: 86.01% Approval: 48.74%	Abstain 4/26/11
i.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Successive Ballot and Non-Binding Poll	5/3/11	5/12/11	Quorum: 78.33% Approval: 67.00%	No Recommendation
j.	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	Recirculation Ballot	5/12/11	5/23/11	Quorum: 91.25% Approval: 78.92%	Yes 5/12/11
k.	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Successive Ballot and Non-Binding Poll	5/18/11	5/31/11	Quorum: 92.07% Approval: 73.99	----
l.	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	Initial Ballot and Non-Binding Poll	5/31/11	6/9/11	Quorum: 88.47% Approval: 48.64%	Reject 5/31/11
m.	Project 2007-09 – Generator Verification – MOD-026-1 Ballot Results Revised because of NERC IT problem	Cast Ballot	7/22/11	8/1/11	Quorum: 90.25% Approval: 46.53%	No Consensus 7/28/11

n.	Project 2007-09 – Generator Verification – MOD-026-1	Cast Non-Binding Poll Opinion	7/22/11	8/1/11	Quorum: 88.75% Approval: 56.00%	----
o.	Project 2007-09 – Generator Verification – PRC-024-1 Ballot Results Revised because of NERC IT problem	Cast Ballot	7/22/11	8/1/11	Quorum: 90.82% Approval: 18.23%	No Consensus 7/28/11
p.	Project 2007-09 – Generator Verification – PRC-024-1	Cast Non-Binding Poll Opinion	7/22/11	8/1/11	Quorum: 88.35% Approval: 20.79%	----
q.	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Recirculation Ballot and Non-Binding Poll	6/20/11	6/30/11	Quorum: 82.97% Approval: 64.76%	Yes 6/28/11
r.	Project 2006-02 - Assess Transmission and Future Needs	Cast Ballot	7/13/11	7/22/11	Quorum: 94.33% Approval: 75.37%	----
s.	Project 2006-06 - Reliability Coordination - IRO-002-3	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 76.99%	Yes 7/22/11
t.	Project 2006-06 - Reliability Coordination - IRO-005-4	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 75.17%	Yes 7/22/11
u.	Project 2006-06 - Reliability Coordination - IRO-014-2	Cast Ballot	7/15/11	7/25/11	Quorum: 94.13% Approval: 76.27%	Yes 7/22/11
v.	Project 2006-06 - Reliability Coordination - IRO-002-3	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.37% Approval: 93%	----
w.	Project 2006-06 - Reliability Coordination - IRO-005-4	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.66% Approval: 93%	----
x.	Project 2006-06 - Reliability Coordination - IRO-014-2	Cast Non-Binding Poll Opinion	7/15/11	7/25/11	Quorum: 75.37% Approval: 89%	-----

y.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Initial Ballot	9/19/11	9/28/11 9/29/11--Technical Difficulties	Quorum: 84.86% Approval: 61.10%	Yes 9/21/11
z.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Non-Binding Poll VRFs and VSLs	9/19/11	9/28/11 9/29/11--Technical Difficulties	Quorum: 83.13% Approval: 68.68%	----
aa.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	Initial Ballot	9/30/11	10/10/11	Quorum: 92.97% Approval: 71.68%	No Consensus 10/3/11
bb.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Detailed Information to Support BES Exceptions Request	Initial Ballot	9/30/11	10/10/11	Quorum: 89.53% Approval: 64.03%	No Consensus 10/7/11
cc.	Project 2007-07 - Vegetation Management	Recirculation Ballot	10/4/11	10/13/11	Quorum: 87.17% Approval: 86.25%	Yes 2/22/11

12. <u>Posted For 30-Day Pre-Ballot Review (Open Ballot Pools) Between RSC Meetings</u>:

a.				

13. <u>Comment Forms Submitted</u> (in Meeting Materials Package), (red entries added since prior RSC Meeting)

a.	Standards Project Prioritization Reference Document and Tool	Comment Form	1/21/11	2/10/11
b.	Project 2007-12 - Frequency Response	Comment Form	2/4/11	3/7/11
c.	Project 2007-07 - Vegetation Management - FAC-003	Comment Form	1/27/11	2/28/11
d.	Project 2007-23 - Violation Severity Levels	Comment Form	1/20/11	2/18/11
e.	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Comment Form	1/18/11	3/7/11

f.	Regional Reliability Standards - PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding	Comment Form (no comments submitted)	1/10/11	2/24/11
g.	CAN-0015--Draft CAN-0015 Unavailability of NERC Tools	Comments	2/4/11	2/18/11
h.	CAN-0016--Draft CAN-0016 CIP-001-1 R1 - Applicability to Non-BES	Comments	2/4/11	2/18/11
i.	CAN-0017--Draft CAN-0017 CIP-007 R5 System Access and Password Controls	Comments	2/11/11	3/4/11
j.	CAN-0018--Draft CAN-0018 FAC-008 R.1.2.1 - Terminal Equipment	Comments	2/4/11	2/18/11
k.	Proposed Changes to Rules of Procedure to Add Section 1700 - Challenges to Determinations	Comments	2/14/11	3/7/11
l.	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	Comment Form	3/17/11	5/2/11
m.	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	Comment Form	3/29/11	4/28/11
n.	Project 2009-02 - Real-time Reliability Monitoring and Analysis Capabilities	Comment Form	2/16/11	4/4/11
o.	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments	Comments (No comments submitted)	3/1/11	4/15/11
p.	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Comments	3/1/11	4/15/11
q.	Project 2010-07 - Generator Requirements at the Transmission Interface	Informal Comment Period	3/4/11	4/4/11
r.	Project 2009-01 - Disturbance and Sabotage Reporting	Comment Form	3/9/11	4/8/11
s.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Comment Form	4/13/11	5/12/11
t.	Project 2010-17 - Definition of Bulk Electric System	Comment Form	4/28/11	5/27/11
u.	Project 2006-02 - Assess Transmission and Future Needs	Comment Form	4/18/11	5/31/11
v.	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	Comment Form	4/26/11	6/9/11
w.	Project 2010-17 - Definition of Bulk Electric System	Comment Form	5/11/11	6/10/11
x.	Rules of Procedure Development Team: BES Definition Exception Process	Comment Form	5/11/11	6/10/11
y.	CAN-0024--Draft CAN-0024 CIP-002 through	Comments	5/20/11	6/10/11

	CIP-009 Routable Protocols and Data Diodes			
z.	CAN-0029--Draft CAN-0029 PRC-004-1 R1, R2 and R3 Misoperations	Comments	5/20/11	6/10/11
aa.	CAN-0030--Draft CAN-0030 Attestations	Comments	5/20/11	6/10/11
bb.	CAN-0039--Draft CAN-0039 DOE Form 407	Comments	5/20/11	6/10/11
cc.	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)	Comment Form	6/10/11	7/11/11
dd.	Project 2007-09 – Generator Verification – MOD-025-2, MOD-027-1, PRC-019-1	Comment Form	6/15/11	7/15/11
ee.	Project 2007-09 – Generator Verification – MOD-026-1 and PRC-024-1	Comment Form	6/15/11	8/1/11
ff.	Project 2010-07 – Generator Requirements at the Transmission Interface – Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards	Comment Form	6/17/11	7/17/11
gg.	Proposed Changes to NERC Rules of Procedure and associated Appendices (Appendix 4B – Sanction Guidelines; and Appendix 4C – Compliance Monitoring and Enforcement Program)	Sent Comments to ROPcomments@nerc.net	6/30/11	8/15/11
hh.	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	Comment Form	8/15/11	9/29/11 (Extended from 9/28/11 because of NERC network problems)
ii.	Compliance Application Notice (CAN) Process	Comment Form	8/15/11	9/6/11
jj.	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	Comment Form	8/15/11	9/6/11
kk.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	Comment Form	8/26/11	10/10/11
ll.	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Detailed Information to Support BES Exception Request	Comment Form	8/26/11	10/10/11
mm.	Proposed Changes to NERC Rules of Procedure and All Appendices	Sent Comments to cancomments@nerc.net No Comments Submitted	9/2/11	10/17/11

nn.	NERC 2012-2014 Reliability Standards Development Plan	Comment Form	9/12/11	9/26/11
oo.	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004 (See note below table)	Sent Comments to cancomments@nerc.net	8/31/11	9/21/11
pp.	New CAN Template, five DRAFT CANs for Industry review, and CANs Status posted to NERC Compliance's Web site.	Sent Comments to cancomments@nerc.net	9/23/11	10/14/11

For Item 13oo--Draft letter from Jerry Mosier regarding CAN-0006. No comments for CAN-0006 had been received for CAN-0006 or submitted by RSC. Soliciting RSC input.

a-beneath--Project 2008-06 Cyber Security Order 706 – Draft Version 5 (CIP-002-CIP-011) Webinar August 24, 2011.

Item 13oo--Jerry Mosier called in. the Restoration Working Group reviewed CAN-0006: EOP-005-1 R7 Verification of Restoration. Comments were that this CAN introduced contradictions. Jerry Mosier discussed a letter that he authored detailing the Group's concerns. The letter was drafted because the Group was not able to submit its comments by the Sept. 21, 2011 deadline. Guy Zito suggested that the letter be signed by the Chair of CO-11 sign the letter. It was suggested that both the TFCO and CO-11 chairs sign the letter, but it was decided that just the CO-11 chair should sign it. Jerry Mosier wanted to insert introductory remarks and re-send to the RSC alter in the day for its review and input. A comment was made that the letter has to be closed with a suggestion, a statement indicating what is felt needs to be done. The letter should also say that table top exercises achieve the results desired in the Standard. Jerry Mosier revised the letter and re-sent it to the RSC. Guy Zito read the letter. It was discussed, and revised. CO-11 went beyond their authority. The letter was revised and sent back to Jerry Mosier.

14. Reference Documents Posted For Comment Between RSC Meetings

a.				

15. Drafting Team Nominations Open (Current and between RSC Meetings)

a.	Project 2007-17 - Protection System Maintenance and Testing Drafting Team	Nomination Period	9/1/11	9/23/11

16. NERC Meetings (in Meeting Materials Package)

a. Board of Trustees Meeting August 4, 2011.

1. Approved four Standards--Project 2006-02 Assess Transmission Future Needs and Develop Transmission Plans (TPL-001-2), and Project

2006-06 Reliability Coordination (IRO-002-3, IRO-005-4 and IRO-014-2)

b. Member Representatives Committee Meeting August 3, 2011.
   1. Nominations and Elections.
c. Compliance Committee Meeting August 3, 2011.
d. Planning Committee Meeting Sept. 13-14, 2011.
e. Standards and Compliance Workshop--Oct. 26-28, 2011.

Sylvain Clermont mentioned that the NERC MRC and Board of Trustees were scheduled to meet next week.

Guy Zito discussed the items on the Agenda that were for information.

17. NERC RSG (in Meeting Materials Package)

a. NERC Regional Reliability Standards Evaluation Procedure to be considered by the RSG.

A white paper has been generated to support this procedure.

18. Standards Committee Report (in Meeting Materials Package)

a. August 11, 2011 Meeting.
b. 2012-2013 Standards Committee elections. Nominations due Nov. 1, 2011.
c. October, 2011 Meeting.

The current Standards Development Process is overloading existing resources. The process needs to be changed to be able to effectively utilize industry resources.

19. SPCS Meeting (in Meeting Materials Package)

a.

20. NERC Compliance Application Notices (CANs) (in Meeting Materials Package--see sections 9 and 13 above)

a. Compliance Application Notices (CANs) and Bulletins (see Items 9 and 13).
b. General discussion (CO-11 request).
c. Updated CAN Status Spreadsheet.
d. Final dispositions of:
   1. CAN Process.
   2. CAN-0016: CIP-001 R1 Sabotage Reporting Procedure.
e. NERC Compliance Announcement Oct. 19, 2011.
   1. CIP Table Three Entities

21. NERC Bulk Electric System Definition (in Meeting Materials Package)

a. August 8-11, 18 meetings. Presentation to NERC Standards Committee August 18, 2011.

b. Bulk Electric System Definition Project - Fact Sheet, Fact Sheet with revisions.
c. NARUC Resolution on BES Definition.
d. Webinar--September 28, 2011.
e. Hydro-Quebec request for discussion of ballot decisions.
f. October 18-20, 2011 Definition of BES Drafting Team Meeting.
g. Updated Definitions of Terms Used in Standard.

22. NPCC Regional Standards, and More--Update (in Meeting Materials Package)

a. Disturbance Monitoring (PRC-002-NPCC-01)
   1. FERC approval October 20, 2011.
b. Underfrequency Load Shedding
   1. Authorization to Post CEAP and Pre Ballot for UFLS PRC -006-01.
c. Regional Reserve Sharing Groups
   1. Draft RSAR developed
   2. TFCO will be the Drafting Team. NPCC, and NERC soliciting for additional Drafting Team members.
d. NPCC Glossary of Terms--for RSC approval, retirement of Criteria A-7 NPCC Glossary of Terms.

Item 22b--RSC was reminded to encourage submission of response to the Cost Effectiveness Questions. Information is needed from the Generator Forum. A CEAP report is to be generated before PRC-006-NPCC-01 is posted for ballot.

Item 22c--Guy Zito stated that there is no NERC Standard to address the issues contained therein. The Regional Reserve Sharing Groups Regional Standard is intended to fill that gap. Guy Zito wants to have the Standard posted. The posting is not intended to be the go ahead for the Standard's development. It is intended to get industry input to assist in the determination of a future course of action. The Standard applies to Balancing Authorities. A directory is being developed in parallel with the Standard. It is hoped that the Standard will encourage the submission or more comments from industry. This was brought to the RSC for its approval for a 45 day posting for comments. Development of the Standard is also a goal of the NPCC Board of Directors (third Regional Standard). The TFCO also requested the development of this "fill in the blank" Standard. Ben Wu asked if NERC was heading towards eliminating Regional Standards. Howard Gugel responded that Regional Standards are needed for a Region to close Regional reliability gaps. Ron Falsetti commented that Ontario market rules were introduced to allow the IESO to participate. Mike Garton made a motion to approve the draft Standard for posting. Seconded by Brian Evans-Mongeon. With the exception of two abstentions, all others were in favor. Regional Reserve Sharing Groups will be posted for a 45 day comment period.

Item 22d--The NPCC Glossary is a tool that the Task Forces will use to check for discrepancies in "in use" definitions. The Glossary will contain all approved terms. The document has been posted for comments. RSC will have to approve. The Glossary will improve efficiency by not having to have the entire document approved when there is a change as had to be done with Criteria A-7. David Kiguel questioned how to ensure consistency in the use of terms. That will be resolved in the Directory approval process. If here is a change in the Glossary, will then have to go back to affected Directories? Under discussion is how to show defined terms in the Directories. If a definition is only in one document, it was suggested that the definition only be identified in that document, and not in the Glossary. Si-Truc Phan made a motion to approve the Glossary, seconded by Bruce Metruck. All were in favor.

Action Item--further discussion required regarding how to show a definition that may only be used in one document (see Action Item List).

23. NPCC Cost Effectiveness Analysis, Triage Process (in Meeting Materials Package)

a. Cost Effectiveness Analysis Procedure.
b. Triage process--discuss for posting.

Item 23a--Guy Zito discussed the intent, and the methods detailed in the CEAP. FERC, and NERC are interested in the development of this document. The NPCC Staff will generate reports from the data received. The comments that Michael Lombardi submitted were acknowledged. Si-Truc Phan commented that he was concerned that would use the CEAP as a vehicle for going against a Standard. The CEAP is not intended to be an analytical tool, just a means for organizing data. Tina Teng asked how an Entity can provide cost data in Phase 1 (Cost Benefit Analysis stage) when only a RSAR exists. Suggested not to ask about cost. It was felt that some entities might not be comfortable answering Question 3--"What approximate one-time and ongoing estimated potential costs would be associated with compliance with the proposed Standard?" It was reiterated that all submitted information will be held in strictest confidence. Guy Zito proposed approving the document as proposed considering comments that Maureen Long had sent in to use as a pilot. Sylvain Clermont made a motion to approve the CEAP, seconded by Greg Campoli. The CEAP will be used for Regional Standards. David Kiguel remarked that the NPCC Board of Directors' position is that cost must be taken into consideration when considering reliability. The CEAP will be piloted on the Underfrequency Load Shedding Regional Standard. All were in favor of approving the CEAP.

Item 23b--The Triage Process was brought up for approval. It was noted that it relies heavily on the RSC Executive Committee. Guy Zito reported that he hasn't received further comments. Michael Lombardi made a motion to approve the RSC Triage Process as written. Mike Garton seconded the motion. All were in favor.

24. NY adoption of more stringent/specific NPCC Criteria

a. The New York filing (as well as an update to the applicable NPCC Criteria in Nova Scotia that were approved by the Nova Scotia Utility and Review Board earlier this year), will be filed by the end of October, 2011.

No updated information was available for the meeting.

25. Directory and Regional Work Plan Status

a. Directory Development and Revision Manual--for RSC approval.

Directory Number	Title	Lead Group, Status	Current Activity
#1 (A-2)	Design and Operation of the Bulk Power System	Approved on 12/1/2009	TFCP has charged CP11 with a comprehensive review of Directory #1 to include the triennial document review, an examination of the NERC TPL standards, the existing NPCC planning criteria, and the implementation of Phase 2 of the Directory Project which will reformat existing Directory criteria into NERC style requirements. TFCO has assigned CO-8 to review the TO requirements within the Directory #1 criteria. TFCP/CP-11 is ready to post the document for its initial Open Process posting upon conclusion of the TFCO/CO-8 review. Open Process posting expected in mid December, 2011.
#2 (A-3)	Emergency Operation	Approved on 10/21/08.	Automatic UFLS language transferred to Directory #12. Next TFCO review Oct. 21, 2011.
#3 (A-4)	Maintenance Criteria for BPS Protection.	Approved on 7/11/08.	Phase 2 reformatting pending.
#4 (A-5)	Bulk Power System Protection Criteria	Approved on 12/1/09.	TFSP expects to begin Phase 2 review of Directory #4 in early 2012.
#5 (A-6)	Operating Reserve	TFCO	Directory#5 was approved by the Full Members on December 2, 2010. TFCO is working to resolve several open issues including how imports from HQ are wheeled within the Region. A TFCO special meeting is scheduled for Dec. 6, 2011 to finalize proposed revisions to Directory #5 in advance of an Open Process posting.
#6 New	Reserve Sharing	TFCO	TFCO has posted a draft of a new Directory#6 on Regional Reserve Sharing which would replace C-38 until a Regional Standard is developed. An Open Process posting for Directory #6 concluded on Oct. 24, 2011.
#7 (A-11)	Special Protection Systems	Approved on 12/27/07.	TFSP, TFSS, and TFCP are revising Directory #7. TFSP to incorporate current NRAP revisions (including Appendix A) of the document into a Phase 2 version and post for member comment after the November, 2011 TFSP Meeting.

#8 (A-12)	System Restoration	Approved on 10/21/08.	CO-11 has recently made revisions to the Directory #8 criteria. These revisions will be incorporated into the draft Phase 2 reformatting of Directory #8 which will be addressed by CO-8 early next year.
#9 (A-13)	Verification of Generator Real Power Capability	Approved on 12/22/08.	TFCO has posted the initial Phase 2 drafts of both Directories #9 and #10 to the Open Process. The initial open process concluded on June 14, 2011. TFCO reviewed comments and posted the revised Directories for a second posting which concluded on 10/24/2011. TFCO expects to present Directories #9 and #10 to the RCC in November, 2011, and anticipates a Full Member ballot of both Directories #9 and #10 in December, 2011.
#10(A14)	Verification of Generator Reactive Power Capability	Approved on 12/22/08.	Refer to Directory #9 preceding.
#12	UFLS Program Requirements	Approved on 6/26/09.	

Item 25a--Guy Zito, Gerry Dunbar, and Michael Lombardi worked on developing the Directory Development and Revision Manual. Gerry Dunbar reported that the Task Forces jurisdictional questions, and a need for rules. The RSC was to vote to approve the document, and then have it presented to the RCC for information. David Kiguel commented that NERC is flooded with requests for interpretations, and "Am I compliant?" questions. The process to verify a request for an interpretation is legitimate (refer to the Interpretation: Response to Request for an Interpretation of Directory XX for the XXXX Corporation) section of the Manual. This appears to be the intent of the Manual. Words should be added to the second paragraph of Section 5 to address David Kiguel's concerns. Greg Campoli suggested publishing a list containing informational data. The RSC would be responsible for this. A motion was made by Michael Lombardi to approve the Directory Development and Revision Manual contingent upon incorporating David Kiguel's suggestion, and develop a separate spreadsheet. It was seconded by Mike Garton. All were in favor.

Gerry Dunbar discussed the status of the Directories.

26. Review RFC, MRO Standards Relevant to NPCC (in Meeting Materials Package)

a. RFC Standards Under Development webpage
https://rsvp.rfirst.org/default.aspx

b. RFC Standard Voting Process (RSVP) webpage
ReliabilityFirst Corporation - Reliability Standards Voting Process

	Standard Under Development	Status	Start Date	End Date

1.	MOD-024-RFC-01.1 (Generator Verification - Real Power) Modified Violation Severity Levels (VSLs)	15 Days Prior to Category Ballot	8/10/11	8/24/11
2.	MOD-024-RFC-01.1 (Generator Verification - Real Power) Modified Violation Severity Levels (VSLs)	15 Day Category Ballot	8/25/11	9/8/11
3.	PRC-006-RFC-01 (Automatic Underfrequency Load Shedding)	Comment Period	9/28/11	10/27/11
	NERC Posting PRC-006-RFC-01	Comment Form	10/3/11	11/2/11

c. Midwest Reliability Organization Approved Standards
http://www.midwestreliability.org/STA_approved_mro_standards.html
(click on RSVP under the MRO header)

d. Midwest Reliability Organization Reliability Standard Voting Process webpage (table lists standards under development)
Midwest Reliability Organization - Reliability Standards Voting Process

	Standard Under Development	Status	Start Date	End Date
1.	PRC-006-MRO-01 - Underfrequency Load Shedding Requirements (see e. below)	Posted for second 30 day comment period	5/19/10	6/17/10
2.				

e. As of June 14, 2010 MRO suspended its regional standards development.

27. Report on NERC, NAESB and Regional Activities (in Meeting Materials Package)

a. Report on NERC, NAESB and Regional Activities
1. August, 2011.
2. September, 2011.

28. Task Force Assignments, et al. (in Meeting Materials Package)

a.

From the May 18-19, 2011 RSC Meeting--The Regions are discussing how to report misoperations. NPCC uses the CDAA. If there is no access to the CDAA then E-mail

can be used to report. An Action Item will be created to put questions together regarding misoperations.

Guy Zito raised the question of who should develop RSAWs. It was suggested that the Drafting Team do it, but they most likely are not familiar with compliance issues.

Ron Falsetti inquired about the criteria for categorizing events. Do Regions develop their own criteria? Ralph Rufrano said no, but Ron believed they did. Ron Falsetti and Ralph will discuss outside the meeting.

Additional information from Ben Eng (NPCC) (refer to the sample letter in the Meeting Materials)--

- The notes are correct in that misoperations are currently being emailed to me (and copied to Henry) for the short term. The long term goal is to modify CDAA so that the reminders and capture mechanism are automated.
- RSAWs already exist for PRC-004. The requirements are that analysis, corrective action plans and implementation must be done by the entity to prevent recurrence. The RSAW/Standard is not prescriptive in describing how, or to what degree, analysis should be done, and the correct actions to resolve the misoperation. Nor should it, since protective relaying is an "art"
- The criteria for the categories were established by the SPCS in the NERC Misoperation Reporting Template, and do not conflict with the NERC Glossary. A NERC webinar on Misoperation Reporting was conducted and an extensive list of Questions and Answers was developed into a document. The references and guidance for Misoperation Reporting are posted on NPCC's public website "Documents; Compliance; CDAA": https://www.npcc.org/Compliance/CDAA/Forms/Public%20List.aspx
- The process is in place to capture misoperation reports. Improvements to the process are planned.
- Initial notification for 3rd Quarter Misoperation Reports sent about 3 weeks prior to the due date.
- Follow up reminder sent the week before the due date
- The notification contained the link to the pertinent materials on the new NPCC Website
- SP-7 has been compiling and reviewing the misoperations and formalizing reports to NERC as scheduled.
- Ensuring that all reportable misoperations that happen in NPCC's footprint has been the biggest challenge.

29. Future Meetings and Other Issues (in Meeting Materials Package)

a. Filings and rulings regarding the NERC and NPCC applications for approval of Reliability Standards and Criteria in Nova Scotia.

b. FERC, NERC joint inquiry into Sept. 8, 2011 Southwest power outage.

1. Blackout news.

c. Balloting, voting process (WECC).

d. NERC Webinars.
   1. Critical Cyber Asset Identification: An Overview of a Process, Sept. 1, 2011.
   2. Project 2008-06 Cyber Security Order 706 – Draft Version 5 (CIP-002-CIP-011), August 24, 2011.
   3. FAC Recommendation Update, September 22, 2011.

e. NERC's New Enforcement Initiative.

f. NERC Webinars.
   1. Sept. 2, 2011 CANs Process
   2. Sept. 9, 2011 Registration and Certification JRO-CFR Webinar
   3. Sept. 15, 2011 Project 2007-17 Protection System Maintenance and Testing Webinar.

g. NERC News.
   1. August, 2011.
   2. September, 2011.

h. NERC Lessons Learned--August 10, 2011, October 20, 2011.
   1. Backup Control Center Operation and Training
   2. Special Protection Systems Maintenance Precautions
   3. Protection Relaying – Out of date prints
   4. Transmission Relaying – Voltage Transformer Failure
   5. Transmission Relaying – Removing Unused Components
   6. Plant Instrument and Sensing Equipment Freezing Due to Heat Trace and Insulation Failures
   7. Plant Fuel Switching and Cold Weather

i. FERC, NERC Report on Outages And Curtailments During the Southwest Cold Weather Event Of February 1-5, 2011.

j. Southwest Power Pool Compliance Update (contains standards information).

k. IESO Market Rules.

l. NERC standard prioritization.

m. Standards effective dates in Ontario.

n. NERC--ERO Best Practices.

o. NERC--Modifications to Mandatory Effective Dates Web page for US Reliability Standards.

p. SERC postings.
   1. The SERC Underfrequency Load Shedding (UFLS) Regional Standard (PRC-006-SERC-01) was posted for a 15-day review period.
   2. SERC Regional Standard Development Procedure.

q. FERC Open Meeting Schedule.

r. NERC--The Key Reliability Standard Spot Check (KRSSC) Program.

s. RSC Work Plan for 2012 -2013.

t. CIPC Meeting--September 14-15, 2011 Meeting--notes.

u. NERC--Report Assessing Risk to Reliability Performance of Bulk Power System.

v. NERC Event Analysis Process.

w. RSC Meeting schedule for 2012.
   1. NPCC Board of Directors proposed meeting dates.
   2. RCC Meeting dates.

x. NERC News.
   1. September, 2011.

y. SPP Compliance Update. Lists standards information.

z. RCC June 1, 2011 Meeting--Minutes.

aa. NERC--Electric Reliability Organization Compliance Analysis Report--Reliability Standard TOP-002 Normal Operations Planning, October, 2011.

bb. NERC Whitepaper on Regional Standards and Variances. Sent to RSG for their comments. Comments due October 28, 2011.

cc. The Reliability Standard Audit Worksheets (RSAW).

dd. New Brunswick Energy Blueprint.

ee. NERC 2012 Actively Monitored List of Reliability Standards and 2012 ERO CMEP Implementation Plan.

ff. WECC Newsletter--September/October 2011.

gg. Regional Reliability Standards Announcement
Comment Period Open for VAR-001-2 WECC Variance
October 20 – December 5, 2011.

hh. NERC--Conference Calls and Meeting Agendas.
   1. Standards Oversight and Technology Committee Meeting--Nov. 2, 2011.
   2. Compliance Committee Meeting--Nov. 2, 2011.
   3. Member Representatives Committee Meeting--Nov. 2, 2011.
   4. NERC Board of Trustees Meeting--Nov. 3, 2011.

Item 29s--The Work Plan 2012-2013 has been sent out several times to the RSC for comments. Guy Zito inquired if there were any additional revisions necessary. He wants to present it to the NPCC Board of Directors. The ninth bullet on page 1 was intended to mean RSC support. David Kiguel suggested that bullet 9 on page 1 be made to read "Monitor and coordinate NERC's CEO top reliability related issues and priorities". A motion was made by Michael Lombardi to approve the Work Plan. It was seconded by Sylvain Clermont. All voted in favor. The Work Plan 2012-2013 will now be presented to the NPCC Board of Directors.

Item 29w--Proposed RSC Meeting dates for 2012:

February 22-23, 2012--NPCC Offices
May 2-3, 2012--Dominion Offices
July 18-19, 2012--New England location
September 5-6, 2012--Montreal
October 17-18, 2012--Toronto
December, 2012 Meeting to coincide with the NPCC General Meeting

David Kiguel suggested that a Webex be used for future RSC Meetings. Guy Zito responded that it can be tried. It is preferable to have face to face meetings, and the option of a Webex should discourage in person attendance. It was agreed to have a Webex in Toronto.

RSC 2011 Meeting Dates

Dec. 1-2, 2011--Joint Meeting with the CC Dec. 2, 2011 Toronto, Ontario

2011 RSC Conference Call Schedule
(call 719-785-1707, Guest Code 8287#)

Nov. 10, 2011 (Thursday)
Dec. 16, 2011
Dec. 30, 2011

BOD 2011/2012 Meeting Dates

October 26, 2011 Teleconference
November 30, 2011 Toronto
January 31, 2012
February 1, 2012
March 13, 2012 (BES Special Teleconference)
May 1, 2012 (Teleconference)
June 26, 2012
August 7, 2012 (Teleconference)
September 19, 2012
October 30, 2012 (Teleconference)
November 28, 2012

RCC, CC, and Task Force Meeting Dates--2011/2012

RCC	Nov. 29, 2011
	2012-- March 1, June 6, Sept. 6, Nov. 27
CC	Nov. 16, Dec. 13-15
TFSS	
TFCP	Nov. 2
TFCO	
TFIST	
TFSP	Nov. 15-17

Respectfully Submitted,

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

Northeast Power Coordinating Council, Inc. (NPCC)

Antitrust Compliance Guidelines

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

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment. Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

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

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's Secretary, Andrianne S. Payson at 212-259-8218.

Action Item List

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
32 (To be deleted)	16b	To discuss with Herbert Schrayshuen how HQ, because of its unique operational requirements, will be addressed in standards development	Guy Zito--member of Standards Committee Process Subcommittee	RSC Meeting	Ongoing as of 2/10/10. Sylvain Clermont, and David Kiguel working with Guy Zito. Herbert Schrayshuen replaced Gerry Adamski at NERC. The new NERC management team will have to be made familiar with this item.
August 20-21, 2008					
Feb. 17-18, 2009					
June 17-18, 2009					
August 6-7, 2009					
60	3a	NPCC representatives from NERC drafting teams that have documents posted for comments report at RSC Meetings	Lee Pedowicz	RSC Meeting	Ongoing.
Sept. 24-25, 2009					

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
Nov. 4-5, 2009					
April 21-22, 2010					
63	----	Coordination with the Compliance Committee to develop Joint Activity Action List	Greg Campoli	RSC Meeting	Outgrowth of RSC/CC joint session April 21, 2010. Ongoing. Joint RSC/CC Meeting this meeting. Ralph Rufrano rejoined the RSC in the capacity of NPCC Compliance liaison. Comments not to be submitted on the CCEP.
June 29-30, 2010					
65	----	RSC to review the NPCC Members on NERC Drafting Teams list. Saurabh Saksena to maintain. Will get input from Carol Sedewitz.	RSC	RSC Meeting	Ongoing.
August 18-19, 2010					
66	----	Status of Memorandum of Understanding	Sylvain Clermont	RSC Meeting	Provide update. (MOU in Meeting Materials Package)

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
Nov. 30, 2010,					
Dec. 2, 2010					
69	----	Revise RSC Scope	Guy Zito	RSC Meeting	Approved at the August 3, 2011 RSC Meeting. To be presented to the NPCC Board of Directors.
Feb. 2-3, 2011					
71	----	Talk to Compliance about Regional Reliability Standard RSAWs. There should be a Compliance Committee representative on the Drafting Team.	Guy Zito	RSC Meeting	Ongoing.
73	----	Discuss consistency with the RSG.	Guy Zito	RSC Meeting	Ongoing.
March 16-17, 2011					
75	11f	Non-convergent contingencies enumerated in Project 2010-13 - Relay Loadability Order - PRC-023 Attachment B4a.	Guy Zito	RSC Meeting	To be discussed with Sal Buffamante.

Action Item Number	Agenda Item Number	Description	Owner	Due	Status
August 3-4, 2011					
76 (To be deleted)	18a	Handling of definitions	Guy Zito	RSC Meeting	To discuss with Pete Heidrich
October 26-27, 2011					
77	22d	If a term only defined in one document, should it be included in the NPCC Glossary?	Guy Zito/Gerry Dunbar	RSC Meeting	Ongoing.

Action Item 32--will be deleted. Hydro-Quebec has interconnection status.

Action Item 60--Lee Pedowicz contacted Brian Evans-Mongeon about discussing the progress of Project 2010-17 - Bulk Electric System.

Action Item 63--Guy Zito won't be at the December, 2011 Compliance Committee Workshop. It is important that Compliance Committee members are aware of what's going on with Standards. Gerry Dunbar and Lee Pedowicz will give a classroom session on Regional Standards. Guy Zito mentioned that it will be helpful to know what standards are coming, and what's on the prioritized list for standards development. David Kiguel discussed CIP versions 4 and 5. There will possibly be no version 4.

David Kiguel will put together an agenda for the joint RSC/CC Meeting Dec. 2, 2011. David Kiguel also reported that the Compliance staff is writing papers focusing on a new definition of BES.

Action Item 65--Saurabh Saksena checked with Carol Sedewitz regarding updates to the NPCC members on NERC Drafting Teams listing. There have been no changes over the past two months. Saurabh Saksena will look into the "holes" in the listing.

Action Item 66--ongoing.

Action Item 69--Guy Zito to present the RSC Scope to the NPCC Board of Directors.

Action Item 71--Topic for the December, 2011 RSC/CC Meeting.

Action Item 73--ongoing.

Action Item 75--nothing additional to report.
Action Item 76--a process is in place, approved by FERC. This item will be deleted.

Meeting adjourned at 16:30.
Meeting adjourned at 11:50.

NPCC Members on NERC Drafting Teams

Updated: July 27, 2010							
Project No.	**Project Title**	**DT Type**	**NPCC Representatives**	**Company**	**Telephone**	**E-mail Address**	**Comments**
2006-02	Assess Transmission Future Needs & Develop Transmission Plans	Standard	Dana Walters	National Grid	781-907-2501	dana.walters@us.ngrid.com	
2006-02	Assess Transmission Future Needs & Develop Transmission Plans	Standard	Yury Tsimberg	Kinectrics	416-207-6000 X6106	Yury.Tsimberg@Kinectrics.com	Observer
2006-03	System Restoration & Blackstart	Standard	Steve Cooper	IESO	905-855-6159	steve.cooper@ieso.ca	
2006-03	System Restoration & Blackstart	Standard	David Mahlmann	NYISO	518-356-6101	dmahlmann@nyiso.com	
2006-03	System Restoration & Blackstart	Standard	Will Houston	National Grid	508-421-7690	will.houston@us.ngrid.com	
2006-04	Backup Facilities	Standard	John Procyk	Hydro One Networks	705-792-3210	john.procyk@hydroone.com	
2006-04	Backup Facilities	Standard	Mike Schiavone	National Grid	315-460-2472	michael.schiavone@us.ngrid.com	Vice-Chair
2006-06	Reliability Coordination	Standard	Earl Barber	National Grid	315-428-5532	earl.barber@us.ngrid.com	
2006-07	ATC/TTC/AFC & CBM/TRM Revisions	Standard	Cheryl Mendrala	ISO-NE	413-535-4184	cmendrala@iso-ne.com	
2006-08	Transmission Loading Relief	Standard	Ben Li	Ben Li Associates, Inc.	647-388-1498	Ben@BenLi.ca	Chair
2007-01	Underfrequency Load Shedding	Standard	Brian Evans-Mongeon	Utility Services	802-552-4022	brian.evans-mongeon@utilitysvcs.com	
2007-01	Underfrequency Load Shedding	Standard	Si Truc Phan	Hydro Quebec - TransEnergie	514-879-4100 X3610	Phan.Si_Truc@hydro.qc.ca	
2007-02	Operating Personnel Communications Protocols	Standard	Tom Irvine	Hydro One Networks	705-792-3004	tom.irvine@hydroone.com	
2007-03	Real-time Operations	Standard	Phil Lavallee	National Grid	508-389-2827	phil.lavallee@us.ngrid.com	
2007-04	Certifying System Operators	Standard	Rob MacDonald	Hydro One Networks	705-792-3095	Rob.Macdonald@HydroOne.com	
2007-05	Balancing Authority Controls	Standard	Guy Quintin	Hydro Quebec - TransEnergie	514-289-2211 X3150	Quintin.Guy@hydro.qc.ca	
2007-06	System Protection Coordination	Standard	Aaron Cooperberg	Hydro One Networks	416-345-5172	cooperberg@HydroOne.com	
2007-06	System Protection Coordination	Standard	David Cirka	National Grid	781-907-3240	david.cirka@us.ngrid.com	
2007-07	Vegetation Management	Standard	Dave Morrell	New York State Dept of Public Svc	518-486-7322	david_morrell@dps.state.ny.us	
2007-07	Vegetation Management	Standard	Orville Cocking	Con Edison			
2007-09	Generator Verification	Standard	Les Hajagos	Kestrel Power Engineering Ltd.	905-272-2191	les@kestrelpower.com	
2007-11	Disturbance Monitoring	Standard	Jeff Pond	National Grid	781-907-3222	jeff.pond@us.ngrid.com	
2007-12	Frequency Response	Standard	Harvey Happ	New York State Dept of Public Svc	518-486-2939	hhh@dps.state.ny.us	
2007-12	Frequency Response	Standard	Mike Potishnak	ISO-NE	413-535-4308	mpotishnak@iso-ne.com	
2007-14	Permanent Change to CI Table	Standard	No representation				
~~2007-17~~	~~Protection System Maintenance & Testing~~	~~Standard~~	~~John Ciufo~~	~~Hydro One Networks~~	~~416-345-5258~~	~~john.ciufo@hydroone.com~~	
~~2007-17~~	~~Protection System Maintenance & Testing~~	~~Standard~~	~~Leonard Swanson~~	~~National Grid~~	~~315-428-5250~~	~~leonard.swanson@us.ngrid.com~~	
2007-18	Reliability-based Control	Standard	Mike Potishnak	ISO-NE	413-535-4308	mpotishnak@iso-ne.com	
2007-23	Replace Levels of Noncompliance w/VSL	Standards	No representation				
2008-01	Reactive Planning and Control	SAR	Edwin E Thompson,	Con Edison	212-460-8199	thompsonedwin@coned.com	
2008-04	Facility Ratings for Order 705	Standard	No representation				
2008-06	Cyber Security for Order 706	Standard	John Lim	Con Edison	212-460-2712	limj@coned.com	Chair
2008-06	Cyber Security for Order 706	Standard	Frank Kim	Hydro One Networks	705-792-3033	Frank.Kim@HydroOne.com	
2008-06	Cyber Security for Order 706	Standard	Doug Johnson	Exelon-Commonwealth Edison	630-691-4593	douglas.johnson@comed.com	
2008-06	Cyber Security for Order 706	Standard	Robert Antonishen	Ontario Power Generation	905-262-2674	rob.antonishen@opg.com	
2008-06	Cyber Security for Order 706	Standard	Thomas Stevenson	Constellation Energy			
2008-08	Revise VSLs for Emergency Operations Standards	Standard	No Representation				
2008-12	Coordinate Interchange Modifications	Standard	Cheryl Mendrala	ISO-NE	413-535-4184	cmendrala@iso-ne.com	
2008-14	Cyber Security Violation Severity Levels	Standard	Mark Engels	Dominion	804-775-5263	mark.engels@dom.com	
2008-14	Cyber Security Violation Severity Levels	Standard	David Dunn	IESO	905-855-6286	david.dunn@ieso.ca	

NPCC Members on NERC Drafting Teams

Updated: July 27, 2010							
2009-01	Disturbance and Sabotage Reporting	Standard	Brian Evans-Mongeon	Utility Services	802-552-4022	brian.evans-mongeon@utilitysvcs.com	Vice-Chair
2009-01	Disturbance and Sabotage Reporting	Standard	Michelle Draxton	Constellation Energy Group	410-474-2993	Michelle.I.draxton@constellation.com	
2009-01	Disturbance and Sabotage Reporting	Standard	Drew Phillips	IESO	905-855-4114	drew.phillips@ieso.ca	
2009-01	Disturbance and Sabotage Reporting	Standard	Thomas J Curran	Con Edison	347-672-4621	currant@coned.com	
2009-02	Real-time Best Tools	SAR	Scott Vidler	Hydro One Networks	705-627-1436	scott.vidler@hydroone.com	
2009-07	Reliability of Protection Systems	SAR	Xiaodong Sun	Ontario Power Generation	289-257-0405	xiaodong.sun@opg.com	
2009-07	Reliability of Protection Systems	SAR	Dean V. Sorensen	National Grid	508-389-2301	Dean.Sorensen@us.ngrid.com	
2009-07	Reliability of Protection Systems	SAR	Stanley J. Lewis	Con Edison	212-780-2845	lewiss@coned.com	
2009-05	Resource Adequacy Assessments	Standard	Curt Dahl	National Grid	516-545-3662	cdahl@keyspanenergy.com	
2009-05	Resource Adequacy Assessments	Standard	Greg Drake	NYISO	518-356-6038	gdrake@nyiso.com	
2009-05	Resource Adequacy Assessments	Standard	Phil Fedora	NPCC	212-840-4909	pfedora@npcc.org	Vice-Chair
2010-05	Protection Systems: Phase 1 (Misoperations)	Standard	Paul Difilippo	Hydro One	647-328-7068	paul.difilippo@hydroone.com	
2010-07	Generator Requirements at the Transmission Interface	SAR	Benjamin Church	FPL Group - NextEra Energy	561-304-5463	benjamin.church@fpl.com	
2010-10	FAC Order 729	Standard	No representation				
2010-17	Proposed Definition of Bulk Electric System	Standard	Jennifer Dering	NYPA		Jennfer.Dering@nypa.gov	
			Brian Evans-Mongeon	Utility Services	802-552-4022	brian.evans-mongeon@utilitysvcs.com	
			Phil Fedora	NPCC	212-840-4909	pfedora@npcc.org	
			Ajay Garg	Hydro One Networks	416.345.5420	ajay.garg@HydroOne.com	
IRO-004	Require Timely Submission of Data	SAR	No representation				
NUC-001-1	Nuclear Plant Interface Coordination for FERC Order 716	SAR	Michael Schiavone	National Grid	315-460-2472	Michael.Schiavone@us.ngrid.com	
RRSWG	Regional Reliability Standards Working Group	N/A	Guy Zito	NPCC	212-840-1070	gzito@npcc.org	
FMWG	Functional Model Working Group	N/A	Mike Yealland	IESO			
FMWG	Functional Model Working Group	N/A	Ben Li	Ben Li Associates, Inc.	647-388-1498	Ben@BenLi.ca	
FMWG	Functional Model Working Group	N/A	Guy Zito	NPCC	212-840-1070	gzito@npcc.org	
FMWG	Functional Model Working Group	N/A	John Walewski	Hydro One Networks	416-345-5878	John.Walewski@HydroOne.com	
FMWG	Functional Model Working Group	N/A	Michael Gildea	Dominion	804-273-4624	michael.gildea@dom.com	
FMWG	Functional Model Working Group	N/A	Peter Munn	Air Liquide LI USA	713-438-6420	peter.munn@airliquide.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Phil Davis	Schneider Electric	404-567-6090	phil.davis@us.schneider-electric.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Stephen C. Knapp	Constellation	410-470-3374	steve.knapp@constellation.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Donna Pratt	NYISO	518-356-8758	dpratt@nyiso.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Ken Clark	Consert, Inc	919-244-7655	kclark@consert.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Aaron Breidenbaugh	EnerNOC	617-224-9918	abreidenbaugh@enernoc.com	
FM DRAT	Functional Model Demand Response Advisory Team	N/A	Eric Winkler	ISO-NE	413-540-4513	ewinkler@iso-ne.com	

From:	Guy V. Zito
To:	gerkemt@nu.com
Cc:	weghgp@nu.com; mckinmb@nu.com; Lee R. Pedowicz
Subject:	RE: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing
Date:	Thursday, November 10, 2011 6:32:47 PM

Mike,

Timing was against us today. At the SC teleconference today, the appointment was not approved. However, they are encouraging you to attend as an observer. The Chair of the drafting team indicated he would seek your appointment in a "couple of months" if you were beneficial to the team. I hope you will consider attending as an observer until such time as you can be formally appointed. Let me know if NU would allow you to participate as an observer, temporarily. The main issue for denial at this time is that there are supposedly about 24 people on the team which is probably one of the largest teams NERC ever formed and they are very relunctant to add more to this unweildy amount of people, usually there are a dozen or less.

Keep me informed. If you aren't able to participate please let me know and I may need to provide one of my staff to "observe" and monitor the team.

Thanks very much,

Guy V. Zito
Assistant Vice President-Standards
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10 th Floor
New York, NY 10018
212-840-1070
212-302-2782 fax

From: gerkemt@nu.com [gerkemt@nu.com]
Sent: Wednesday, November 09, 2011 2:00 PM
To: Guy V. Zito
Cc: weghgp@nu.com; Guy V. Zito; mckinmb@nu.com
Subject: RE: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

Guy,

Here is my nomination form.

Mike Gerken
Manager Transmission
Test & Tech Support
3333 Berlin Turnpike
Newington, CT 06111
Cell: 860-883-1330
Phone: 860-665-5842

This e-mail, including any files or attachments transmitted with it, contains information which may be confidential, proprietary, privileged or otherwise protected from disclosure. The information is intended for a specific purpose and for use only by the individual or entity to whom it is addressed. If you are not the intended recipient, please notify the sender immediately and delete it from your system. Any review, disclosure, copying, distribution or use of this e-mail or the taking of any action based on its contents, other than for its intended purpose, is strictly

prohibited. Any views or opinions expressed in this e-mail are not necessarily those of Northeast Utilities, its subsidiaries and affiliates (NU). E-mail transmission cannot be guaranteed to be error-free or secure or free from viruses, and NU disclaims all liability for any resulting damage, errors, or omissions.

From: "Guy V. Zito" <gzito@npcc.org>

To: "Guy V. Zito" <gzito@npcc.org>, George P. Wegh/NUS@NU
Cc: Michael T. Gerken/NUS@NU, Michael B. McKinnon/NUS@NU, "carol.sedewitz@us.ngrid.com" <carol.sedewitz@us.ngrid.com>

Date: 11/08/2011 07:58 PM

Subject: RE: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

---

George,

Is Mike able to help us out on this? If so please send us the Self nomination form I emailed previously to you folks.

Thanks,

Guy V. Zito
Assistant Vice President-Standards
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10 th Floor
New York, NY 10018
212-840-1070
212-302-2782 fax

From: Guy V. Zito
Sent: Friday, November 04, 2011 9:35 AM
To: weghgp@nu.com
Cc: gerkemt@nu.com; mckinmb@nu.com; carol.sedewitz@us.ngrid.com
Subject: RE: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

George,

Yes he would be a good candidate. He doesn’t need to be serving NPCC on any TF or Comm. Please fill out the attached form ASAP and return to me. I will work with our SC rep and NERC staff to see if he can be added to the slate of candidates.

Thanks,

Guy V. Zito
Asst. Vice President-Standards
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018
212-840-1070
212-302-2782 fax

From: weghgp@nu.com [mailto:weghgp@nu.com]

Sent: Friday, November 04, 2011 9:12 AM

To: Guy V. Zito

Cc: rsc; tfsp; gerkemt@nu.com; mckinmb@nu.com

Subject: Re: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

Hi Guy:

Mike Gerken, our Manager of Transmission Test and Maintenance is interested in serving on this SDT. He presently does not serve on any NPCC task force or committee so I'm not sure if that is a prerequisite that would prevent him from serving. Would he be a viable candidate?

Thanks,

George Wegh, P.E.

Manager

Transmission Protection and Control Engineering

Northeast Utilities

P. O. Box 270

Hartford, CT 06141

Mail Stop: NUE2

Phone: 860-665-2967

Email: weghgp@nu.com<mailto:weghgp@nu.com>

From: "Guy V. Zito" <gzito@npcc.org<mailto:gzito@npcc.org>>

To: tfsp <tfsp@npcc.org<mailto:tfsp@npcc.org>>

Cc: rsc <rsc@npcc.org<mailto:rsc@npcc.org>>

Date: 11/03/2011 09:11 PM

Subject: FW: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

---

TFSP Members,

Seems we are lacking NPCC representation on the subject drafting team slate of candidates. We are attempting to solicit an opening and would like TFSP to solicit their members for any interest. Please let me know as soon as possible if anyone has interest and is able to participate on behalf of the Region.

Thanks,

Guy V. Zito

Assistant Vice President-Standards

Northeast Power Coordinating Council, Inc.

1040 Avenue of the Americas, 10 th Floor

New York, NY 10018

212-840-1070

212-302-2782 fax

From: Sedewitz, Carol A. [CAROL.SEDEWITZ@us.ngrid.com]

Sent: Thursday, November 03, 2011 4:36 PM

To: Guy V. Zito

Cc: saurabh.saksena@us.ngrid.com<mailto:saurabh.saksena@us.ngrid.com>;
Michael.Schiavone@us.ngrid.com<mailto:Michael.Schiavone@us.ngrid.com>;
leonard.swanson@us.ngrid.com<mailto:leonard.swanson@us.ngrid.com>

Subject: SDT candidates for Project 2007-17 Protection System Maintenance and Testing

Hi Guy,

I received today the proposed agenda and the confidential information for the drafting teams that are up for discussion on the SC meeting next week.

I noticed that on the "Project 2007-17 Protection System Maintenance and Testing Standard Drafting Team Candidates" there are none from NPCC. In the past John Ciufo(Hyrdo One) and Len Swanson(National Grid) had participated on the team.

I'm pretty sure that Len Swanson does not have the availability to continue with the team (I have reached out to confirm).

It may be too late since no one nominated themselves from NPCC, but I am happy to bring up at the SC meeting that we should reach out and get a member from NPCC to participate and we would like an opportunity to do that.

Let me know if you are comfortable with that approach and if you might be able to reach out to TFSP members to see if there might be someone interested in participating on this SDT from our region.

Thanks,

Carol

****

This e-mail and any files transmitted with it, are confidential to National Grid and are intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error, please reply to this message and let the sender know.

This email and any of its attachments may contain information that is privileged, confidential, classified as CEII, or subject to copyright belonging to NPCC. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout.

********** This e-mail, including any files or attachments transmitted with it, is confidential and/or proprietary and is intended for a specific purpose and for use only by the individual or entity to whom it is addressed. Any disclosure, copying or distribution of this e-mail or the taking of any action based on its contents, other than for its intended purpose, is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately and delete it from your system. Any views or opinions expressed in this e-mail are not necessarily those of Northeast Utilities, its subsidiaries and affiliates (NU). E-mail transmission cannot be guaranteed to be error-free or secure or free from viruses, and NU disclaims all liability for any resulting damage, errors, or omissions. **********

This email and any of its attachments may contain information that is privileged, confidential, classified as CEII, or subject to copyright belonging to NPCC. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout.

Revised: 11/18/2011

Tab Name	Last Revised	Summary of Changes
NERC RS Exec Tracking Summary	11/18/2011	- Project 2009-06, Facility Ratings -- FERC Approved - Project 2010-10, FAC Order 729 -- FERC Approved - Project 2007-07, Vegetation Management -- NERC BOT Approved
NERC CANs	11/16/2011	- Nine revised CANs approved and posted - Two new CANs posted for comment
NPCC RRS Tracking Summary	11/8/2011	- PRC-006-NPCC-01 Automatic UFLS Program -- Posted for ballot - BAL-002-NPCC-01 Regional Reserve Sharing -- Posted for Comment
NPCC Doc Tracking Summary	10/28/2011	- A-07 Glossary of Terms -- Anottated A-07 will be retired pending approval of Glossary
NPCC Directory Tracking Summary	10/28/2011	- Updated comment section for numerous Directories

NERC Reliability Standards Executive Tracking Summary

Revised: 11/18/2011

Line No.	Project No. / Title	High Priority?	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
1	Project 2009-06 — Facility Ratings	Normal	FAC-008-3 (was FAC-008-2)	Yes 2nd (Thru 9/9/09)	Yes 3rd (Formal Thru 5/2/11)	Yes 6th (Recirculation Thru 5/23/11)	Yes (5/23/11)	Yes (5/24/11)	Yes (6/15/11)	Yes (11/17/11)	FAC-008-3 is effective the first day of the first calendar quarter that is twelve months after issuance of the FERC Order. FAC-008-3 combines FAC-008-1 and FAC-009-1 into a single standard.	Completed
2	Project 2009-17 — Interpretation of PRC-004-1 and PRC-005-1 R2 by Y-W Electric and Tri-State G & T	No	PRC-004-1 and PRC-005-1	x	x	Yes 3rd (Recirc Thru 12/3/10)	Yes (12/3/10)	Yes (2/17/11)	Yes (4/15/11)	Yes (9/26/11)		Completed
3	Project 2009-27 — Interpretation of TOP-002-2a R10 by FMPP	No	TOP-002-2a, R10	x	x	Yes (Recirc Thru 10/16/10)	Yes (10/16/10)	Yes (11/4/10)	Yes (4/15/11)	Yes (10/20/11)		Completed
4	Project 2010-10 — FAC Order 729	No	FAC-013-2	Yes 1st (Thru 4/29/10)	Yes 3rd (Thru 1/8/11)	Yes 3rd (Recirc Thru 1/23/11)	Yes (1/23/11)	Yes (1/24/11)	Yes (1/28/11)	Yes (11/17/11)	FAC-013-2 is effective the first day of the calendar quarter twelve months after Commission approval.	Completed
5	Project 2006-02 — Assess Transmission and Future Needs	High	TPL-001-2	Yes 3rd (Thru 3/16/07)	Yes 5th (Formal Thru 5/31/11)	Yes (Recirculation Thru 7/22/11)	Yes (7/22/11)	Yes (8/4/11)	Yes (10/19/11)			Under Development
6	Project 2007-01 — Underfrequency Load Shedding	No	EOP-003-1 and PRC-006-1	Yes 3rd (Thru 3/29/07)	Yes 3rd (Thru 7/16/10)	Yes 6th (Recirc Thru 10/28/10)	Yes (10/28/10)	Yes (11/4/10)	Yes (3/31/11)		NOPR Issued 10/20/11. NOPR proposes to approve Reliability Standards PRC-006-1 (Automatic Underfrequency Load Shedding) and EOP-003-2 (Load Shedding Plans) submitted by NERC. Comments are due 60 days after publication in the Federal Register.	Pending Regulatory Approval
7	Project 2008-06 — Cyber Security — Order 706 (CIP-002-4)	High	CIP-002-4 thru CIP-009-4	x	Yes 1st (Thru 11/3/10)	Yes Recirc Thru 12/30/10) - passed	Yes (12/30/10)	Yes (1/24/11)	Yes (2/10/11)		- FERC NOPR issued 9/15/11 - NOPR would require NERC to make a filing to fully comply with Order No. 706 by the end of the third quarter of 2012. Comments on the proposed rule (RM11-11) are due 60 days after publication in the Federal Register. - Posted in Federal Register on 9/21/11 - Comments are due 11/21/11	Pending Regulatory Approval
8	Project 2008-09 — Interpretation of EOP-001-0 R1 by Regional Entity Compliance Managers	No	EOP-001-0, R1	x	x	Yes 4th (Recirc Thru 10/14/10)	Yes (10/14/10)	Yes (11/4/10)	Yes (9/9/11)			Pending Regulatory Filing
9	Project 2008-14 — Cyber Security Violation Severity Levels	No	CIP family of standards	Yes 2nd (Thru 04/20/09)	Yes 1st (Thru 04/20/09)	Yes (Recirc Thru 7/16/09)	Yes (7/16/09)	Date?	Date?			Pending Regulatory Approval
10	Project 2009-10 — Interpretation of PRC-005-1 R1 by Compliance Monitoring Processes Working Group (CMPWG)	No	PRC-005-1, R1	x	x	Yes (Recirc Thru 8/6/09)	Yes (8/6/09)	Yes (11/5/09)	Yes (11/17/09)		NOPR issued 12/16/10 - Comments are due 2/25/11	Pending Regulatory Approval
11	Project 2009-28 — Interpretation of EOP-001-1 and EOP-001-2 R2.2 by FMPP	No	EOP-001-1 and EOP-001-2	x	x	Yes (Recirc Thru 10/15/10)	Yes (10/15/10)	Yes (11/4/10)	Yes (9/9/11)			Pending Regulatory Filing
12	Project 2010-11 — TPL Table 1 Order	No	TPL-002 Footnote b	Yes 1st (Thru 5/26/10)	Yes 3rd (Thru 1/5/11)	Yes 3rd (Recirc Thru 2/5/11)	Yes (2/5/11)	Yes (2/17/11)	Yes (3/31/11)		- FERC NOPR issued 10/20/11. This Notice of Proposed Rulemaking (NOPR) proposes to remand to NERC its proposed modification to Reliability Standard TPL-002, Table 1, footnote 'b' because it does not adequately clarify or define the circumstances in which an entity can plan to shed firm load for a single contingency. Comments are due 60 days after publication in the Federal Register. - Ref: FERC 3/18/10 Order Setting Deadline for Compliance [Docket RM06-16-009] -- NERC to clarify Std TPL 002-0	Pending Regulatory Approval
13	Project 2010-13 — Relay Loadability Order	Normal	PRC-023-2	Yes 1st (Thru 9/19/10)	Yes 3rd (Thru 12/16/10)	Yes 3rd (Recirculation Thru 3/6/11)	Yes (3/6/11)	Yes (3/10/11)	Yes (3/18/11)		- FERC NOPR issued 9/15/11 - NOPR proposes to approve Reliability Standard PRC-023-2 (Transmission Relay Loadability). The proposed Reliability Standard modifies an existing standard addressing setting protective relays to ensure they reliably detect and protect the electric network from fault conditions but do not limit transmission loadability or interfere with system operators' ability to protect system reliability. - Posted in Federal Register on 9/21/11 - Comments are due 11/21/11	Pending Regulatory Approval
14	Urgent Action SAR for Revision	No	BAL-004-1	Yes 2nd (Thru 10/18/07)	Yes 2nd (Thru 10/18/07)	Yes 1st (Recirc Thru 12/4/07)	Yes (12/4/07)	Yes (3/26/08)	Yes (3/11/09)		- NERC Motion to Further Defer Action Issued 8/11/11 - NERC Motion to Defer Action Issued 8/20/10 - FERC NOPR [Docket RM09-13-000 (March 18, 2010)] - Commission proposes to remand BAL-004-1	Pending Regulatory Approval
15	Project 2006-06 — Reliability Coordination	Normal	COM-001-2, COM-002-3, IRO-001-2 and IRO-014-2 (possibly IRO-003-2 - see comments)	Yes 3rd "Supp" (Thru 9/3/10)	Yes 4th (Thru 3/7/11)	Yes 2nd (Initial Thru 7/25/11)	IRO-002-3 IRO-005-4 IRO-014-2 Yes (7/25/11)	Yes (8/4/11)			DT to address comments on Supplemental SAR. SAR proposes to expand the scope of work under to address some directives from Order 693 that are associated with IRO-003-2	Under Development
16	Project 2007-07 — Vegetation Management	Normal	FAC-003-2	Yes 3rd (Thru 7/17/07)	Yes 5th (Thru 2/28/11)	Yes 6th (Recirculation Thru 10/13/11)	Yes (10/13/11)	Yes (11/3/11)				Under Development
17	Project 2010-09 — Cyber Security Order 706B — Nuclear Plant Implementation Plan	No	Various CIP Standards	Yes 1st (Thru 3/15/10)	Yes 1st (Thru 3/15/10)	Yes (Recirc Thru 7/2/10)	Yes (7/2/10)	Yes (8/5/10)				Pending Regulatory Filing
18	Project 2009-20 — Interpretation of BAL-003-0 R2 and R5 by Energy Mark, Inc.	No	BAL-003-0.1b	x	x	Yes (Recirc Thru 2/26/10)	Yes (2/26/10)					Under Development
19	Project 2007-03 — Real-time Operations	High	TOP-001-2, TOP-002-3 and TOP-003-2	Yes 2nd (Thru 9/07/07)	Yes 5th (Formal Thru 6/9/11)	Yes 1st (Intitial Thru 6/9/11)						Under Development
20	Project 2007-09 — Generator Verification	High	MOD-026-1 and PRC-024-1* MOD-024-2** MOD-025-2, MOD-027-1, PRC-019-1***	Yes 1st (Thru 5/21/07)	*Yes 2nd (Thru 8/1/11) **Yes 1st (Thru 2/18/10) ***Yes 1st (Thru 7/15/11)	*Yes 1st (Thru 8/1/11)						Under Development
21	Project 2007-12 — Frequency Response	High	BAL-003-1	Yes 3rd (Thru 3/09/07)	Yes 2nd (45 Day Formal Thru 12/8/11)	Yes 1st (Initial Thru 12/8/11)						Under Development
22	Project 2007-17 — Protection System Maintenance & Testing RE-INITIATED	High	PRC-005-2	Yes 1st (Thru 9/28/11)	Yes 1st (Thru 9/28/11)	Yes 1st (Initial Thru 9/28/11)						Under Development

NERC Reliability Standards Executive Tracking Summary

Revised: 11/18/2011

Line No.	Project No. / Title	High Priority?	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
23	Project 2008-10 — Interpretation of CIP-006-1 R1.1 by Progress Energy	No	CIP-006, R1.1	x	x	Yes 2nd (Initial Thru 10/12/09)					Since at least one negative ballot included a comment, the results are not final. A second (or recirculation) ballot must be conducted.	Under Development
24	Project 2009-01 — Disturbance and Sabotage Reporting	High	EOP-004-2	Yes 1st (Thru 5/21/09)	Yes 3rd (45 Day Formal Thru 12/12/11)	Yes 1st (Initial Thru 12/12/11)						Under Development
25	Project 2009-22 — Interpretation of COM-002-2 R2 by the IRC	High - Interp.	COM-002-2	x	2nd (45 day Formal thru 11/17/11)	Yes 1st (Intitial Thru 11/17/11)						Under Development
26	Project 2009-24 — Interpretation of EOP-005-1 R7 by FMPA	No	EOP-005-1, R7	x	x	Yes 1st (Intitial Thru 1/15/10)					Balloting Deferred per Standards Committee	Under Development
27	Project 2009-26 — Interpretation of CIP-004-1 by WECC	No	CIP-004-1, R2, R3 and R4	x	x	Yes 1st (Intitial Thru 1/19/10)					Balloting Deferred per Standards Committee	Under Development
28	Project 2010-07 — Generator Requirements at the Transmission Interface	High	FAC-001-1, FAC-003-3, FAC-003-X	Yes 1st (Thru 3/15/10)	Yes 3rd (45 Day Formal Thru 11/18/11)	Yes 1st (Intitial Thru 11/18/11)						Under Development
29	Project 2010-07 — Generator Requirements at the Transmission Interface	High	PRC-004-2	Yes 1st (Thru 3/15/10)	Yes 1st (45 Day Formal Thru 11/18/11)	Yes 1st (Intitial Thru 11/18/11)					9/8/11 - SC waived initial 30 day comment period	Under Development
30	Project 2010-17 — Definition of Bulk Electric System	High	NERC Glossary Of Terms	Yes 1st (Thru 1/21/11)	- Yes 3rd (Definition Thru 10/10/11) - Yes 2nd (ROP & Tech Principles Thru 10/10/11)	Yes 2nd (Definiton Intitial Thru 10/10/11) Yes 2nd (Tech Principles Thru 10/10/11) Yes 2nd (ROP Thru 10/27/11)						
31	Project 2011-INT-01 Interpretation of MOD-028 for FPL	No	MOD-028	Yes 1st (Thru 11/16/11)	Yes 1st (Thru 11/16/11)	Yes 1st (Thru 11/16/11)						Under Development
32	Project 2007-02 — Operating Personnel Communications Protocols	High	COM-003-1 and COM-002-2	Yes 2nd (Thru 5/2/07)	Yes 1st (Thru 1/15/10)							Under Development
33	Project 2007-06 — System Protection Coordination	High	PRC-001-1	Yes 1st (Thru 7/10/07)	Yes 1st (Thru 10/26/09)							Under Development
34	Project 2007-11 — Disturbance Monitoring	No	PRC-002-1 and PRC-018-1	Yes 1st (Thru 4/20/07)	Yes 1st (Thru 3/18/09)							Under Development
35	Project 2008-12 — Coordinate Interchange Standards	No	INT-004-, INT-006-4, INT-009-2, INT-010-2 and INT-011-1	Yes 1st (Thru 7/31/08)	Yes 1st (Thru 12/11/09)							Under Development
36	Project 2009-02 — Real-time Reliability Monitoring and Analysis Capabilities	No	"New"	Yes 2nd (Thru 2/18/10)	Yes 1st (Informal Thru 4/4/11)						Concept White Paper posted for informal comment period	Under Development
37	Project 2010-05.1 — Protection Systems: Phase 1 (Misoperations)	High	PRC-004-3	Yes 1st (Informal Thru 7/11/11)	Yes 1st (30 Day Formal Thru 7/11/11)						".1" refers to Phase 1 of the Project	
38	Project 2010-16 — Definition of System Operator	No	NERC Glossary Of Terms	Yes 1st (Thru 12/3/10)	Yes 1st (Thru 12/3/10)							Under Development
39	Project 2010-INT-05 CIP-002-1 Requirement R3 for Duke Energy	No	CIP-002-1, R3	x	Yes 1st (Thru 10/8/10)						To be worked in parallel with Project 2009-26	Under Development
40	Project 2008-01 — Voltage and Reactive planning and control	No	VAR-001 and VAR-002	Yes 2nd (Thru 3/26/10)								Under Development
41	Project 2008-02 — Undervoltage Load Shedding	No	PRC-010-0 and PRC-022-1	Yes 1st (Thru 02/19/10)							June 2010 SC meeting - Project deferred until Higher Priority projects are completed	Project Deferred
42	Project 2009-03 — Emergency Operations	No	EOP-001, EOP-002, EOP-003 and IRO-001	Yes 1st (Thru 1/15/10)								Under Development
43	Project 2009-05 — Resource Adequacy Assessments	No	"New"	Yes 2nd (Thru 3/30/06)								Under Development
44	Project 2009-07 — Reliability of Protection Systems	No	"New"	Yes 1st (Thru 2/18/09)							Pending prioritization - may be postponed	Under Development
45	Project 2010-08 — Functional Model Glossary Revisions	No		Yes 1st (Thru 2/22/10)							June 2010 SC meeting - Project deferred until Higher Priority projects are completed	Project Deferred
46	Project 2008-06 — Cyber Security — Order 706 -- CIP Version 5 Standards										Posting for comment and ballot planned for November 2011	Under Development
47	Project 2009-04 — Phasor Measurement Units	No										Project has not started
48	Project 2010-01 — Support Personnel Training	No										Project has not started
49	Project 2010-02 — Connecting New Facilities to the Grid	No										Project has not started
50	Project 2010-03 — Modeling Data	No										Project has not started
51	Project 2010-04 — Demand Data	No										Project has not started
52	Project 2010-06 — Results-based Reliability Standards	No	Results-based Reliability Standards Transistion Plan								Transistion Plan posted 7/26/10	
53	Project 2010-14 — Balancing Authority Reliability-based Control	No									As of July 28, 2010 this project has merges Project 2007-18 - Reliability-based Controls and is now Project 2010-14 - Balancing Authority Reliability-based Control into a single project	Under Development
54	Project 2010-INT-01 Interpretation of TOP-006-2 R1.2 and R3 for FMPP	No	TOP-006-2, R1.2 and R3								Requester has been contacted to see if CAN provides necessary clarication - awaiting response	On Hold
55	Project 2010-INT-02 Interpretation of TOP-003-1 R2 for FMPP	No	TOP-003-1, R2								Requester has been contacted to see if a CAN would satisfy their concerns until the standard is revised - awaiting response	On Hold
56	Project 2010-INT-03 Interpretation of TOP-002-2a R2, R8, and R19 for FMPP	No	TOP-002-2a, R2, R8 and R19								Requester has been contacted to see if a CAN would satisfy their concerns until the standard is revised - awaiting response	On Hold
57	Project 2012-01 Equipment Monitoring and Diagnostic Devices	No	FUTURE									
58	Project 2012-02 Physical Protection	No	FUTURE									
59	Pre-2006 — Operate Within Interconnection Reliability Operating Limits	No	IRO-008-1, IRO-009-1 and IRO-010-1a	Yes 2nd (Thru 9/23/02)	Yes 9th (Thru 4/25/08)	Yes 1st (Recirc Thru 8/21/08)	Yes (8/21/08)	Yes (10/17/08)	Yes (12/31/09)	Yes (3/17/11)	- Order on Rehearing published in Federal Register on July 19, 2011 - Rule published in Federal Register on March 23, 2011	Completed

NERC Reliability Standards Executive Tracking Summary

Revised: 11/18/2011

Line No.	Project No. / Title	High Priority?	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
60	Project 2006-01 — System Personnel Training	No	PER-004-2 and PER-005-1	Yes 2nd (Thru 3/20/06)	Yes 4th (Thru 7/17/08)	Yes 5th (Recirc Thru 12/22/08)	Yes (12/22/08)	Yes (04/01/09)	Yes (9/30/09)	Yes (11/18/10)		Completed
61	Project 2006-03 — System Restoration and Blackstart	No	EOP-001-1, EOP-005-2 and EOP-006-2	Yes 2nd (Thru 3/09/07)	Yes 4 th (Thru 11/18/08)	Yes 5th (Recirc Thru 5/18/09)	Yes (5/18/09)	Yes (8/5/09)	Yes (12/31/09)	Yes (3/17/11)	- Order on Rehearing published in Federal Register on July 19, 2011 (Effective Std EOP-001-2) - Rule published in Federal Register on March 23, 2011	Completed
62	Project 2006-04 — Backup Facilities	No	EOP-008-1	Yes 2nd (Thru 3/16/07)	Yes 5th (Thru 3/8/10)	Yes 7th (Recirc Thru 7/26/10)	Yes (7/26/10)	Yes (8/5/010)	Yes (2/11/11)	Yes (4/21/11)	Posted in Federal Register on 4/28/11	Completed
63	Project 2006-08 — Transmission Loading Relief	No	IRO-006-5 and IRO-006-East-1	Yes (For DT Nomination 1/12/07)	Yes 4th (Thru 11/30/09)	Yes 6th (Recirc Thru 8/30/10)	Yes (8/30/10)	Yes (11/4/10)	Yes (1/13/11)	Yes (4/21/11)		Completed
64	Project 2007-04 — Certifying System Operators	Normal	PER-003-1	Yes 2nd (Thru 1/31/08)	Yes 1st (Thru 11/20/09)	Yes 3rd (Recirc Thru 12/13/10)	Yes (12/31/10)	Yes (2/17/11)	Yes (4/29/11)	Yes (9/15/11)		Completed
65	Project 2007-05 — Balancing Authority Controls	No	NA	NA	NA	NA	NA	NA	NA	NA	As of July 28, 2010 this project has been merged with Project 2007-18 - Reliability-based Controls and is now Project 2010-14 - Balancing Authority Reliability-based Control	NA
66	Project 2007-17 — Protection System Maintenance & Testing	High	PRC-005-2	Yes 1st (Thru 7/10/07)	Yes 4th (30 day formal Thru 5/12/11)	Yes 8th (Recirculation Thru 6/30/11)	Failed to reach ballot pool aproval	NA	NA	NA	After PRC-005-2 failed to reach ballot pool approval in the recirculation ballot that ended on 6/30/11, the drafting team revised the standard. The Standards Committee authorized re-initiating the project with a posting of the SAR and revised standard for a 45-day comment period, with an initial ballot of the standard conducted during the last 10 days of the comment period.	Re-initiated
67	Project 2007-18 — Reliability-based Control	No	NA	NA	NA	NA	NA	NA	NA	NA	As of July 28, 2010 this project has been merged with Project 2007-18 - Reliability-based Controls and is now Project 2010-14 - Balancing Authority Reliability-based Control	NA
68	Project 2007-23 — Violation Severity Levels	No	Six sets of VSLs for various standards	Yes 2nd "Supp" (Thru 9/16/10)	Yes 6th (Thru 2/18/11)	Yes (Non-Binding Poll Thru 2/18/11	NA - Non Binding Poll Only	Yes (3/10/11)	Yes (3/21/11)	Yes (5/19/11)		Completed
69	Project 2007-24 - Interpretation of TPL-002 and TPL-003	No	TPL-002-0a and TPL-003-0a	x	x	Yes 2nd (Thru 7/7/08)	Yes (7/7/08)	Yes (7/30/08)	Yes (10/24/08)	Yes (4/23/10)		Completed
70	Project 2007-27 — Interpretation of CIP-006 R1.1 by SCE&G	No	CIP-006, R1.1	x	x	Yes (Recirc Thru 12/4/07)	Yes (12/4/07)	Yes (2/12/08)	Yes (12/22/09)	Yes (5/19/11)		Completed
71	Project 2008-06 — Cyber Security — Order 706 (VRFs and VSLs)	No	CIP VRFs and VSLs	x	Yes 1st (Thru 4/20/09)	Yes (Recirc Thru 11/12/09)	Yes (11/12/09)	Yes (12/16/09)	Yes (12/18/09)	Yes (1/20/11)		Completed
72	Project 2008-07 — Interpretation of EOP-002-2 R6.3 and R7.1 by Brookfield Power	No	EOP-002-2, R6.3 and R7.1	x	x	Yes (Recirc Thru 8/31/09)	Yes (8/31/09)	No (Remanded 2/16/10)	NA	NA	2/16/10 NERC BOT: (1) Remands the proposed interpretation of EOP-002-2, Requirements R6.3 and R7.1, to the Standards Committee because the proposed interpretation adds requirements not in the standard, thereby exceeding the permissible scope of an interpretation, and (2) Directs the Standards Committee to initiate action to revise EOP-002-2 as appropriate	NA
73	Project 2008-08 — EOP VSL Revisions	No	EOP family of standards	Yes 1st (Thru 5/19/08)	Yes 2nd (Thru 12/3/09)	Yes (Non-Binding Poll Thru 2/18/11	NA - Non Binding Poll Only	Yes (3/10/11)	Yes (3/21/11)	Yes (5/19/11)		Completed
74	Project 2008-11 — Interpretation of VAR-002a by ICF Consulting	No	VAR-002-1.1b	x	x	Yes (Recirc Thru 1/6/09)	Yes (1/6/09)	Yes (2/10/09)	Yes (3/5/09)	Yes (9/16/10)		Completed
75	Project 2008-15 — Interpretation of CIP-006-1a By US Army Corps of Engineers	No	CIP-006-1a, R4	x	x	Yes (Recirc Thru 2/16/09)	Yes (2/16/09)	Yes (8/5/09)	Yes (12/22/09)	Yes (5/19/11)		Completed
76	Project 2008-18 — Interpretation of TOP-005-1 and IRO-005-1 by Manitoba Hydro	No	TOP-005-1 , R3 and IRO-005-1, R12	x	x	Yes (Recirc Thru 4/27/09)	Yes (4/27/09)	Yes (11/5/09)	Yes (11/24/09)	Yes (4/21/11)	Posted in Federal Register on 4/26/11	Completed
77	Project 2009-08 — Nuclear Plant Interface Coordination	No	NUC-001-2	Yes 1st (Thru 3/18/09)	Yes 1st (Thru 3/18/09)	Yes (Recirc Thru 7/20/09)	Yes (7/20/09)	Yes (8/5/09)	Date?	Yes (1/21/10)		Completed
78	Project 2009-09 — Interpretation of CIP-001-1 by Covanta	No	CIP-001-1a	x	x	Yes (Recirc Thru 10/9/09)	Yes (10/09/09)	Yes (2/16/10)	Yes (4/21/10)	Yes (2/2/11)	Approved by Letter Order	Completed
79	Project 2009-11 — Interpretation of IRO-010-1 R1.2 and R3 by WECC Reliability Coordination Subcommittee	No	IRO-010-1 R1.2 and R3 --> IRO-010-1a	x	x	Yes (Recirc Thru 6/5/09)	Yes (6/5/09)	Yes (8/5/09)	Yes (12/31/09)	Yes (3/17/11)	NOPR issued 11/18/10, Comments were due 1/24/11	Completed
80	Project 2009-12 — Interpretation of CIP-005-1 by PacifiCorp	No	CIP-005-3a	x	x	Yes (Recirc Thru 10/26/09)	Yes (10/26/09)	Yes (2/16/10)	Yes (4/21/10)	Yes (2/2/11)	Approved by Letter Order	Completed
81	Project 2009-13 — interpretation of CIP-006-1 by PacifiCorp	No	CIP-006-2c	x	x	Yes (Recirc Thru 12/23/09)	Yes (12/23/09)	Yes (2/16/10)	Yes (4/20/10)	Yes (7/15/10)		Completed
82	Project 2009-14 — Interpretation of TPL-002-0 R1.3.10 by PacifiCorp	No	TPL-002-0, R1.3.10	x	x	Yes (Recirc Thru 8/6/09)	Yes (8/6/09)	Yes (11/5/09)	Yes (11/17/09)	Yes (9/15/11)	Posted in Federal Register on 9/22/11 - Effective Date: This rule will become effective October 24, 2011	Completed
83	Project 2009-15 — Interpretation of MOD-001-1 R2 and R8 and MOD-029-1 R5 and R6 by NYISO	No	MOD-001-1, R2 and R8 and MOD-029-1 R5 and R6	x	x	Yes (Recirc Thru 7/17/09)	Yes (7/17/09)	Yes (11/5/09)	Yes (12/2/09)	Yes (9/16/10)		Completed
84	Project 2009-16 — Interpretation - CIP-007-1, R2 — Systems Security Management	No	CIP-007-2a	x	x	Yes (Initial Thru 9/21/09)	Yes (9/21/09)	Yes (11/5/09)	Yes (11/17/09)	Yes (3/18/10)		Completed
85	Project 2009-18 — Withdraw Three Midwest ISO Waivers	No	BAL-006-2 and INT-003-3	x	x	Yes (Initial Thru 9/8/09)	Yes (9/8/09)	Yes (11/5/09)	Yes (11/20/09)	Yes (1/6/11)		Completed
86	Project 2009-19 — Interpretation of BAL-002-0 R4 and R5 by NWPP Reserve Sharing Group	No	BAL-002-0 R4 and R5	x	x	Yes (Initial Thru 2/26/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11
87	Project 2009-21 — Cyber Security Ninety-day Response — CIP Family of Standards	No	CIP-002 through CIP-009, V3	Yes 1st (Thru 11/12/09)	Yes 1st (Thru 11/12/09)	Yes (Recirc Thru 12/14/09)	Yes (12/14/09)	Yes	Yes (1/19/10)	Yes (3/18/10)		Completed
88	Project 2009-23 — Interpretation of CIP-004-2 R3 by Army Corps of Engineers	No	CIP-004-2	x	x	Yes 2nd (Intitial Thru 4/8/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11
89	Project 2009-25 — Interpretation of BAL-001-01 and BAL-002-0 by BPA	No	BAL-001-0.1a and BAL-002-0	x	x	Yes 1st (Intitial Thru 1/15/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11
90	Project 2009-29 — Interpretation of TOP-002-2a R6 by FMPP	No	TOP-002-2a, R6	x	x	Yes 1st (Intitial Thru 2/22/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11
91	Project 2009-30 — Interpretation of PRC-001-1 R1 by WPSC	No	PRC-001-1	x	x	Yes 1st (Intitial Thru 2/26/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11

NERC Reliability Standards Executive Tracking Summary

Revised: 11/18/2011

Line No.	Project No. / Title	High Priority?	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
92	Project 2009-31 — Interpretation of TOP-001-1 R8 by FMPP	No	TOP-001-1, R8	x	x	Yes 1st (Intitial Thru 3/16/10)	Yes (3/16/10)	Yes (5/12/10)	Yes (7/16/10)	Yes (9/15/11)	Posted in Federal Register on 9/20/11 - Effective Date: This rule will become effective November 21, 2011	Completed
93	Project 2009-32 — Interpretation of EOP-003-1 R3 and R5 by FMPP	No	EOP-003-1, R3 and R5	x	x	Yes 2nd (Re-ballot Thru 3/31/10)	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11
94	Project 2010-12 — Order 693 Directives	No	BAL-002-1, EOP-002-3, FAC-002-1, MOD-021-1, PRC-004-2 and VAR-001-2	Yes 1st (Thru 7/13/10)	Yes 1st (Thru 7/13/10)	Yes 2nd (Recirc Thru 7/31/10)	Yes (7/31/10)	Yes (8/5/10)	Yes (9/9/10)	Yes (1/10/11)		Completed
95	Project 2010-15 — Urgent Action Revisions to CIP-005-3	Urgent	CIP-005-4	Yes 1st (Thru 9/27/10)	Yes 3rd (Thru 4/28/11)	Yes 3rd (Thru 4/28/11)	NA	NA	NA	NA	Absorbed into Project 2008-06; Project 2010-15 curtailed	Project Curtailed
96	Project 2010-INT-04 Interpretation of EOP-001-1 R2.4 for FMPP	No	EOP-001-1, R2.4	x	x	x	NA	NA	NA	NA		Standards Committee curtailed work 04/12/11

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

NERC Compliance Application Notice Executive Tracking Summary

Revised: 11/16/2011

Further details regarding the individual documents may be found at: http://www.nerc.com/page.php?cid=3%7C22%7C354

CAN#	Project No. / Title	Associated Standard or Issue	Requirement	Advance Notice?	Posted for Comment?	Comments Posted?	CAN Issued?	Comments
~~CAN-0001~~	~~INT-004-2 R1: Compliance Application Notice~~	~~INT-004-2~~	~~1~~	~~x~~	~~x~~	~~x~~	~~Yes (5/5/10)~~	Retired August 31, 2011
~~CAN-0002~~	~~TOP-003-0 R1.3: Compliance Application Notice~~	~~TOP-003-0~~	~~1.3~~	~~x~~	~~x~~	~~x~~	~~Yes (5/5/10)~~	Retired August 31, 2011
~~CAN-0003~~	~~IRO-006-4.1 R2: Compliance Application Notice~~	~~IRO-006-4.1~~	~~2~~	~~x~~	~~x~~	~~x~~	~~Yes (5/5/10)~~	Retired August 31, 2011
~~CAN-0004~~	~~IRO-004-1 R3: Compliance Application Notice~~	~~IRO-004-1~~	~~3~~	~~x~~	~~x~~	~~x~~	~~Yes (5/5/10)~~	Retired August 31, 2011
CAN-0005	CIP-002-3 R3: Compliance Application Notice (Revised)	CIP-002-3	3	x	Yes 8/31/11 (Thru 9/21/11) - Revision	x	Yes (7/6/11 - Revised)	Under Revision
CAN-0006	EOP-005 R7: Verification of Restoration Procedure (Revised)	EOP-005-1	7	x	Yes 8/31/11 (Thru 9/21/11) - Revision	Yes (11/11/11)	Yes (11/11/11)	Revised CAN posted 11/11/11
CAN-0007	CIP-004-2 R4.2 and CIP-004-3 R4.2: Compliance Application Notice	CIP-004-2, CIP-004-3	4.2, 4.2	x	Yes 8/31/11 (Thru 9/21/11) - Revision	x	Yes (12/2/10)	Under Revision
CAN-0008	PRC-005 R2: Basis for First Maintenance and Testing Date (Revised)	PRC-005-1	R2 Pre-June 18 evidence	x	Yes 8/31/11 (Thru 9/21/11) - Revision	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0009	FAC-008 and FAC-009: Facility Ratings and Design Specifications (Revised)	FAC-008 & FAC-009	R1, R1, R2	x	Yes 9/23/11 (Thru 10/14/11)	Yes (11/11/11)	Yes (11/11/11)	Revised CAN issued 11/11/11
CAN-0010	Implementation of Annual in Reliability Standards Requirements (Revised)	Definition of "Annual"		x	x	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0011	PRC-005 R2: Interval Start Date for New Equipment (Revised)	PRC-005-1	R2 - new equipment	x	x	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0012	Completion of Periodic Activity Requirements During Implementation Plan (Revised)			x	Yes 1/21/11 (Thru 2/4/11)	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0013	PRC-023 R1 and R2: Effective Dates for Switch-On-To-Fault Schemes (Revised)	PRC-023		x	Yes 1/21/11 (Thru 2/4/11)	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0015	Unavailability of NERC Software Tools			x	Yes 2/4/11 (Thru 2/18/11)	Yes (10/10/11)	Yes (7/18/11)	On 10/10/11, RE-DRAFTED CANs posted for 21-Day Industry Comment Period ending 10/31/11
CAN-0016	CIP-001 R1: Sabotage Reporting Procedure (Revised)	CIP-001		x	Yes 8/15/11 (Thru 9/6/11) - Revision	Yes (10/14/11)	Yes (10/14/11)	Revised CAN posted 10/14/11
CAN-0017	CIP-007 R5: Technical and Procedural System Access and Password Controls	CIP-007	R5	x	Yes 9/23/11 (Thru 10/14/11)	Yes (11/11/11)	Yes (11/11/11)	Revised CAN posted 11/11/11
CAN-0018	FAC-008 R1.2.1: Terminal Equipment (Revised)	FAC-008		x	Yes 8/31/11 (Thru 9/21/11) - Revision	Yes (11/11/11)	Yes (11/11/11)	Revised CAN posted 11/11/11
CAN-0022	CAN-0022 VAR-002-1.1b R1 and R3	VAR-002		x	Yes 4/19/11 (Thru 5/11/11)	Yes (10/10/11)	Yes (6/17/11)	On 10/10/11, RE-DRAFTED CANs posted for 21-Day Industry Comment Period ending 10/31/11
CAN-0026	CAN-0026 TOP-006-X R3 Protection Relays	TOP-006		x	Yes 4/19/11 (Thru 5/11/11)	Yes (10/10/11)	Yes (6/17/11)	On 10/10/11, RE-DRAFTED CANs posted for 21-Day Industry Comment Period ending 10/31/11
CAN-0028	TOP-006 R1.2: Reporting Responsibilities (Revised)	TOP-006		x	Yes 4/19/11 (Thru 5/11/11)	Yes (11/16/11)	Yes (11/16/11)	Revised CAN posted 11/16/11
CAN-0024	Draft CAN-0024 CIP-002 through CIP-009 Routable Protocols and Data Diodes	CIP-002 through CIP-009		x	Yes 5/20/11 (Thru 6/10/11)	Yes (10/10/11)		On 10/10/11, RE-DRAFTED CANs posted for 21-Day Industry Comment Period ending 10/31/11
CAN-0029	Protection System Misoperations, PRC-004-1 R1, R2, R3	PRC-004	R1, R2, R3	x	Yes 9/23/11 (Thru 10/14/11)	Yes (11/11/11)		Under Revision
CAN-0031	Acceptable Opening Dimensions, CIP-005 and CIP-006	CIP-005 and CIP-006		x	Yes 9/23/11 (Thru 10/14/11)	Yes (11/16/11)		Under Development
CAN-0039	Filing DOE Form OE-417 Event Reports, EOP-004-1	EOP-004		x	Yes 9/23/11 (Thru 10/14/11)	Yes (11/11/11)		Under Revision
CAN-0020	Draft CAN-0020 TPL-002, TPL-003, TPL-004 and TOP-002	TPL-002, TPL-003, TPL-004		x	Yes 10/19/11 (Thru 11/9/11)			
CAN-0027	Draft CAN-0027 TOP-003 R1.1 and R2 Generator	TOP-003		x	Yes 4/19/11 (Thru 5/11/11)			
CAN-0030	Draft CAN-0030 Attestations	Attestations		x	Yes 10/19/11 (Thru 11/9/11)			
CAN-0021	Draft CAN-0021 COM-002 Definition of Directive and Use of Three-Part Communications	COM-002		Yes (5/9/11)				
CAN-0040	BAL- 003 Frequency Response Calculation	BAL-003		x	Yes 11/2/11 (Thru 11/23/11)			
CAN-0043	PRC-005 Protection System Maintenance and Testing Evidence	PRC-005		x	Yes 11/2/11 (Thru 11/23/11)			

Acronyms:
CAN - Compliance Application Notice

NPCC Regional Reliability Standards Executive Tracking Summary

Revised: 11/8/2011

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

Line No.	Regional Standard ID	Regional Reliability Standard Title	RSAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NPCC BOD Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
1	BPS-501-NPCC-01	Classification of Bulk Power System Elements (Withdrawn by RSC 8/07/09)	Yes (Thru 2/4/08)	NA	NA	NA	NA	NA	NA	NA	Withdrawn by RSC 8/07/09	Withdrawn
2	PRC-002-NPCC-01	Disturbance Monitoring	Yes (Thru 9/10/08)	Yes (Thru 10/24/09)	Yes (Thru 1/6/10)	Yes (1/6/10)	Yes (1/9/10)	Yes (11/4/10)	Yes (5/31/11)	Yes (10/20/11)	10/24/11 - Approved Standard posted publicly	Completed
3	PRC-006-NPCC-01	Automatic Underfrequency Load Shedding Program	Yes (Thru 8/25/08)	Yes (Thru 11/2/11)	Yes (Pre-ballot Thru 11/2/11)	Yes 11/8/11 (Thru 11/19/11)					- Pre-ballot review Document posted publicly on 10/19/11 - Replaces Directory #12, Under frequency Load Shedding Program Requirements	Under Development
4	BAL-002-NPCC-01	Regional Reserve Sharing	Yes (Thru 11/2/10)	Yes 11/1/11 (Thru 12/16/11)							Nomination Form posted - nominations due by 11/10/11	Under Development
5	PRC-012-NPCC-01	Special Protection Systems	Yes (thru 8/18/08)									On Hold
6												
7												
8												
9												
10												

Acronyms:

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

NPCC Document Open Process Executive Tracking Summary

Revised: **10/28/2011**

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

Line No.	Type	Document	Description	Effective Date	Comments	Status
1	Criteria	A-01	Criteria for Review and Approval of Documents			
2	Criteria	A-07	Revise Critical Component Definition (Glossary of Tterms)		To be retired - pending approval of Glossary	
3	Criteria	A-10	Classification of BPS Elements			
4	Criteria	A-15	Disturbance Monitoring Equipment Criteria			
5	Guideline	B-01	NPCC Guide for the Application of Autoreclosing to the Bulk Power System			
6	Guideline	B-12	Guidelines for On-Line Computer System Performance During Disturbances			
7	Guideline	B-25	Guide to Time Suynchronization			
8	Guideline	B-26	Guide for Application of Disturbance Recording Equipement			
9	Guideline	B-27	Regional Critical Asset Identification Methodology			
10	Guideline	B-28	Guide for Generator Sequence of Events Monitoring			
11	Procedure	C-00	Listing of NPCC Documents by Type			
12	Procedure	C-01	NPCC Emergency Preparedness Conference Call Procedures - NPCC Security Conference Call Procedures			
13	Procedure	C-05	Monitoring Procedures for Emergency Operation Criteria			
14	Procedure	C-07	Monitoring Procedures for the Guide for Rating Generating Capability			
15	Procedure	C-15	Procedures for Solar Magnetic Disturbances Which Affect Electric Power Systems			
16	Procedure	C-17	Procedures for Monitoring and Reporting Critical Operating Tool Failures			Open Process - comment period ended 7/22/11
17	Procedure	C-21	Monitoring Procedures for Conformance with Normal and Emergency Transfer Limits			
18	Procedure	C-25	Procedure to Collect Power System Event Data			
19	Procedure	C-29	Procedures for System Modeling:Data Requirements and Facility Ratings			
20	Procedure	C-30	Procedure for Task Force on System Protection Review of Disturbances and Protection Misoperations			
21	Procedure	C-33	Procedure for Analysis and Classification of Dynamic Control Systems			Open Process - comment period ended 3/27/11
22	Procedure	C-36	Procedures for Communications During Emergencies			
23	Procedure	C-39	Procedure to Collect Major Disturbance Event Data			
24	Procedure	C-42	Procedure for Reporting and Reviewing System Disturbances			
25	Procedure	C-43	NPCC Operational Review for the Integration of New facilities			
26	Procedure	C-44	NPCC Regional Methodology and Procedures for Forecasting TTC and ATC			
27	Procedure	C-45	Procedure for Analysis and Reporting of Protection System Misoperations	5/25/2011	[C-45 was previously reserved for CO-12 Seasonal Assessment Methodology (previously proposed but not issued - information included in the CO-12 Working Group scope instead)]	
28	Procedure	Cost Effectiveness Analysis Procedure - CEAP				Open Process - Comment period through 9/19/11
29	Glossary	NPCC Glossary of Terms				Open Process - Comment period through 9/12/11
30	Criteria	A-02 (retired)	Basic Criteria for Design and Operation Of Interconnected Power Systems		A2 retired	Directory #1 established
31	Criteria	A-03 (retired)	Emergency Operation Criteria		A3 retired	Directory #2 established
32	Criteria	A-04 (retired)	Maintenance Criteria for Bulk Power System Protection		A4 retired 7/11/2008	Directory #3 established
33	Criteria	A-05 (retired)	Bulk Power System Protection Criteria		A5 retired	Directory #4 established
34	Criteria	A-06 (retired)	Operating Reserve Criteria		A6 retired 12/2/2010	Directory #5 established
35	Criteria	A-08 (retired)	NPCC Reliability Compliance and Enforcement Program		A-08 retired	CCEP-1 established
36	Criteria	A-11 (retired)	Special Protection System Criteria			Directory #7 established
37	Criteria	A-12 (retired)	System Restoration Criteria		A12 draft replaced by Directory #8 10/21/08	Directory #8 established
38	Criteria	A-13 (retired)	NPCC Inc. Verification of Generator Gross and Net Real Power Capability		A13 retired 12/22/2008	
39	Criteria	A-14 (retired)	Verification of Generator Gross and Net Reactive Power Capability		A14 retired 12/22/2008	
40	Guideline	B-02 (retired)	Control Performance Guide		B2 retired	Content transferred to Directory #5 App. 5
41	Guideline	B-03 (retired)	Guidelines for Inter-AREA Voltage Control		B3 retired	Replaced by Procedure C-40

NPCC Document Open Process Executive Tracking Summary

Revised: **10/28/2011**

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

Line No.	Type	Document	Description	Effective Date	Comments	Status
42	Guideline	B-04 (retired)	Guidelines for NPCC Area Transmission Reviews		B4 retired	Content transferred to Directory #1 App.B
43	Guideline	B-05 (retired)	Bulk Power System Protection Guide		B5 retired	Content transferred to Directory #4 App. A
44	Guideline	B-06 (retired)	Automatic Load Shedding Employing Underfrequency Threshold Relays		B6 retired	Replaced by Guideline B-07
45	Guideline	B-07 (retired)	Automatic Underfrequency Load Shedding Program		B7 retired	Content transferred to Directory #4 App. A
46	Guideline	B-08 (retired)	Guidelines for Area Review of Resource Adequacy		B8 retired	Content transferred to Directory #1 App.D
47	Guideline	B-09 (retired)	Guide for Rating Generating Capability		B9 retired	Replaced by Criteria A-13 Document on July 18, 2007
48	Guideline	B-10 (retired)	Guidelines for Requesting Exclusions		B10 retired	Content transferred to Directory #1 App. E
49	Guideline	B-11 (retired)	Special Protection System Guideline		B11 retired	Replaced by Criteria A-11
50	Guideline	B-13 (retired)	Guide for Reporting System Disturbances		B13 retired	Replaced by Procedure C-42
51	Guideline	B-21 (retired)	NPCC Guide for Analysis and Reporting of Protection System Misoperations		Superseded by C-45	Replaced by Procedure C-45
52	Guideline	B-22 (retired)	Guidelines for Implementation of the NPCC Compliance Program		B-22 retired	CCEP-1 established
53	Guideline	B-24 (retired)	Security Guidelines for Protection System IEDS		B24 retired	Content transferred to Directory #4 App. A
54	Procedure	C-03 (retired)			C3 retired	Replaced by Procedure C-36
55	Procedure	C-04 (retired)	Monitoring Procedure for Guides Inter-AREA Volt Control		C4 retired	Content transferred to Directory #1 App. G
56	Procedure	C-08 (retired)	Monitoring Procedures for Control Performance Guide		C8 retired	Content transferred to Directory #5 App. #5
57	Procedure	C-09 (retired)	Monitoring Procedures for Operating Reserve Criteria		C9 retired	Content transferred to Directory #5 App. #2
58	Procedure	C-10 (discontinued)			C10 discontinued	
59	Procedure	C-11 (retired)	Monitoring Procedures for Interconnected System Freq Response		C11 retired	Content transferred to Directory #5 App. #1
60	Procedure	C-12 (retired)	Procedure Shared Activation Ten Minute Reserve		C12 retired	Content transferred to Directory #5 Sect 5.8 & App. #4
61	Procedure	C-13 (retired)	Operational Planning Coordination		C13 retired	Content transferred to Directory #1 App. F
62	Procedure	C-14 (retired)			C14 retired	Procedure C-14 was incorporated in Procedure C-13
63	Procedure	C-16 (retired)	Procedure for Review of New or Modified BPS SPS		C16 retired	Content transferred to Directory #7 App.B
64	Procedure	C-18 (retired)	Procedure for Test & Analysis Extreme Contingencies		C18 retired	Content transferred to Directory #1 App.C
65	Procedure	C-20 (retired)	Procedures During Abnormal Operating Conditions		C20 retired	Content transferred to Directory #5 App. #3
66	Procedure	C-22 (retired)	Procedure for Reporting & Review Proposed BPS Protection Systems		C22 retired	Content transferred to Directory #4 App. A
67	Procedure	C-32 (retired)	Review Process for NPCC Reliability Compliance Enforcement Program		C-32 retired	CCEP-1 established
68	Procedure	C-35 (retired)	NPCC Inter-Area Power System Restoration Procedure		C35 retired	Incorporated within Directory #8 System Restoration
69	Procedure	C-37 (retired)	Operating Procedures for ACE Diversity Interchange		C37 retired	Content transferred to Directory #5 Sect.5.11
70	Procedure	C-38 (retired)	Procedure for Operating Reserve Assistance			Content will be transferred to new Directory #5 Reserve
71	Procedure	C-40 (retired)	Procedures for Inter-AREA Voltage Control		C40 retired	Content transferred to Directory #1 App. G & Directory #2 App. B

Acronyms:

NPCC Directory Executive Tracking Summary

Revised: 10/28/2011 Further details regarding the individual documents may be found at: http://www.npcc.org/regStandards/opOther.aspx

Line No.	Document	Developed From	Description	Version Date	Phase	Task Force Review	Posted Open Process?	RCC Approval?	Full Membership Ballot?	Comments	Status
1	Directory #1	Criteria A-2	Design and Operation of the Bulk Power System	12/1/09 (V0)		Under TFCO/CO-8 review				Open Process posting expected in mid December, 2011	Revision Under Development
2	Directory #2	Criteria A-3	Emergency Operations	1/6/11 (V3)		TFCO Review					
3	Directory #3	Criteria A-4	Maintenance Criteria for Bulk Power System Protection	6/3/09 (V1)						Phase 2 reformatting pending	
4	Directory #4	Criteria A-5	Bulk Power System Protection Criteria	12/1/09 (V0)						TFSP expects to begin Phase 2 review of Directory #4 in early 2012.	
5	Directory #5	Criteria A-6	Reserve	12/2/10 (V0)						TFCO special meeting is scheduled for Dec. 6, 2011 to finalize proposed revisions to Directory #5 in advance of an Open Process posting.	Revision Under Development
6	Directory #6		Regional Reserve Sharing				Yes (Thru 10/24/11)			Open Process posting for Directory #6 concluded on Oct. 24, 2011	
7	Directory #7	Criteria A-11	Special Protection Systems	12/27/07 (V0)						Post for member comment is expected after the November 2011 TFSP Meeting	
8	Directory #8	Criteria A-12	System Restoration	10/22/10 (V1)						Reformatting of Directory #8 which will be addressed by CO-8 early next year	
9	Directory #9	Criteria A-13	Verification of Generator Gross and Net Real Power Capability	7/7/09 (V1)			Yes 2nd (Thru 10/24/11)			TFCO expects to present Directories #9 and #10 to the RCC in November, 2011, and anticipates a Full Member ballot of both Directories #9 and #10 in December, 2011.	Phase 2 Reformatting
10	Directory #10	Criteria A-14	Verification of Generator Gross and Net Reactive Power Capability	7/7/09 (V1)			Yes 2nd (Thru 10/24/11)			TFCO expects to present Directories #9 and #10 to the RCC in November, 2011, and anticipates a Full Member ballot of both Directories #9 and #10 in December, 2011.	Phase 2 Reformatting
11	Directory #11										
12	Directory #12		Under frequency Load Shedding Program Requirements	1/6/11 (V2)			Yes (Thru 1/21/11)			V2 - Errata	Will be replaced by Regional Standard PRC-006-NPCC-01
13	Manual	New	Directory Development and Revison manual				Yes (Thru 9/12/11)			10/26/11 - RSC approved proceding with manual for RCC review and approval	

Acronyms:
MC - Members Committee
RCC - Reliability Coordinating Committee

[Federal Register Volume 76, Number 207 (Wednesday, October 26, 2011)]
[Proposed Rules]
[Pages 66220-66229]
From the Federal Register Online via the Government Printing Office [www.gpo.gov]
[FR Doc No: 2011-27625]

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM11-20-000]

Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards

October 20, 2011.
AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: Under section 215 of the Federal Power Act, the Federal Energy Regulatory Commission (Commission) proposes to approve Reliability Standards PRC-006-1 (Automatic Underfrequency Load Shedding) and EOP-003-2 (Load Shedding Plans), developed and submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC), the Electric Reliability Organization certified by the Commission. The proposed Reliability Standards establish design and documentation requirements for automatic underfrequency load shedding programs that arrest declining frequency and assist recovery of frequency following system events leading to frequency degradation. The Commission also proposes to approve the related Violation Risk Factors and Violation Severity Levels, implementation plan, and effective date proposed by NERC.

DATES: Comments are due December 27, 2011.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:
Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE., Washington, DC 20426.
Instructions: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:
Stephanie Schmidt (Technical Information), Office of Electric Reliability, Division of Reliability Standards, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502-6568, Stephanie.Schmidt@ferc.gov.
Matthew Vlissides (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502-8408, Matthew.Vlissides@ferc.gov.

SUPPLEMENTARY INFORMATION:
1. Under section 215 of the Federal Power Act (FPA),\1\ the Commission proposes to approve proposed Reliability Standards PRC-006-1

[[Page 66221]]

(Automatic Underfrequency Load Shedding) and EOP-003-2 (Load Shedding Plans). The proposed Reliability Standards were developed and submitted for approval to the Commission by the North American Electric Reliability Corporation (NERC), which the Commission certified as the Electric Reliability Organization (ERO) responsible for developing and enforcing mandatory Reliability Standards.\2\ The proposed Reliability Standards establish design and documentation requirements for automatic

underfrequency load shedding (UFLS) programs, which are meant to arrest declining frequency and assist recovery of frequency following underfrequency events and provide last resort system preservation measures.

\1\ 16 U.S.C. 824o (2006).
\2\ North American Electric Reliability Corp., 116 FERC] 61,062, order on reh'g & compliance, 117 FERC] 61,126 (2006), aff'd sub nom. Alcoa, Inc. v. FERC, 564 F.3d 1342 (DC Cir. 2009).

---

2. The Commission proposes to approve the related Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), implementation plan, and effective date proposed by NERC. The Commission also proposes to approve the retirement of the currently effective Reliability Standards PRC-007-0, PRC-009-0, and EOP-003-1, and the NERC-approved Reliability Standard PRC-006-0.

3. The Commission seeks comments from NERC and other interested persons on specific issues concerning the proposed Reliability Standards.

I. Background

A. Underfrequency Load Shedding

4. An interconnected electric power system must balance load and generation in order to maintain frequency within a reliable range.\3\ The balance between generation and load within an interconnected electric power system is shown in the frequency of the system.\4\ Underfrequency protection schemes are drastic measures employed if the system frequency falls below a specified value.\5\ The Blackout Report provides the following explanation:

\3\ Electric Power Research Institute, EPRI Power Systems Dynamics Tutorial, Chapter 4 at page 4-78 (2009), available at http://www.epri.com (EPRI Tutorial).
\4\ Id.
\5\ Id.

> [A]utomatic under-frequency load-shedding (UFLS) is designed for use in extreme conditions to stabilize the balance between generation and load after an electrical island has been formed, dropping enough load to allow frequency to stabilize within the island. All synchronous generators in North America are designed to operate at 60 cycles per second (Hertz) and frequency reflects how well load and generation are balanced--if there is more load than generation at any moment, frequency drops below 60 Hz, and it rises above that level if there is more generation than load. By dropping load to match available generation within the island, UFLS is a safety net that helps to prevent the complete blackout of the island, which allows faster system restoration afterward. UFLS is not effective if there is electrical instability or voltage collapse within the island.\6\

\6\ U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations at 92-93 (2004) (Blackout Report).

---

5. UFLS programs are designed for each defined area or system, and they are commonly implemented with devices installed on the distribution side of the power system.\7\ Factors considered in developing a UFLS program include: (1) Underfrequency set point, (2) minimum amount of load to shed, and (3) what load and at what locations to shed.

\7\ UFLS programs are designed to maintain a balance between resources and demand in a defined area (e.g., Interconnection, Regional Entity area, or planning coordinator area).

---

1. Underfrequency Set Point

6. The underfrequency set point is the frequency at which a specified load will disconnect from the system in a UFLS program.\8\ Separately, generators have their own underfrequency set points, which will disconnect them from the system if the frequency drops to a certain value, thus protecting them from damage.\9\ Underfrequency set

points for load shedding are set above the frequencies at which generators disconnect.\10\ This is done to prevent losing additional resources that would exacerbate the imbalance between resources and demand, resulting in further frequency declines. UFLS programs initiate at a specified point to shed the first load block, and if necessary additional load blocks at other lower set points, to arrest system frequency decline prior to the loss of additional resources.\11\

\8\ In Order No. 693-A, the Commission directed NERC to collect the frequency and magnitude of load in UFLS systems. Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, FERC Stats. & Regs.] 31,242, order on reh'g, Order No. 693-A, 120 FERC] 61,053, at P 145 (2007). NERC submitted a response to this request on February 1, 2008 that included the underfrequency set points and magnitude of load shed in each Regional Entity. NERC, Response to FERC Supplemental Request for Information on the Status of Underfrequency Load Shedding, Docket No. RM06-16-000 (filed Feb. 1, 2008).

\9\ EPRI Tutorial at page 4-81.

\10\ Id.

\11\ Id. at P 4-78, 4-79.

---

7. Once a frequency threshold \12\ is identified, the balance of resources and demand to be maintained to prevent the system from reaching that frequency threshold is determined. UFLS programs use validated models of the power system, which consist of mathematical representations of static (e.g., transformers and transmission lines) and dynamic (e.g., generators and motor loads) components of the power system aggregated to simulate how the system performs during system operations.\13\ Models are validated, typically, by comparing actual system operations against simulated system operations to ensure the simulated system operations are within a defined and acceptable margin of tolerance relative to actual system operations. Inaccurate power system models may result in a UFLS program that does not perform as desired, thus undermining the reliability objective of UFLS.

\12\ A frequency threshold is a pre-determined frequency that UFLS programs are designed to avoid reaching, as the system may become unstable at this frequency.

\13\ See, e.g., PowerTech Labs Inc., 2010 Evaluation and Assessment of Southwest Power Pool (SPP) Under-Frequency Load Shedding Scheme, available at http://www.spp.org/publications/SPP-2010-UFLS-Final.pdf.

---

8. A UFLS program is designed to shed sufficient load to arrest system frequency decline without shedding too much load such that frequency increases above 60 Hz. If a UFLS program is not effective, either because of invalid power system models or miscoordination of the UFLS program with entities inside and outside of the intended island, it may not achieve the reliability objective of preventing cascading outages. This, in turn, could further undermine reliability and recovery of the Bulk-Power System during a system emergency.\14\

\14\ For example, if not enough load is shed to arrest frequency decline, additional resources may disconnect from the Interconnection to prevent damage to generators, and thus system frequency will continue to collapse. Conversely, if too much load is shed, the system frequency could exceed 60 Hz also causing resources to disconnect from the Interconnection to prevent damage to generators. EPRI Tutorial at page 4-78.

---

2. Minimum Amount of Load to Shed

9. The amount of load to disconnect is the amount of load shed at each underfrequency set point, typically expressed in megawatts or percent of system peak load or both.\15\

\15\ EPRI Tutorial at page 4-78.

---

3. What Load to Shed

10. In addition to determining the amount of load to disconnect based on validated power system models, a UFLS program identifies what loads to shed

[[Page 66222]]

and their locations. Therefore, in deciding what specific loads to shed, consideration is given to whether the load is critical (e.g., hospitals, police stations, or fire stations). These loads would typically not be included in a UFLS program.

B. Mandatory Reliability Standards

11. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.\16\

\16\ See 16 U.S.C. 824o(e).

---

12. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO \17\ and, subsequently, certified NERC as the ERO.\18\ On March 16, 2007, the Commission issued Order No. 693, approving 83 of the 107 Reliability Standards filed by NERC, including Reliability Standards PRC-007-0, PRC-009-0, and EOP-003-1.\19\ The Commission neither approved nor remanded NERC-approved Reliability Standard PRC-006-0 in Order No. 693.\20\

\17\ Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, Order No. 672, FERC Stats. & Regs.] 31,204, order on reh'g, Order No. 672-A, FERC Stats. & Regs.] 31,212 (2006).

\18\ North American Electric Reliability Corp., 116 FERC] 61,062, order on reh'g & compliance, 117 FERC] 61,126 (2006), aff'd sub nom., Alcoa, Inc. v. FERC, 564 F.3d 1342 (D.C. Cir. 2009).

\19\ Order No. 693, FERC Stats. & Regs.] 31,242 at P 603.

\20\ Id. P 1479.

C. NERC-Approved Reliability Standard

1. PRC-006-0

13. NERC-approved Reliability Standard PRC-006-0 addresses the development of a regional UFLS program that is used as a last resort to preserve islanding operation following a major system event on the Bulk-Power System that could otherwise cause the island system frequency to collapse. PRC-006-0 requires regional reliability organizations to develop, coordinate, document and assess UFLS program design and effectiveness at least every five years. In Order No. 693, the Commission determined neither to approve nor remand this ``fill-in-the-blank'' Reliability Standard because the regional procedures had not been submitted, and the Commission held that it would not propose to approve or remand PRC-006-0 until the ERO submitted the additional information.\21\

\21\ Id. P 1477, 1479.

D. Currently Effective Reliability Standards

1. PRC-007-0

14. Reliability Standard PRC-007-0 requires transmission owners, transmission operators, load serving entities (LSEs) and distribution providers to provide, and annually update, their underfrequency data to facilitate the regional reliability organization's maintenance of the UFLS program database.

2. PRC-009-0

15. Reliability Standard PRC-009-0 requires that the performance of a UFLS system be analyzed and documented following an underfrequency event by requiring the transmission owner, transmission operator, LSE and distribution provider to document the deployment of their UFLS systems in accordance with the regional reliability organization's program.

3. EOP-003-1

16. Reliability Standard EOP-003-1 addresses load shedding plans and requires that balancing authorities and transmission operators operating with insufficient transmission and/or generation capacity have the capability and authority to shed load rather than risk a failure of the system. It includes requirements to establish plans for automatic load shedding for underfrequency or undervoltage, manual load

shedding to respond to real-time emergencies, and communication with other balancing authorities and transmission operators.

II. Proposed Reliability Standards

17. On March 31, 2011, NERC filed a petition seeking Commission approval of proposed Reliability Standards PRC-006-1 and EOP-003-2 and requesting the concurrent retirement of the currently effective Reliability Standards PRC-007-0, PRC-009-0, and EOP-003-1 and NERC-approved Reliability Standard PRC-006-0.\22\ NERC requests an effective date for PRC-006-1 and EOP-003-2 of one year following the first day of the first calendar quarter after applicable regulatory approvals with respect to all Requirements of the proposed Reliability Standards except Parts 4.1 through 4.6 of Requirement R4 of PRC-006-1. With respect to Parts 4.1 through 4.6 of Requirement R4 of PRC-006-1, NERC requests an effective date of one year following the receipt of generation data as would be required in draft Reliability Standard PRC-024-1 \23\ but no sooner than one year following the first day of the first calendar quarter after applicable regulatory approvals of PRC-006-1.

\22\ NERC Petition at 1. The proposed new Reliability Standards are not attached to the NOPR. They are, however, available on the Commission's eLibrary document retrieval system in Docket No. RM11-20-000 and are available on the ERO's Web site, http://www.nerc.com. Reliability Standards approved by the Commission are not codified in the CFR.

\23\ PRC-024-1 addresses ``Generator Performance During Frequency and Voltage Excursions'' and is currently being developed in the NERC standard drafting process.

A. PRC-006-1

18. Proposed Reliability Standard PRC-006-1 would apply to planning coordinators, ``UFLS entities,'' \24\ and transmission owners that ``own Elements identified in the UFLS program established by the Planning Coordinators.'' NERC states that the primary purpose of the proposed Reliability Standard is the establishment of design and document requirements for UFLS programs that arrest declining frequency and assist recovery of frequency following system events leading to frequency degradation.

\24\ PRC-006-1 defines ``UFLS entities'' as: ``All entities that are responsible for the ownership, operation, or control of UFLS equipment as required by the UFLS program established by the Planning Coordinators.''

---

19. NERC states that PRC-006-1 satisfies the Commission's criteria, set forth in Order No. 672, for determining whether a proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest.\25\

\25\ Order No. 672, FERC Stats. & Regs.] 31,204 at P 323-37.

---

20. According to NERC, PRC-006-1 is designed to achieve a specific reliability goal by establishing design and documentation requirements for automatic UFLS programs to arrest declining frequency, assist recovery of frequency following underfrequency events and provide last resort system preservation measures. NERC contends that PRC-006-1 contains a technically sound method to achieve its reliability goal by establishing a framework for developing, designing, assessing and coordinating UFLS programs, and that PRC-006-1 is clear and unambiguous regarding what is required and who is required to comply with the Reliability Standard.

21. NERC states that PRC-006-1 does not reflect ``best practices'' without regard to implementation cost.\26\ NERC contends that it achieves a specific reliability goal of establishing design

[[Page 66223]]

and documentation requirements for automatic UFLS programs to arrest declining frequency and assist recovery following underfrequency events, and that UFLS programs provide last resort system preservation measures by shedding load during system disturbances that result in substantial imbalance between load and generation. NERC also maintains

that PRC-006-1 does not aim at a ``lowest common denominator'' but instead establishes common performance characteristics that all UFLS programs must meet to effectively protect Bulk-Power System reliability.\27\

\26\ NERC Petition at 24.
\27\ Id. at 26.

---

22. NERC states that PRC-006-1 does not include any differentiation in requirements based on entity size, though it provides the opportunity for planning coordinators to consider input from smaller entities when developing the UFLS program. NERC further explains that PRC-006-1 would apply throughout North America, with variances for entities within the Western Electricity Coordinating Council (WECC) and the Quebec Interconnections.

23. As proposed by NERC, PRC-006-1 has 14 requirements and 19 sub-requirements, summarized as follows:

Requirement R1: Requires each planning coordinator to develop and document criteria to identify portions of the bulk electric system that may form islands.

Requirement R2: Requires each planning coordinator to identify the islands to serve as a basis for designing its UFLS program. Sub-Requirements 2.1, 2.2, and 2.3 serve as a checklist of items that the entity must consider when identifying islands.

Requirement R3: Requires each planning coordinator to develop a UFLS program, including notification of and a schedule for implementation by the UFLS entities within its area, that meets the specific performance characteristics set forth in sub-Requirements 3.1 through 3.3 in simulations of underfrequency conditions resulting from an imbalance of up to 25 percent within the identified island.

Requirement R4: Requires each planning coordinator to conduct and document a UFLS design assessment at least once every five years that determines through dynamic simulation whether the UFLS program design meets the performance characteristics in Requirement R3 for each island identified in Requirement R2, with sub-Requirements 4.1 through 4.7 specifying items that the simulation must model.

Requirement R5: Requires each planning coordinator to coordinate its UFLS design with all other planning coordinators whose areas or portions of whose areas are also part of the same identified island through specific actions identified in Requirement R5.

Requirement R6: Requires each planning coordinator to maintain a UFLS database containing data necessary to model its UFLS program for use in event analyses and assessments of the UFLS program at least once each calendar year, with no more than 15 months between maintenance activities.

Requirement R7: Requires each planning coordinator to provide its UFLS database to other planning coordinators within its Interconnection within 30 calendar days of request.

Requirement R8: Requires each UFLS entity to provide data to its planning coordinator(s) according to the format and schedule specified by the planning coordinator(s) to support maintenance of the UFLS database.

Requirement R9: Requires each UFLS entity to provide automatic tripping of load in accordance with the UFLS program design and schedule for application determined by its planning coordinator(s) in each planning coordinator area in which it owns assets.

Requirement R10: Requires each transmission owner to provide automatic switching of its existing capacitor banks, transmission lines, and reactors to control overvoltage as a result of underfrequency load shedding if required by the UFLS program and schedule for application determined by the planning coordinator(s) in each planning coordinator area in which the transmission owner owns transmission.

Requirement R11: Requires each planning coordinator, in whose area a bulk electric system islanding event results in system frequency excursions below the initializing set points of the UFLS program, to conduct and document an assessment of the event within one year of event actuation that evaluates the performance of the UFLS equipment (sub-Requirement 11.1), and the effectiveness of the UFLS program (sub-Requirement 11.2).

Requirement R12: Requires each planning coordinator, in whose islanding event assessment (Requirement R11) UFLS program deficiencies are identified, to conduct and document a UFLS design assessment to consider the identified deficiencies within two years of event actuation.

Requirement R13: Requires each planning coordinator, in whose area a bulk electric system islanding event occurred that also included the area(s) or portions of area(s) of other planning coordinator(s) in the same islanding event and that resulted in system frequency excursions

below the initializing set points of the UFLS program, to coordinate its event assessment (in accordance with Requirement R11) with all other planning coordinators whose areas or portions of whose areas were also included in the same islanding event by either: (i) Conducting a joint event assessment per Requirement R11 among the planning coordinators whose areas or portions of whose areas were included in the same islanding event; or (ii) conducting an independent event assessment per Requirement R11 that reaches conclusions and recommendations consistent with those of the event assessments of the other planning coordinators whose areas or portions of whose areas were included in the same islanding event; or (iii) conducting an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the event assessments of the other planning coordinators whose areas or portions of whose areas were included in the same islanding event, identifying differences in the assessments that likely resulted in the differences in the conclusions and recommendations and report these differences to the other planning coordinators whose areas or portions of whose areas were included in the same islanding event and to the ERO.

Requirement R14: Requires the planning coordinator to respond to written comments submitted by UFLS entities and transmission owners within its planning coordinator area following a comment period and before finalizing its UFLS program, indicating in the written response to comments whether changes will be made or reasons why changes will not be made to the UFLS program, including a schedule for implementation (sub-Requirement 14.1) and the UFLS design assessment (sub-Requirement 14.2).

B. EOP-003-2

24. Proposed Reliability Standard EOP-003-2 would apply to balancing authorities and transmission operators. NERC states that EOP-003-2 makes minimal changes to EOP-003-1 by removing references to UFLS, which NERC describes as redundant in light of proposed Reliability Standard PRC-006-1, and instead focuses proposed Reliability Standard EOP-003-2 on undervoltage conditions.

[[Page 66224]]

III. Discussion

25. Pursuant to section 215(d)(2) of the FPA, the Commission proposes to approve Reliability Standard PRC-006-1 and EOP-003-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission believes that the UFLS program addressed in the proposed Reliability Standards is important to arresting declining frequency and assisting recovery of frequency following system events that lead to system instability, which can result in a blackout. The Commission finds that the proposed Reliability Standards are necessary for reliability because UFLS is used in extreme conditions to stabilize the balance between generation and load after an electrical island has been formed, dropping enough load to allow frequency to stabilize within the island. Reliability Standard PRC-006-1, in conjunction with the conforming changes to EOP-003-2, provides last resort Bulk-Power System preservation measures by establishing the first national Reliability Standard of common performance characteristics that all UFLS programs must meet. In addition, the Commission proposes to approve the related VRFs and VSLs, implementation plan, and effective date proposed by NERC. Finally, the Commission proposes to approve the retirement of the currently effective Reliability Standards PRC-007-0, PRC-009-0, and EOP-003-1, and the NERC-approved Reliability Standard PRC-006-0.

26. The Commission addresses or seeks comments from the ERO and other interested persons on aspects of the proposed Reliability Standards. Specifically, we address or seek comments on the following issues: (A) Impact of resources not connected to the bulk electric system; (B) validation of power system models used to simulate ULFS programs; (C) scope of UFLS events assessments; (D) impact of generator owner trip settings outside of the UFLS program; (E) UFLS program coordination with other protection systems; (F) identification of island boundaries in UFLS programs; (G) automatic load shedding in PRC-006-1 and manual load shedding in EOP-003-2; (H) elimination of balancing authority responsibilities in EOP-003-2; and (I) the ``Lower VSL'' for Requirement R8 and the ``Medium'' VRF for Requirement R5 of PRC-006-1. These issues also apply to the corresponding Requirements in the requested regional variance for WECC in PRC-006-1.

A. Impact of Resources Not Connected to Bulk Electric System Facilities

27. As described above, UFLS programs are designed to maintain

balance between resources and load in a defined area (e.g., an Interconnection, Regional Entity area, or planning coordinator area). When a resource is lost, load exceeds supply causing frequency to decrease below its scheduled value (e.g., 60 Hz in the United States). Conversely, a loss of load or excess supply can result in higher frequencies than scheduled, resulting in an overfrequency condition. As a last resort, UFLS programs are initiated during extreme underfrequency conditions to reestablish balance by shedding load at predetermined frequencies and times to prevent system-wide blackouts.

28. Requirement R2 of PRC-006-1 requires planning coordinators to identify islands to serve as a basis for designing UFLS programs. Requirement R3 addresses performance characteristics for UFLS programs. Requirement R4 requires each planning coordinator to conduct and document the assessment of its UFLS design and determine if the UFLS program meets the performance characteristics in Requirement R3 for each island identified in Requirement R2.

29. The simulations outlined in Requirement R4 all concern individual generating units greater than 20 MVA gross nameplate rating or generating plants/facilities greater then 75 MVA ``connected to the bulk electric system.'' However, some generation that meets the 20 MVA and 75 MVA criteria is not connected to bulk electric system facilities. Accordingly, those resources not connected to bulk electric system facilities would not be modeled pursuant to Requirement R4. However, a resource not connected to the bulk electric system may serve load designed to be shed in a UFLS program. The Commission is concerned that failure to account for resources not connected to the bulk electric system in a planning coordinator's UFLS program could result in the planning coordinator being unaware of how such resources respond to underfrequency conditions. If the planning coordinator is unaware of how these facilities have responded, it may plan to shed more load than is required for an area's frequency to return to normal. This could lead to an unintended overfrequency condition if the plan is carried out in the operating timeframe. These conditions, in turn, could lead the plan to violate the performance characteristics specified in Requirement R3.

30. The performance characteristics identified in Requirement R3 provide acceptable parameters for developing UFLS programs that are designed to restore balance between resources and load. However, the Commission is concerned that generation resources or facilities that are not connected to the bulk electric system may not be considered during the development of UFLS programs.

31. The Commission seeks comments from the ERO and other interested persons as to whether and how all resources required for the reliable operation of the bulk electric system, including resources not connected to bulk electric system facilities, are considered in the development of UFLS programs under Requirements R3 and R4.

B. Validation of Power System Models

32. Power systems consist of static components (e.g., transformers and transmission lines) and dynamic components (e.g., generators and motor loads). Mathematical representations of these components are aggregated to create an area's power system model. Power system planners \28\ and system operators base decisions on simulations, both static and dynamic, using area power system models to meet requirements in both Commission-approved planning and operational Reliability Standards.\29\

\28\ Power system planners may include functional entities such as transmission planners and planning coordinators.

\29\ See, e.g., Reliability Standards MOD-010-0, MOD-012-0 and TOP-002-2a, Requirement R19.

---

33. Requirements R4 and R11 of PRC-006-1 require applicable entities to use dynamic simulations to design and assess the effectiveness of UFLS programs. As previously discussed, UFLS programs are designed to provide last resort system preservation measures by: (1) Arresting declining frequency; and (2) assisting recovery of frequency following underfrequency events. Dynamic simulations that do not accurately represent the power system can result in an UFLS program that is ineffective.

34. The Commission believes that the UFLS program design requirements established in Requirement R2 and the required assessments established in Requirements R4 and R11 of PRC-006-1 are generally acceptable and include improvements above the current Reliability Standards. Accordingly, the Commission believes that the language in the proposed Requirements is appropriate.

[[Page 66225]]

C. UFLS Event Assessments

1. Assessments in the Absence of Island Formation

35. Requirement R11 of PRC-006-1 requires planning coordinators to conduct assessments after a ``BES islanding event results in system frequency excursion below the initializing set points of the UFLS program.'' The Commission is concerned whether the phrase ``BES islanding event'' could be interpreted to mean that a planning coordinator only has to assess an event if it meets both of the following requirements: (1) System frequency excursions fall below the initializing set point for UFLS; and (2) bulk electric system islands form within the Interconnection. If the frequency falls below the initializing UFLS set point but islands do not form (e.g., because the event was not severe enough to isolate portions of the Interconnection, or UFLS or other protection systems failed to operate properly to form islands), an assessment of the performance of the UFLS program for this event is still useful because it can determine if the UFLS program operated as expected.

36. The Commission seeks clarification from the ERO regarding what actions must planning coordinators take under Requirement R11 if an event results in system frequency excursions falling below this initializing set point for UFLS but without the formation of a bulk electric system island.

2. Coordination of Assessments and Results

37. Requirements R5 and R13 of PRC-006-1 require planning coordinators that share identified islands to coordinate UFLS program design and event assessment. The options for coordinating designs of UFLS programs in Requirement R5 include: (1) Developing a common program; (2) conducting a joint UFLS design assessment among the planning coordinators whose area or portions of whose areas are part of the same identified island; or (3) conducting an independent design assessment and, in the event the UFLS design assessment fails to meet Requirement R3, identify modifications to the UFLS program(s) to meet Requirement R3 and report these modifications as recommendations to the other planning coordinators.

38. The options for coordinating event assessments in Requirement R13 include: (1) Conducting a joint event assessment per Requirement R11 among planning coordinators whose areas were affected; (2) conducting an independent event assessment per Requirement R11 that reaches conclusions and recommendations consistent with other planning coordinators whose areas were affected; or (3) conducting an independent event assessment per Requirement R11 and where the assessment fails to reach conclusions and recommendations consistent with those of the other planning coordinators whose areas were affected by the same islanding event, identify differences in the assessments and report these differences to the other affected planning coordinators. The Commission seeks comments from the ERO and other interested persons as to whether the differences should be subsequently reported to the reliability coordinator for resolution in the event that the process does not resolve differences in the assessments.

39. The Commission believes that Requirements R5 and R13 provide flexibility in coordinating UFLS design programs and event assessments among planning coordinators whose areas fall within the same island or whose areas are affected by the same event. Accordingly, the Commission believes that the language in the proposed Requirements is appropriate.

3. Assessment Timeline for Completion

40. Requirement R11 of Reliability Standard PRC-006-1 requires a planning coordinator to perform an island event assessment within one year of an event. If the planning coordinator identifies program deficiencies, Requirement R12 requires the planning coordinator to conduct and document UFLS design assessments, which are meant to consider the deficiencies, within two years of an event. The Commission is concerned that this time frame may be too long since it appears that island event assessments and consideration of deficiencies could reasonably be conducted in a much shorter time frame. Under NERC's proposal, deficiencies could remain within a UFLS program for two years from an event exposing the Bulk-Power System to instability, uncontrolled separation and cascading outages should a frequency event occur that the UFLS program mishandles. NERC provided no explanation of its basis for the proposed two-year time frame.

41. The Commission asks the ERO and other interested persons what the basis is for proposing a two-year time frame. In addition, the Commission seeks clarification from the ERO as to how soon after event actuation would an entity need to implement corrections in response to any deficiencies identified in the event assessment under Requirement R11.

D. Generator Owner Trip Settings Outside of the UFLS Program

42. Requirements 4.1 through 4.7 of Reliability Standard PRC-006-1

are intended to capture the effects of generators that trip prior to UFLS initiation. As previously discussed, a generator trip normally creates an imbalance between resources and load causing system frequency to decline. Some generators may need to disconnect from the system prior to reaching underfrequency set points to protect their components from permanent damage. If this loss occurs during a system event, the generator can no longer provide a response to assist in arresting frequency decline. This resource loss also counteracts the response provided by other resources to arrest frequency decline, increasing the likelihood of instability, uncontrolled separation, and cascading outages.

43. We agree that planning coordinators should consider generators that trip prior to underfrequency set points when developing their UFLS programs. The Commission seeks comments from the ERO and other interested persons on how generation losses outside of the UFLS set points (i.e., generators having trip settings prior to the UFLS underfrequency set points) should be accounted for in UFLS programs (e.g., generator owners who trip outside of the UFLS set points could procure load to shed to account for the loss in generation).

E. UFLS Program Coordination With Other Protection Systems

44. Recommendation 21C of the Blackout Report addresses the coordination of protection systems.\30\ The recommendation states that NERC shall ``determine the goals and principles needed to establish an integrated approach to relay protection for generators and transmission lines and the use of underfrequency and undervoltage load shedding (UFLS and UVLS) programs. An integrated approach is needed to ensure that at the local and regional levels, these interactive components provide an appropriate balance of risks and benefits in terms of protecting specific assets and facilitating overall grid survival.'' \31\ Accordingly, an integrated approach requires coordination of all types of protection systems (e.g., UFLS, UVLS), internally and externally to an entity's

[[Page 66226]]

area, to be responsive to the Blackout Report.

\30\ Blackout Report at 159.

\31\ Id.

---

45. While PRC-006-1 requires coordination of UFLS programs among planning coordinators in Requirements R5, R7, and R13, it does not appear to capture the same level of coordination with other protection systems as in Requirement R1.2.8 of PRC-006-0.\32\ The Commission seeks comments from NERC and other interested persons on whether and how coordination with other protection systems is or is not achieved under the new requirements.

\32\ Requirement 1.2.8 of PRC-006-0 encompasses ``[a]ny other schemes that are part of or impact the UFLS program.''

F. Identification of Island Boundaries

46. Requirement R1 of PRC-006-1 directs planning coordinators to develop criteria to select areas that may form islands based on historical events and system studies. Historical events and system studies provide planning coordinators with the data necessary to determine where islands will occur based on the physics of the system. Requirement R2.3 clarifies that islands identified in Requirement R1, which span two or more Regional Entity areas, should be broken up such that each Regional Entity area forms an island. Requirement R2.3 allows planning coordinators to ``adjust the island boundaries to differ from the Regional Entity area boundaries by mutual consent where necessary'' to preserve contiguous island boundaries that better reflect simulations. The Commission agrees that identifying island boundaries based on where they are likely to occur due to system characteristics, as opposed to maintaining rigid Regional Entity area boundaries, should result in more effective UFLS programs. Accordingly, the Commission encourages cooperation among entities to create UFLS programs that set island boundaries based on where separations are expected to occur during an underfrequency event.

47. In its petition, NERC states that the Requirements allow planning coordinators to ``select islands including interconnected portions of the bulk electric system in adjacent Planning Coordinator areas and Regional Entity areas, without the need for coordinating this

selection with Planning Coordinators in neighboring regions.'' \33\ Requirement R2.3 of PRC-006-1, however, requires ``mutual consent'' to adjust island boundaries from Regional Entity boundaries. The Commission seeks clarification from the ERO concerning the required degree of cooperation and/or ``mutual consent'' between planning coordinators under the proposed Reliability Standard in order for island boundaries to be set so that, while deviating from Regional Entity boundaries, they better approximate actual island separation boundaries.

\33\ NERC Petition at 75-76.

G. Automatic Load Shedding and Manual Load Shedding

48. Proposed Reliability Standard PRC-006-1 requires automatically shedding predetermined amounts of load if frequency declines to the UFLS set point in order to rebalance resources and demand and prevent frequency decline that might cause instability, uncontrolled separation, or cascading outages. Proposed Reliability Standard EOP-003-2 requires manual load shedding plans, which may be employed in addition to the automatic load shedding in the UFLS program, or to mitigate other reliability issues. If load allocated to be shed automatically is also planned for manual load shedding, then that load resource would be double-counted. Once load is disconnected from the system, either automatically or manually, it cannot be used again to arrest frequency decline. In the event that a load resource is double-counted and removed during automatic UFLS, the manual load shedding cannot be completed if called upon. Even if additional load is located and shed to compensate for this missing load, the system would be put into an un-studied state and could have unpredicted, negative responses. Accordingly, resources allocated to each type of load shedding (i.e., automatic and manual) should not overlap.

49. There are no requirements in PRC-006-1 to coordinate automatic load shedding by UFLS and manual load shedding under EOP-003-2. The Commission seeks comments from the ERO and other interested persons on how the coordination of automatic and manual load shedding is considered in light of the fact that the proposed Reliability Standards do not explicitly require coordination.

H. Elimination of Requirements for Balancing Authorities in EOP-003-2

50. Requirements R2, R4, and R7 of the currently-effective Reliability Standard EOP-003-1 apply to transmission operators and balancing authorities. Proposed Reliability Standard EOP-003-2 proposes to eliminate balancing authorities from Requirements R2, R4, and R7.

51. Under the proposed modification, balancing authorities would no longer: (i) Establish plans for automatic load shedding for underfrequency or undervoltage conditions (Requirement R2); (ii) consider factors (including frequency, rate of frequency decay, voltage level, rate of voltage decay, or power flow levels) in designing an automatic undervoltage load shedding scheme (Requirement R4); and (iii) coordinate automatic load shedding throughout its area with underfrequency isolation of generating units, tripping of shunt capacitors, and other automatic actions that will occur under abnormal frequency, voltage, or power flow conditions (Requirement R7). In its petition, NERC explains that balancing authorities were deleted from Requirements R2 and R4 ``because the frequency related aspects of these requirements were removed, leaving only consideration of automatic undervoltage load shedding in these two requirements.'' \34\ NERC's petition, however, does not explain why balancing authorities were removed from Requirement R7. Moreover, given that balancing authorities would no longer be subject to Requirements R2, R4, and R7 of EOP-003-2 and are not listed as applicable entities in PRC-006-1, the proposed Reliability Standards do not preserve these existing balancing authority responsibilities.

\34\ NERC Petition at 42.

---

52. The Commission seeks clarification from the ERO as to why these existing balancing authority responsibilities were not incorporated into Reliability Standards PRC-006-1 or EOP-003-2. The Commission also seeks comments from the ERO and other interested persons as to why balancing authorities should not be informed of UFLS program plans that directly impact balancing authority functions.

I. Violation Risk Factors and Violation Severity Levels

53. NERC states that each primary requirement in PRC-006-1 and EOP-003-2 is assigned a Violation Risk Factor (VRF) and Violation Severity Level (VSL) and that these elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in Commission-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

54. The Commission proposes to approve the VRFs and VSLs in PRC-006-1 and EOP-003-2. However, the Commission seeks comments from the ERO and other interested persons regarding one proposed VSL and one proposed VRF for PRC-006-1.

55. The ``Lower VSL'' assignment for Requirement R8 in PRC-006-1 applies

[[Page 66227]]

when a UFLS entity fails to provide data to its planning coordinator for 5 to 10 calendar days following the schedule specified by the planning coordinator. Requirement R8 of PRC-006-1 does not include a 5-day grace period for providing data to planning coordinators. Accordingly, the subject VSL assignment may be inconsistent with the Commission's VSL Guideline 3. The guideline states that a VSL ``should not appear to redefine or undermine the requirement.'' \35\ The five-day grace period implicit in the proposed VSL appears to be inconsistent with this guideline. In addition, the proposed VSL creates a compliance issue. Specifically, it is unclear where a UFLS entity falls in the VRF and VSL matrices if it fails to provide data to its planning coordinator within 1 to 5 days of its scheduled date.

\35\ North American Electric Reliability Corp., 123 FERC] 61,284, at P 32 (2008).

---

56. The VRF for Requirement R5, which requires planning coordinators to coordinate their UFLS program design with other planning coordinators whose area is in part of the same identified island, is proposed as ``Medium.'' NERC states that Requirement R5 is ``not related to similar reliability goals in other standards.'' \36\ However, coordination of load shedding plans is required in a similar manner in Requirement R3 of currently effective Reliability Standard EOP-003-1,\37\ which includes a VRF of ``High.'' The lack of coordination of UFLS programs among planning coordinators within the same identified island could lead to ineffective UFLS operations and further cascading outages within the island when UFLS is activated.

\36\ NERC Petition at 46.

\37\ Proposed Reliability Standard EOP-003-2 includes the same VRF assignment of ``High'' for Requirement R3.

---

57. Guideline 3 of the Commission's VRF Guidelines states that ``[a]bsent justification to the contrary, the Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.'' \38\ The Commission seeks clarification from the ERO why coordination of load shedding plans is a ``High'' VRF for transmission operators and balancing authorities in EOP-003-2 but NERC proposes a ``Medium'' VRF for planning coordinators in, PRC-006-1.

\38\ North American Electric Reliability Corp., 119 FERC] 61,145, at P 25 (2007).

J. Implementation Plan and Effective Date

58. NERC requests an effective date for PRC-006-1 and EOP-003-2 of one year following the first day of the first calendar quarter after applicable regulatory approvals with respect to all Requirements of the proposed Reliability Standards except Parts 4.1 through 4.6 of Requirement R4 of PRC-006-1. With respect to Parts 4.1 through 4.6 of Requirement R4 of PRC-006-1, NERC requests an effective date of one year following the receipt of generation data as required in Reliability Standard PRC-024-1,\39\ but no sooner than one year following the first day of the first calendar quarter after applicable regulatory approvals of PRC-006-1.

\39\ PRC-024-1 addresses ``Generator Performance During Frequency and Voltage Excursions'' and is currently being developed

in the NERC standard drafting process under Project 2007-09 (Generator Verification), which is one of NERC's priority projects.

---

59. NERC contends that the proposed implementation plan is not excessively long and allows sufficient time for entities to transition and install the necessary processes to become compliant. NERC maintains that the one year phase-in for compliance provides planning coordinators sufficient time: (1) To develop, modify, or validate (to determine that an existing program meets required performance characteristics) existing UFLS programs; and (2) to establish a schedule for implementation, or validate a schedule for completion of program revisions already in progress. Moreover, NERC states that transmission owners and distribution providers will comply with the schedule determined by planning coordinators but no sooner than the effective date of the standard.

60. The Commission proposes to accept the implementation plan and effective date proposed by the ERO for PRC-006-1 and EOP-003-2. However, the Commission seeks comments from the ERO and other interested persons about any potential reliability gaps that may occur during the development and implementation of PRC-024-1, such as how the planning coordinators will adequately determine and apply UFLS simulations and plans in the absence of generator trip settings.

IV. Information Collection Statement

61. The Office of Management and Budget (OMB) regulations require that OMB approve certain reporting and recordkeeping (collections of information) imposed by an agency.\40\ Upon approval of a collection(s) of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

\40\ 5 CFR 1320.11.

---

62. The Commission is submitting these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of PRA. Comments are solicited on the Commission's need for this information, whether the information will have practical utility, the accuracy of provided burden estimate, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques.

63. This Notice of Proposed Rulemaking proposes to approve Reliability Standards PRC-006-1 and EOP-003-2, which would replace currently effective Reliability Standards PRC-007-0, PRC-009-0, EOP-003-1 and NERC-approved Reliability Standard PRC-006-0.\41\ As noted previously, Reliability Standard PRC-006-0 was never approved by the Commission, and therefore has never been mandatory and enforceable. On the other hand, Reliability Standards PRC-007-0 and PRC-009-0 were approved by the Commission and are currently mandatory and enforceable. Because Proposed Reliability Standard PRC-006-1 incorporates the requirements from Reliability Standards PRC-006-0, PRC-007-0, and PRC-009-0 some of the existing requirements will become mandatory and enforceable (where previously they were voluntary), while others continue to be so. To properly account for the burden on respondents, the Commission will treat the burden resulting from NERC-approved Reliability Standard PRC-006-0 as essentially new to the industry, even though it is likely that most applicable entities have already been complying.\42\

\41\ PRC-006-0 was not approved by the Commission but remained effective as a NERC-approved standard (but not mandatory or enforceable). The other three standards were approved by the Commission. Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, FERC Stats. & Regs.] 31,242, order on reh'g, Order No. 693-A, 120 FERC] 61,053 (2007).

\42\ This statement is made because currently effective Reliability Standards PRC-007-0 and PRC-009-0 required UFLS entities to follow the UFLS program implemented by Reliability Standard PRC-006-0. Therefore, it is likely that entities have already been following the requirements contained in Reliability Standard PRC-006-0.

---

64. The reporting requirements in proposed Reliability Standard

EOP-

003-2 are virtually the same as those in currently effective Reliability Standard EOP-003-1. The difference is that proposed Reliability Standard EOP-003-2 proposes to eliminate balancing authorities from Requirements R2 and from Measure M1.\43\ This requirement and measure deal with establishing and documenting automatic load shedding plans.

\43\ Balancing authorities are also removed from Requirements R4 and R7, but these do not have reporting requirements associated with them.

---

65. Public Reporting Burden: Our estimate below regarding the number of respondents is based on the NERC compliance registry as of 7/29/11. According to the NERC compliance registry, there are 72 planning coordinators and 126 balancing authorities. The individual burden estimates are based on the time needed to gather data, run studies, and analyze study results to design or update the UFLS programs. Additionally, documentation and the review of UFLS program results by supervisors and management is included in the administrative estimations. These are consistent with estimates for similar tasks in other Commission approved standards.

	Number of respondents annually	Number of responses per respondent		Average burden hours per response	Total annual burden hours
	(1)	(2)		(3)	(1)x(2)x(3)
PRC-006-1 (Automatic underfrequency load shedding) \44\					
PCs *: Design and document Automatic UFLS Program				120	8,640
PCs: Management Review of Documentation	72	1		40	2,880
PCs: Record Retention				16	1,152
Total					12,672
EOP-003-2 (Load Shedding Plans) \45\					
Removal of BAs * from Reporting Requirements in R2 and M1 (Burden Reduction)	126	1	Reporting	-10	-1260
			Record Retention	-1	-126
Total					-1,386
Net Change in Burden					11,286

* PC = Planning Coordinator; BA = Balancing Authority.

Total Annual Hours for Collection: (Compliance/Documentation) = 11,286 hours.
Total Reporting Cost for Planning Coordinators: = 11,520 hours @ $120/hour = $1,382,400.
Total Record Retention Cost for Planning Coordinators: 1,152 hours @ $28/hour = $32,256.
Total Reporting and Record Retention Cost Savings for Balancing Authorities: = (1,260 hours @ $120/hour) + (126 hours @ $28/hour) = $154,728.

\44\ Proposed Reliability Standard PRC-006-1 applies to both planning coordinators and to UFLS entities. However, the burden associated with the UFLS entities is not new because it was accounted for under Commission approved Reliability Standards PRC-007-0 and PRC-009-0.
\45\ Transmission operators also have to comply with Reliability Standard EOP-003-2 but since the applicable reporting requirements (and associated burden) have not changed from the existing standard to the proposed standard these entities are not included here.

Total Annual Cost (Reporting + Record Retention) \46\: = $1,414,656-$154,728 = $1,259,928.

\46\ The hourly reporting cost is based on the cost of an engineer to implement the requirements of the rule. The record retention cost comes from Commission staff research on record retention requirements.

Title: Mandatory Reliability Standards for the Bulk-Power System.
Action: Proposed Collection FERC-725A.
OMB Control No.: 1902-0244.
Respondents: Businesses or other for-profit institutions; not-for-profit institutions.
Frequency of Responses: On occasion.
Necessity of the Information: This proposed rule proposes to approve the requested modifications to Reliability Standards pertaining to automatic underfrequency load shedding. The proposed Reliability Standards help ensure the reliable operation of the bulk electric system by arresting declining frequency and assisting recovery of frequency following system events leading to frequency degradation.
Internal Review: The Commission has reviewed the proposed Reliability Standards and made a determination that its action is necessary to implement section 215 of the FPA. These requirements, if accepted, should conform to the Commission's expectation for UFLS programs as well as procedures within the energy industry.
66. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE. Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].
67. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM11-20 and OMB Control Number 1902-0244.

V. Environmental Analysis

68. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement

[[Page 66229]]

for any action that may have a significant adverse effect on the human environment.\47\ The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.\48\ The actions proposed here fall within this categorical exclusion in the Commission's regulations.

\47\ Order No. 486, Regulations Implementing the National Environmental Policy Act of 1969, FERC Stats. & Regs., Regulations Preambles 1986-1990] 30,783 (1987).
\48\ 18 CFR 380.4(a)(2)(ii).

VI. Regulatory Flexibility Act Certification

69. The Regulatory Flexibility Act of 1980 (RFA) \49\ generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The RFA mandates consideration of regulatory alternatives that accomplish the stated objectives of a proposed rule and that minimize any significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.\50\ The SBA has established a size standard for electric utilities, stating that a firm is small if, including its affiliates, it is primarily engaged in the transmission, generation and/or distribution of electric energy for sale and its total electric output for the preceding twelve months did not exceed four million megawatt hours.\51\

\49\ 5 U.S.C. 601-612.
\50\ 13 CFR 121.101.
\51\ 13 CFR 121.201, Sector 22, Utilities & n.1.

---

70. Proposed Reliability Standard PRC-006-1 proposes to establish design, assessment, and documentation requirements for automatic UFLS program. It will be applicable to planning coordinators and entities that are responsible for the ownership, operation, or control of UFLS equipment. Proposed Standard EOP-003-2 proposes to remove balancing authorities from having to comply with R2 and M1 of the standard. Comparison of the NERC compliance registry with data submitted to the Energy Information Administration on Form EIA-861 indicates that perhaps as many as 8 small entities are registered as planning coordinators and 18 small entities are registered as balancing authorities. The Commission estimates that the small planning coordinators to whom the proposed Reliability Standard will apply will incur compliance and recordkeeping costs of $157,184 ($19,648 per planning coordinator) associated with the Standard's requirements. The small balancing authorities will receive a savings of $154,728 ($8,596 per balancing authority). Accordingly, proposed Reliability Standards PRC-006-1 and EOP-003-2 should not impose a significant operating cost increase or decrease on the affected small entities.

71. Based on this understanding, the Commission certifies that these Reliability Standards will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

VII. Comment Procedures

72. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due December 27, 2011. Comments must refer to Docket No. RM11-20-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

73. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's Web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

74. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE., Washington, DC 20426.

75. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VIII. Document Availability

76. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the

Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5 p.m. Eastern time) at 888 First Street, NE., Room 2A, Washington, DC 20426.

77. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

78. User assistance is available for eLibrary and the Commission's Web site during normal business hours from the Commission's Online Support at 202-502-6652 (toll free at 1-866-208-3676) or e-mail at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

List of Subjects in 18 CFR Part 40

Electric power; Electric utilities; Reporting and recordkeeping requirements.

By direction of the Commission. Commissioner Spitzer is not participating.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2011-27625 Filed 10-25-11; 8:45 am]
BILLING CODE 6717-01-P

20111115-3000 FERC PDF (Unofficial) 11/15/2011

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426
OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RR11-2-000

November 15, 2011

Schiff Hardin LLP
1666 K Street, N.W., Suite 300
Washington, D.C. 20036-4390

Attention: Owen E. MacBride
Attorney for North American Electric Reliability Corporation

Reference: Petition for Approval of Compliance Monitoring and Enforcement Agreement Between Northeast Power Coordinating Council, Inc. and Western Electricity Coordinating Council and Related Amendments to Delegation Agreements

Dear Mr. MacBride:

1. On May 25, 2011, the North American Electric Reliability Corporation (NERC) submitted a petition requesting approval of: (1) an agreement between Northeast Power Coordinating Council, Inc. (NPCC) and Western Electricity Coordinating Council (WECC) concerning compliance monitoring and enforcement of WECC registered functions; (2) an agreement between NERC and WECC regarding termination of the existing agreement concerning compliance monitoring and enforcement of WECC registered functions; and (3) related amendments to delegation agreements between NERC and NPCC, and NERC and WECC. NERC requests an effective date of January 1, 2012.

2. NERC states that the purpose of its petition is to provide for NPCC to assume responsibility for performing Regional Entity compliance monitoring and enforcement program functions with respect to those reliability functions for which WECC is the registered entity within the United States portion of the WECC region. Currently, NERC acts as the Compliance Enforcement Authority for WECC registered functions in the United States portion of the WECC region, pursuant to an agreement between NERC and WECC.

20111115-3000 FERC PDF (Unofficial) 11/15/2011

3. Notice of this filing was issued on May 25, 2011, with comments, protests or motions to intervene due on or before June 15, 2011. No protests or adverse comments were filed.

4. NERC's uncontested filing is accepted pursuant to the authority delegated to the Director, Office of Electric Reliability, under 18 C.F.R. § 375.303, effective January 1, 2012.

5. This action shall not be construed as accepting any other contingency plan pursuant to 18 C.F.R. § 375.303(a)(1)(i) or any other data or report pursuant to C.F.R. § 375.303(b)(3)(iv). This action shall not be construed as approving any other application including Electric Reliability Organization or Regional Entity Rules or procedures pursuant to 18 C.F.R. § 375.303(a)(2)(i). Such acceptance or approval shall not be deemed as recognition of any claimed right or obligation associated therewith; and such acceptance or approval is without prejudice to any findings or orders which have been or which may hereafter be made by the Commission in any proceeding now or pending or hereafter instituted by or against NERC.

6. This order constitutes final agency action. Requests for rehearing by the Commission may be filed within 30 days of the date of issuance of this order, pursuant to 18 C.F.R. § 385.713.

Sincerely,

Joseph H. McClelland, Director
Office of Electric Reliability

Document Content(s)

RR11-2-000.DOC.....1-2

137 FERC ¶ 61,123
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Philip D. Moeller, John R. Norris,
and Cheryl A. LaFleur.

North American Electric Reliability Corporation Docket No. RD11-10-000

ORDER APPROVING RELIABILITY STANDARD

(Issued November 17, 2011)

1. The North American Electric Reliability Corporation (NERC) filed a petition requesting approval, pursuant to section 215(d)(1) of the Federal Power Act (FPA) and section 39.5 of the Commission's regulations,[1] of Reliability Standard FAC-008-3 (Facility Ratings), the associated Violation Risk Factors (VRF) and Violation Severity Levels (VSL), and retirement of Reliability Standards FAC-008-1 (Facility Ratings Methodology) and FAC-009-1 (Establish and Communicate Facility Ratings). Reliability Standard FAC-008-3 presents clear, measurable, and enforceable Requirements that obligate transmission owners and generator owners to develop facility ratings methodologies for its facilities. Reliability Standard FAC-008-3 combines currently effective standards FAC-008-1 and FAC-009-1 into a single standard.

2. As discussed in this order, we approve Reliability Standard FAC-008-3 and the retirement of FAC-008-1 and FAC-009-1. We also approve the associated VRFs with one modification, and approve the associated VSLs. The new Reliability Standard, FAC-008-3 will be effective, and Reliability Standards FAC-008-1 and FAC-009-1 will be retired on the first day of the first calendar quarter that is twelve months after issuance of this order, as requested by NERC.

I. Background

A. EPAct 2005 and Mandatory Reliability Standards

3. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which

[1] 16 U.S.C. § 824o(d)(2) (2006) and 18 C.F.R. § 39.5 (2011).

provide for the reliable operation of the Bulk-Power System, subject to Commission review and approval.[2] Section 215(d)(2) of the FPA states that the Commission may approve, by rule or order, a proposed Reliability Standard or modification to a Reliability Standard if it determines that the Reliability Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[3] On February 3, 2006, the Commission issued Order No. 672 to implement the requirements of section 215 of the FPA governing electric reliability.[4] In July 2006, the Commission certified NERC as the ERO.[5]

4. On March 16, 2007, the Commission issued Order No. 693 approving 83 Reliability Standards proposed by NERC, including Reliability Standard FAC-008-1.[6] In Order No. 693, the Commission also directed the ERO to modify Reliability Standard FAC-008-1 to: (1) document underlying assumptions and methods used to determine normal and emergency facility ratings; (2) develop facility ratings consistent with industry standards developed through an open, transparent and validated process, and (3) for each facility, identify the limiting component and, for critical facilities, the resulting increase in rating if that component is no longer limiting.[7]

---

[2] 16 U.S.C. § 824o(d)(2) (2006).

[3] *See id.* § 824o(e)(3).

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

[5] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on clarification and reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[6] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 736, *order on reh'g,* Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[7] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 771.

B. NERC Filing

5. On June 15, 2011, NERC filed a petition requesting approval of Reliability Standard FAC-008-3, the associated VRFs and VSLs for this Reliability Standard, and retirement of Reliability Standards FAC-008-1 and FAC-009-1. NERC states that it developed Reliability Standard FAC-008-3 using the NERC Reliability Standards Development Procedure, and further states that FAC-008-3 addresses all three Commission directives from Order No. 693. Proposed Reliability Standard FAC-008-3 was approved by the NERC Board of Trustees.

6. NERC states that FAC-008-3 addresses the important reliability goal of improving uniformity and transparency in the facility ratings process. NERC avers that the Reliability Standard presents clear, measurable, and enforceable requirements that each transmission owner develop facility ratings methodologies for its facilities, which are essential for the determination of system operating limits.[8] NERC further states that FAC-008-3 requires transmission owners and generator owners to document underlying assumptions and methods used to determine normal and emergency facility ratings. NERC maintains that this added transparency will allow customers, regulators and other affected users, owners, and operators of the Bulk-Power System to understand how facility owners set facility ratings through differing methods that provide equivalent results. NERC notes that FAC-008-3 requires transmission owners and generator owners to make their facility ratings documentation and methodologies available for inspection and technical review, thereby contributing to the important reliability goal of improving uniformity and transparency in the facility ratings process.

7. NERC describes each of the eight FAC-008-3 Requirements as follows.[9]

- Requirement R1 establishes the documentation requirements placed upon a generator owner for determining the facility ratings of its solely and jointly owned generator facility(ies).

---

[8] NERC defines System Operating Limits as "The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria." *Glossary of Terms Used in NERC Reliability Standards* at 42, updated Aug. 4, 2011, *available at:* http://www.nerc.com/files/Glossary_of_Terms_2011August4.pdf (*NERC Glossary*) (examples of the operating criteria omitted).

[9] NERC Petition at 18-20.

- Requirement R2 requires each generator owner to have a documented methodology for determining facility ratings of its solely and jointly owned equipment connected between the location specified in Requirement R1 and the point of interconnection with the transmission owner.

- Requirement R3 requires each transmission owner to have documented methodology for determining facility ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities.

- Requirement R4, which is carried over from Requirement R2 of the currently-effective FAC-008-1 standard, requires each entity to make its documentation and methodology available to other reliability entities for inspection and technical review.

- Requirement R5 revises the currently-effective FAC-008-1, Requirement R3, and requires generator owners and transmission owners that receive comments from another entity as a result of that entity's technical review of a transmission owner's facility ratings methodology or generator owner's documentation for determining its facility ratings and its facility rating methodology, to respond to the commenting entity within 45 calendar days of receipt of those comments. The response must indicate whether a change will be made to the facility ratings methodology and, if no change will be made, the reasons for that decision.

- Requirement R6 carries forward currently-effective FAC-009-1, Requirement R1, and requires that the generator owner and transmission owner also establish facility ratings for their solely and jointly owned facilities that are consistent with the associated facility rating methodology or documentation for determining their facility ratings.

- Requirement R7 provides that the ratings must be provided to other entities as specified in the requirements.

- Requirement R8 requires the identification and documentation of the limiting component for all facilities and the increase in rating if that component were no longer the limiting component, i.e., the rating for the second most limiting component, for facilities associated with an

Interconnection Reliability Operating Limit,[10] a limitation of Total Transfer Capability, an impediment to generator deliverability, or an impediment to service to a major load center.

- Requirement R8 requires entities to provide information to requesting entities regarding their facilities. Sub-requirement R8.1 requires an entity to provide the identity of the most limiting equipment of a facility as well as the facility rating to requesting entities. Sub-requirement R8.2 requires the identity of the next most limiting equipment of a facility as well as the thermal rating of that equipment.

8. NERC states that proposed Reliability Standard FAC-008-3 addresses the three directives in Order No. 693 related to FAC-008-1. In response to the first directive, that the Reliability Standard document underlying assumptions and methods used to determine normal and emergency facility ratings, FAC-008-3 requires transmission owners and generator owners to document underlying assumptions and methods used to determine normal and emergency facility ratings. NERC notes this added transparency will allow customers, regulators, and other affected users, owners, and operators of the Bulk-Power System to understand how facility owners set facility ratings through differing methods that provide equivalent results. Additionally, NERC states FAC-008-3 requires transmission owners and generator owners to make their facility ratings documentation and methodologies available for inspection and technical review, which will improve uniformity and transparency in the facility ratings process.

9. In response to the second Order No. 693 directive that facility ratings be developed consistent with industry standards developed through an open, transparent, and validated process, proposed Reliability Standard FAC-008-3 requires that the methodology used to establish the facility ratings of the equipment that comprises the facilities be consistent with at least: (1) ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating; (2) one or more industry standards developed through an open process such as the Institute of Electrical and Electronic Engineers (IEEE) or International Council on Large Electric Systems (CIGRE); or (3) a practice that has been verified by testing, performance history, or engineering analysis. NERC states that these requirements will ensure that a

[10] NERC defines Interconnection Reliability Operating Limit as "A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." *NERC Glossary* at 24.

methodology chosen by a facility owner is consistent with industry standards developed through an open, transparent, and validated process.

10. Finally, to address the third Order No. 693 directive, that for each facility, the limiting component be identified and, for critical facilities, the resulting increase in rating if that component is no longer limiting, FAC-008-1 is modified to require transmission owners and generator owners to calculate the increase in rating if the first-limiting element is removed only for those facilities for which thermal ratings cause: (1) an Interconnection Reliability Operating Limit; (2) a limitation of Total Transfer Capability; (3) an impediment to generation deliverability; or (4) an impediment to service to major cities or load pockets. NERC states that the standard drafting team interpreted this directive to allow reliability entities to take rating information and prepare operating plans or planning assessments prior to real-time, which could allow for better situational awareness and improved reliability of the bulk electric system.

11. The proposed effective date for mandatory compliance with proposed Reliability Standard FAC-008-3 is the first day of the first calendar quarter that is twelve months following the effective date of Commission approval. NERC states that this effective date will allow applicable entities adequate time to develop the documentation and other evidence necessary to exhibit compliance with the standard.

12. Finally, NERC states that proposed Reliability Standard FAC-008-3 includes clear and understandable consequences for a violation by assigning a VRF and VSL to each main requirement. With respect to the VSL assignments for FAC-008-3, for each Requirement in FAC-008-3, NERC carried forward the approved VSLs from the corresponding Requirements in FAC-008-1 and FAC-009-1.

13. With respect to the VRF assignments for FAC-008-3, NERC assigned a VRF to each main Requirement. The VRFs assigned to Requirements R4 through R8 are carried forward from the approved VRFs for the corresponding Requirements from Reliability Standards FAC-008-1 and FAC-009-1. Requirements R1 through R3 of FAC-008-3, correspond to Requirement R1 of currently effective Reliability Standard FAC-008-1. NERC developed VRFs for proposed FAC-008-3, Requirements R1 through R3 that vary from the currently approved VRFs assigned to FAC-008-1, Requirement 1 and its sub-requirements. NERC states that FAC-008-3, Requirements R1 and R2, which apply to generator owners and radial facilities only are planning-related requirements, are administrative in nature and, if violated, would not under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. Accordingly, NERC proposes these two Requirements be assigned a VRF of "Lower." FAC-008-3, Requirement 3 which pertains to transmission owners, is assigned a VRF of "Medium" consistent with the existing approved VRF for Sub-requirements R1.1 through R1.2.2 of FAC-008-1.

II. Notice of Filing and Comments

14. Notice of NERC's Filing was published in the *Federal Register,* 76 Fed. Reg. 53,119 (2011), with interventions and protests due on or before September 16, 2011. American Municipal Power, Inc. filed a motion to intervene. International Transmission Company d/b/a/ ITC*Transmission*, Michigan Electric Transmission Company, LLC, ITC Midwest LLC, and ITC Great Plains, LLC (ITC Companies) filed comments but did not seek to intervene in this proceeding.

III. Discussion

15. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2011), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

16. We approve Reliability Standard FAC-008-3 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We believe that the modifications are an improvement to the currently-effective Reliability Standard and adequately address the Commission's directives set forth in Order No. 693 that NERC develop certain modifications to FAC-008-1.[11] In several instances, NERC developed alternative approaches to address the concerns articulated in Order No. 693. As discussed below, we find that the proposed Reliability Standard, FAC-008-3 adequately addresses the Commission's Order No. 693 directives by providing equally effective and efficient approaches. Below, we discuss three aspects of NERC's filing: (1) normal and emergency ratings; (2) methodology options for developing facility ratings; and (3) requests for facility ratings data.

A. Normal Rating and Emergency Rating Glossary Terms

17. In Order No. 693, the Commission directed the ERO to submit a modification to FAC-008-1 "that requires transmission and generation facility owners to document underlying assumptions and methods used to determine normal and emergency facility ratings."[12] NERC states that this directive is addressed in Requirements R2.4.2 and R3.4.2 of FAC-008-3,[13] each of which requires that, in developing a documented rating methodology, "the scope of Ratings addressed shall include, as a minimum, both Normal

[11] *See* Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 771.

[12] *Id*. P 739.

[13] NERC Petition at 10.

and Emergency Ratings."[14] We find that the above provisions adequately address the Commission's directive in Order No. 693. Further, the language of Requirements R2.4.2 and R3.4.2 of FAC-008-3 is beneficial because it makes clear that applicable entities must develop documented methods for calculating normal ratings and, separately, emergency ratings; a distinction that may have been somewhat blurred in the past.

B. Methodology Options for Specific Types of Equipment

18. NERC states in its petition that proposed FAC-008-3, Requirement R3.1 achieves the Commission's Order No. 693 directive that *facility ratings* be based on a "methodology chosen by a facility owner be consistent with industry standards developed through an open process such as IEEE or CIGRE."[15] A facility rating is determined by the individual equipment rating of the most limiting element that comprises that facility.[16] Requirement R3.1 provides:

> The methodology used to establish the Ratings of the equipment that comprises the Facility shall be consistent with at least one of the following:
>
> • Ratings provided by equipment manufacturers or obtained from equipment manufacturer specifications such as nameplate rating.

[14] NERC defines Normal Rating as "[t]he rating as defined by the equipment owner that specifies the level of electrical loading, usually expressed in megawatts (MW) or other appropriate units that a system, facility, or element can support or withstand through the daily demand cycles without loss of equipment life." NERC defines Emergency Rating as "[t]he rating as defined by the equipment owner that specifies the level of electrical loading or output, usually expressed in megawatts (MW) or Mvar or other appropriate units, that a system, facility, or element can support, produce, or withstand for a finite period. The rating assumes acceptable loss of equipment life or other physical or safety limitations for the equipment involved." *NERC Glossary* at 17 and 28.

[15] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 742.

[16] *See* FAC-008-3, Requirement R3.3. Requirement R3.3 provides that the transmission owner's documented methodology for determining facility ratings must include a statement that "a Facility Rating shall respect the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility."

> • One or more industry standards developed through an open process such as Institute of Electrical and Electronics Engineers (IEEE) or International Council on Large Electric Systems (CIGRE).
>
> • A practice that has been verified by testing, performance history or engineering analysis.

The Commission believes that Requirement R3 adequately satisfies the Commission's directive in Order No. 693, however, there is one potential application of the new provision that is worthy of discussion. In particular, Requirement R3 allows an applicable entity to determine equipment ratings using manufacturer nameplate ratings, which ratings reflect the manufacturer's design conditions. With regard to the option of using nameplate ratings for setting an equipment rating under Requirement R3.1, the Commission notes that the ERO issued a recommendation to consider actual field conditions when determining facility ratings for transmission facilities in its October 7, 2010 Alert titled "Consideration of Actual Field Conditions in Determination of Facility Ratings."[17] This Alert recommends that recipients review their current facility ratings methodology for their solely and jointly owned transmission lines to verify that the methodology used to determine facility ratings is based on actual field conditions. The Alert further recommends that entities should determine if their facility ratings methodology will produce appropriate ratings, even when considering differences between design and actual field conditions.

C. Request for Facility Ratings Data

19. In their comments, the ITC Companies raise a concern regarding Sub-requirement R8.1, which requires transmission owners and certain generator owners to provide facility ratings and the identity of the most limiting equipment of the facilities, "as scheduled by the requesting entities." The ITC Companies believe the language "as scheduled by the requesting entities" is too open-ended such that there could be repeated and frequent requests for this data. The ITC Companies state this could result in burdensome "nuisance" data requests. The ITC Companies propose revising Sub-requirement R8.1 to make the schedule for ratings requests be mutually agreed between requester and the transmission owner or generator owner rather than solely the requester's schedule.

20. The Commission notes that the phrase "as scheduled by the requesting entities" is virtually identical to language in Requirement R2 of currently effective Reliability

[17] The October 7, 2010 Alert is *available on-line at:* http://www.nerc.com/fileUploads/File/Events%20Analysis/Ratings_Recommendation_to_Industry_20100929Final.pdf.

Standard FAC-009-1,[18] which requires transmission owners and generator owners to provide facility ratings "as scheduled by such requesting entities." Requirement R2 of FAC-009-1 has been in effect since October 2006,[19] and the Commission is not aware that the use of similar language in FAC-009-1, Requirement 2 has been a source of concern for applicable entities. [20] Thus, we are not persuaded by ITC Companies' pleading that FAC-008-3, Sub-requirement R8.1 will result in an unreasonable or unmanageable number of requests for facility ratings or the identity of limiting equipment.

21. Based on the foregoing, the Commission finds that Reliability Standard FAC-008-3 is just, reasonable, not unduly discriminatory or preferential, and in the public interest. Accordingly, the Commission approves Reliability Standard FAC-008-3. As requested by NERC, Reliability Standard FAC-008-3 will be effective on the first day of the first calendar quarter twelve months following the date of this order. Concurrent with the effective date of FAC-008-3, Reliability Standards FAC-008-1 and FAC-009-1 shall retire.

D. VRFs and VSLs

22. The Commission also finds that the VSLs assigned to the Reliability Standard FAC-008-3 Requirements are consistent with the Commission's established guidelines

---

[18] FAC-009-1, Requirement 2 provides:

> R2. The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities.

[19] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 773-774.

[20] Based on the development record for FAC-008-3 provided by NERC, it does not appear that the ITC Companies or any other stakeholder raised this issue during the comment periods. The ITC Companies cast affirmative votes to approve FAC-008-3, without comment, in both the initial ballot (April 21, 2011 to May 2, 2011) and the recirculation ballot (May 12, 2011 to May 23, 2011). *See* NERC Petition, Exhibit E at 845 and 1010.

for review of proposed VSLs.[21] With respect to the VRF assignments, the Commission approves NERC's proposed VRF designations for FAC-008-3, subject to one modification discussed below.

23. The Commission agrees that the VRFs assigned to FAC-008-3, Requirements R4 through R8 are carried forward from and match the approved VRFs for the corresponding Requirements from Reliability Standards FAC-008-1 and FAC-009-1.[22] However, as NERC explained in its filing, while Requirements R1 through R3 of FAC-008-3 correspond to Requirement R1 of currently effective Reliability Standard FAC-008-1, they do not directly align. Thus, NERC developed VRFs for proposed FAC-008-3, Requirements R1 through R3 that vary from the currently approved VRFs assigned to FAC-008-1, Requirement 1 and its sub-requirements. NERC proposes to assign Requirements R1 and R2 a VRF of "Lower," and to assign Requirement 3 a VRF of "Medium."

24. We agree with the "Lower" VRF for Requirement R1 and the "Medium" VRF for Requirement R3. However, we reject NERC's proposed "Lower" VRF for FAC-008-3, Requirement R2. Unlike FAC-008-3, Requirement R1, which applies, generally, to generator facilities behind the main step up transformer,[23] Requirement R2 applies to radial feed facilities which are more likely than "behind-the-transformer" generator facilities to directly affect the electric state of the bulk electric system. Further, while Requirement R1 is a documentation-only requirement, Requirement R2 imposes more than documentation requirements. Specifically, Requirement R2 mandates the provision of the underlying assumptions and methods used to determine the equipment ratings (Sub-requirement R2.2) and the process for determining the equipment rating (Sub-requirement R2.4). Thus, Requirement R2 while a planning requirement is not merely administrative in nature. It therefore falls outside of NERC's definition of "Lower Risk Requirements," which defines a "Lower" Requirement as one that is "administrative in

[21] *See North American Electric Reliability Corp.*, 123 FERC ¶ 61,284, at P 20-35, *order on reh'g & compliance*, 125 FERC ¶ 61,212 (2008) (VSL Guidance Order).

[22] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,145, *order on reh'g*, 120 FERC ¶ 61,145, at P 8-13 (2007) (VRF Guidance Order).

[23] Specifically, Requirement R1 applies to generator facilities up to the low side terminals of the main step up transformer if the generator owner does not own the main step up transformer, and the high side terminals of the main step up transformer if the generator owner owns the main step up transformer.

nature."[24] The Commission's VRF guidelines require consistency with NERC's definition of the VRF level. Accordingly, the Commission directs the ERO to modify the VRF assignment for FAC-008-3, Requirement R2 to "medium" and to submit the modification in a compliance filing within 60 days from the date this order issues.

The Commission orders:

(A) Reliability Standard FAC-008-3, the assigned VSLs, and the implementation plan proposed by NERC are approved, as discussed in this order.

(B) Reliability Standards FAC-008-1 and FAC-009-1 shall be retired upon the effective date of Reliability Standard FAC-008-3, as discussed in the body of this order.

(C) The VRF assignments for Reliability Standard FAC-008-3, Requirements R1, and R3 through R8 are approved. The Commission directs the ERO to modify the VRF for Requirement R2 as discussed in this order.

---

[24] The approved NERC definition for a "lower" VRF designation is as follows:

> Lower Risk Requirement: is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to effectively monitor and control the Bulk-Power System; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to effectively monitor, control, or restore the Bulk-Power System.

See North American Electric Reliability Corporation, 119 FERC ¶ 61,145, at P 9, *order on compliance,* 121 FERC ¶ 61,179, at P 2 and Appendix A (2007).

(D) NERC is directed to file a compliance filing within 60 days of the date of this order, as discussed in the body of this order.

By the Commission. Commissioner Spitzer is not participating.

(S E A L)

Kimberly D. Bose,
Secretary.

From: Margaret Mayora
To: grpStaff
Subject: Fw: Recent FERC Reliability Issuances
Date: Friday, November 25, 2011 12:22:15 PM

Fyi.

----- Original Message -----
From: McCarthy, Catherine P. <CMcCarthy@deweyleboeuf.com>
To: cmccarthy@deweyleboeuf.com
Sent: Wed Nov 23 11:55:36 2011
Subject: Recent FERC Reliability Issuances

1. Order Approving Reliability Standard (RD11-10)

A November 17, 2011, FERC approved reliability standards dealing with Facility Ratings and Facility Ratings Methodology. NERC petitioned FERC requesting approval of Reliability Standard FAC-008-3 (Facility Ratings), the associated Violation Risk Factors (VRF) and Violation Severity Levels (VSL), and retirement of Reliability Standards FAC-008-1 (Facility Ratings Methodology) and FAC-009-1 (Establish and Communicate Facility Ratings). Reliability Standard FAC-008-3 creates requirements that obligate transmission owners and generator owners to develop facility ratings methodologies for their facilities.

http://elibrary.ferc.gov/idmws/File_list.asp?document_id=13971989

BACKGROUND: On June 15, 2011, NERC filed a petition requesting approval of Reliability Standard FAC-008-3, the associated VRFs and VSLs for this Reliability Standard, and retirement of Reliability Standards FAC-008-1 and FAC-009-1. NERC states that it developed Reliability Standard FAC-008-3 using the NERC Reliability Standards Development Procedure, and further states that FAC-008-3 addresses all three Commission directives from Order No. 693. Proposed Reliability Standard FAC-008-3 was approved by the NERC Board of Trustees.

2. Order Approving Reliability Standard (RD11-3)

A November 17, 2011 FERC Order approved reliability standard FAC-103-12, dealing with the Assessment of Transfer Capability for the Near-Term Transmission Plan Horizon. FERC also found that the violation risk factors (VRFs) assigned to the requirements are consistent with the Commission's established guidelines and approved them as filed. However, FERC found that NERC has not adequately justified its proposed "lower" VRF designation for certain requirements and directed NERC to provide additional justification for these VRF designations or to propose a revised VRF designation responding to FERC's concerns.

http://elibrary.ferc.gov/idmws/File_list.asp?document_id=13972009

BACKGROUND: On January 28, 2011, NERC submitted a petition seeking approval of a revised Facilities Design, Connections, and Maintenance (FAC) Reliability Standard FAC-013-2 – Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon, pursuant to section 215(d)(1) of the Federal Power Act (FPA) and section 39.5 of the Commission's regulations. The revised Reliability Standard requires planning coordinators to have a transparent methodology for, and to annually perform, an assessment of transmission transfer capability for the Near-Term Transmission Planning Horizon, as a basis for identifying system weaknesses or limiting facilities that could limit energy transfers in the future. NERC also requested approval of two new terms utilized in the proposed Reliability Standard, to be included in NERC's Glossary of Terms Used in NERC Reliability Standards (NERC Glossary or Glossary). Finally, NERC requested approval of its implementation plan for Reliability Standard FAC-013-2, setting an effective date that will allow planning coordinators a reasonable time, after certain related Modeling, Data, and Analysis (MOD) Reliability Standards have gone into effect, to meet the requirements of the revised Reliability Standard.

3. Order Approving Amendment to Rules of Procedure (RR11-5)

On November 17, 2011, FERC issued an Order Approving NERC's Proposed Amendments to Rules of Procedure.

http://elibrary.ferc.gov/idmws/File_list.asp?document_id=13972021

BACKGROUND: On June 14, 2011, NERC sought FERC approval for amendments to the NERC Rules of Procedure. The Appendix 3B Election Procedure for Members of NERC Standards Committee includes procedures used to facilitate the election of industry stakeholder segment representatives to the Standards Committee. The NERC Standards Committee consists of two representatives from the following industry segments: (1) Transmission Owners; (2) RTOs and ISOs; (3) Load-Serving Entities; (4) Transmission Dependent Utilities; (5) Electric Generators; (6) Electricity Brokers, Aggregators, and Marketers; (7) Large Electricity End Users; (8) Small Electricity Users; (9) Federal, State, and Provincial Regulatory or other Government Entities; and (10) Regional Entities. The proposed amendments would: (1) require the Chair and Vice Chair of the Standards Committee to serve as non-voting members; (2) require a Canadian representative on the Standards Committee to be either a company or association incorporated in Canada; an agency of a federal, provincial, or local government in Canada; or any person with Canadian citizenship who is residing in Canada; and (3) simplify the process of filling vacant Standards Committee positions by eliminating the need to collect and hold a ratification vote. The purpose of these amendments is to eliminate potential conflicts of interest for elected officers of the Standards Committee, increase the likelihood that Canadian representatives are familiar with Canadian issues, and improve efficiency by shortening vacancies on the Standards Committee.

4. Order Denying Rehearing and Partially Granting Clarification (RC11-1; RC11-2)

On November 17, 2011, FERC issued an Order Denying Rehearing and Partially Granting Clarification with respect to Cedar Creek Wind Energy LLC and Milford Wind Corridor Phase I, LLC. FERC affirmed its earlier holding that Cedar Creek and Milford Wind were properly included on the NERC Compliance Registry as transmission owners and transmission operators. Several entities that filed requests for rehearing argued that there was no factual support that the generator lines were material to Bulk-Power System reliability. FERC stated that applying the fact-specific analysis used in the June 16th Order, the reliable operation and maintenance of the interconnection facilities connected to Cedar Creek and Milford generating facilities were material to the reliability of the Bulk-Power System.

http://elibrary.ferc.gov/idmws/File_list.asp?document_id=13972082

BACKGROUND: On July 18, 2011, NERC submitted a request for clarification, or in the alternative, rehearing with regard to the June 16, 2011 Order which denied the appeals of Cedar Creek Wind Energy, LLC and Milford Wind Corridor Phase I, LLC ("Milford") of their registration as transmission owners ("TO") and transmission operators ("TOP").

On June 16, 2011, the Commission denied the appeals of two registry decisions in which NERC found that two wind generators, Cedar Creek and Milford, were properly included on the NERC Compliance Registry as transmission owners and transmission operators. Although the ruling is specific to Cedar Creek and Milford, FERC encouraged NERC to work on an approach that would provide guidance on when generators must register as a transmission owner and operator. WECC registered Cedar Creek and Milford as transmission owners and transmission operators. Cedar Creek and Milford appealed WECC's decisions to NERC, arguing that their respective tie-line facilities do not fall within NERC's registration criteria as transmission owners and operators. The Commission denied the appeals and affirmed NERC's registry decisions. FERC found that the wind generators operated high voltage tie-lines that moved power from the generating facility to a central switching station and that these lines were material to the bulk power system reliability. On October 6, 2010, NERC upheld WECC's registration of Cedar Creek as a transmission owner and operator. NERC explained that Cedar Creek meets the requirements of the Registry Criteria. In a separate October 6, 2010, decision, NERC upheld WECC's registration of Milford as a transmission owner and operator. NERC concluded that Milford meets the Registry Criteria requirements for owning and operating an integrated transmission element associated with the Bulk-Power System 100 kV or above. On October 27, 2010, Milford filed its request for appeal of the NERC's Milford Decision.

http://elibrary.ferc.gov/idmws/File_list.asp?document_id=13939112

Catherine P. McCarthy

Partner

Dewey & LeBoeuf LLP

1101 New York Avenue, N.W.

Washington, D.C. 20005

Direct: +1 202 346 8753

General: +1 202 346 8000

Fax: +1 202 346 8102

cmccarthy@dl.com <mailto:cmccarthy@dl.com>

www.dl.com <http://www.dl.com>

==========

Pursuant to U.S. Treasury Department Circular 230, unless we expressly state otherwise, any tax advice contained in this communication (including any attachments) was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties or (ii) promoting, marketing or recommending to another party any matter(s) addressed herein.

Dewey & LeBoeuf LLP in London and Paris is a limited liability partnership registered in England and Wales under number OC355432 with its registered office at 1 Minster Court, Mincing Lane, London EC3R 7YL and is a law firm authorised and regulated by the Solicitors Regulation Authority. We use the word "partner" to refer to a member of the LLP, or an employee or consultant who is a lawyer with equivalent standing and qualifications. A list of the members of Dewey & LeBoeuf LLP and of the non-members who are designated as partners is available for inspection at the above address. Further important information about Dewey & LeBoeuf can be found on www.dl.com.

Dewey & LeBoeuf LLP in Doha is licensed by the Qatar Financial Centre Authority, QFC License Number 00102.

Dewey & LeBoeuf LLP in Dubai is licensed by the Dubai Financial Services Authority, DFSA Reference No. F000755.

This e-mail message, including attachments, is confidential, is intended only for the named recipient(s) above and may contain information that is privileged, attorney work product, proprietary or exempt from disclosure under applicable law. The unauthorized use, dissemination, distribution or reproduction of this e-mail message, including attachments, is strictly prohibited. If you have received this message in error, or are not an intended recipient, please immediately notify the sender and delete this e-mail message, including attachments, from your computer. Thank you.

==========

[Federal Register Volume 76, Number 207 (Wednesday, October 26, 2011)]
[Proposed Rules]
[Pages 66229-66235]
From the Federal Register Online via the Government Printing Office [www.gpo.gov]
[FR Doc No: 2011-27624]

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM11-18-000]

Transmission Planning Reliability Standards

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Notice of proposed rulemaking.

SUMMARY: Transmission Planning (TPL) Reliability Standards are intended to ensure that the transmission system is planned and designed to meet an appropriate and specific set of reliability criteria. Reliability Standard TPL-002-0a references a table which identifies different categories of contingencies and allowable system impacts in the planning process. The table includes a footnote regarding planned or controlled interruption of electric supply where a single contingency occurs on a transmission system. North American Electric Reliability Corporation (NERC), the Commission-certified Electric

[[Page 66230]]

Reliability Organization, requests approval of a revision to the footnote. In this notice, the Commission proposes to remand NERC's proposed revision to the footnote.

DATES: Comments are due December 27, 2011.

ADDRESSES: You may submit comments, identified by docket number by any of the following methods:

Agency Web Site: http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.

Mail/Hand Delivery: Commenters unable to file comments electronically must mail or hand deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE., Washington, DC 20426.

FOR FURTHER INFORMATION CONTACT:

Robert T. Stroh (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, Telephone: (202) 502-8473.
Eugene Blick (Technical Information), Office of Electric Reliability, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, Telephone: (202) 502-8066.

SUPPLEMENTARY INFORMATION:

Notice of Proposed Rulemaking

October 20, 2011.

1. On March 31, 2011, the North American Electric Reliability Corporation (NERC) filed a petition seeking approval of Table 1, footnote `b' of four Reliability Standards: Transmission Planning: TPL-001-1--System Performance Under Normal (No Contingency) Conditions (Category A), TPL-002-1b--System Performance Following Loss of a Single Bulk Electric System Element (Category B), TPL-003-1a--System Performance Following Loss of Two or More Bulk Electric System Elements (Category C), and TPL-004-1- System Performance Following Extreme Events Resulting in the Loss of Two or More Bulk Electric System Elements (Category D).\1\ Pursuant to section 215(d)(4) of the Federal Power Act (FPA) \2\, the Commission proposes to remand the proposed Table 1, footnote b. As discussed below, the Commission believes that

the proposed Reliability Standard does not meet the statutory criteria for approval that it be just, reasonable, not unduly discriminatory or preferential, and in the public interest.\3\ The Commission seeks comments on its proposal.

\1\ While footnote `b' appears in all four of the above referenced TPL Reliability Standards, its relevance and practical applicability is limited to TPL-002-0a.

\2\ 18 U.S.C. 824o(d)(4) (2006).

\3\ 16 U.S.C. 824o(d)(2) (2006).

I. Background

2. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Approved Reliability Standards are enforced by the ERO, subject to Commission oversight, or by the Commission independently.

3. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO \4\ and, subsequently, certified NERC as the ERO.\5\ On March 16, 2007, the Commission issued Order No. 693, approving 83 of the 107 Reliability Standards filed by NERC, including Reliability Standard TPL-002-0, Table 1, footnote `b.' \6\ In addition, pursuant to section 215(d)(5) of the FPA,\7\ the Commission directed NERC to develop modifications to 56 of the 83 approved Reliability Standards, including footnote `b' of Reliability Standard TPL-002-0.\8\

\4\ Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, Order No. 672, FERC Stats. & Regs.] 31,204, order on reh'g, Order No. 672-A, FERC Stats. & Regs.] 31,212 (2006).

\5\ North American Electric Reliability Corp., 116 FERC] 61,062, order on reh'g & compliance, 117 FERC] 61,126 (2006), aff'd sub nom., Alcoa, Inc. v. FERC, 564 F.3d 1342 (D.C. Cir. 2009).

\6\ Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, FERC Stats. & Regs.] 31,242, order on reh'g, Order No. 693-A, 120 FERC] 61,053 (2007).

\7\ 16 U.S.C. 824o(d)(5)(2006).

\8\ Order No. 693, FERC Stats & Regs.] 31,242 at P 1797.

A. Transmission Planning (TPL) Reliability Standards

4. Currently-effective Reliability Standard TPL-002-0a addresses Bulk-Power System planning and related system performance for single element contingency conditions. Requirement R1 of TPL-002-0a requires that each Planning Authority and Transmission Planner ``demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I.'' \9\ Table I identifies different categories of contingencies and allowable system impacts in the planning process. With regard to system impacts, Table I further provides that a Category B (single) contingency must not result in cascading outages, loss of demand or curtailed firm transfers, system instability or exceeded voltage or thermal limits. With regard to the clause regarding loss of demand, current footnote `b' of Table 1 states:

\9\ Reliability Standard TPL-002-0a, Requirement R1.

Planned or controlled interruption of electric supply to radial customers or some local Network customers, connected to or supplied by the Faulted element or by the affected area, may occur in certain areas without impacting the overall reliability of the interconnected transmission systems. To prepare for the next contingency, system adjustments are permitted, including curtailments of contracted Firm (non-recallable reserved) electric power Transfers.

B. Order No. 693 Directive

5. In Order No. 693, the Commission stated that it believes that the transmission planning Reliability Standard should not allow an

entity to plan for the loss of non-consequential firm load in the event of a single contingency.\10\ The Commission directed the ERO to develop certain modifications, including a clarification of Table 1, footnote `b'. The Commission stated that:

\10\ See Order No. 693, FERC Stats. & Regs.] 31,242 at P 1794. Non-consequential load loss includes the removal, by any means, of any planned firm load that is not directly served by the elements that are removed from service as a result of the contingency. Currently-effective footnote `b' deals with both consequential load loss and non-consequential load loss. NERC's proposed footnote `b' characterizes both types of load loss as ``Firm Demand.'' The focus of this NOPR is NERC's proposed treatment of non-consequential load loss or planned interruption of ``Firm Demand.''

Based on the record before us, we believe that the transmission planning Reliability Standard should not allow an entity to plan for the loss of non-consequential load in the event of a single contingency. The Commission directs the ERO to clarify the Reliability Standard. Regarding the comments of Entergy and Northern Indiana that the Reliability Standard should allow entities to plan for the loss of firm service for a single contingency, the Commission finds that their comments may be considered through the Reliability Standards development process. However, we strongly discourage an approach that reflects the lowest common denominator. The Commission also clarifies that an entity may seek a regional difference to the Reliability Standard from the ERO for case-specific circumstances.\11\

\11\ Order No. 693, FERC Stats. & Regs.] 31,242 at P 1794 (footnotes omitted).

[[Page 66231]]

6. In a subsequent clarifying order, the Commission stated that it believed that a regional difference, or a case-specific exception process that can be technically justified, to plan for the loss of firm service ``at the fringes of various systems'' would be an acceptable approach in limited circumstances.\12\ Specifically, the Commission clarified that:

\12\ Mandatory Reliability Standards for the Bulk Power System, 131 FERC] 61,231, at P 21 (2010) (June 2010 Order).

Moreover, the Commission, in * * * Order No. 693, then provided a clarification that an entity may seek a regional difference to the Reliability Standard from the ERO for case-specific circumstances. We believe that a regional difference, or a case-specific exception process that can be technically justified, to plan for the loss of firm service ``at the fringes of various systems'' would be an acceptable approach. Thus, the Commission did not dictate a single solution as NERC and others now claim. In any event, NERC must provide a strong technical justification for its proposal.\13\

\13\ Id.

C. NERC's Petition for Approval of TPL-002-0a, Footnote b

7. On March 31, 2011, NERC filed a petition seeking approval of its proposal to revise and clarify footnote `b' ``in regard to load loss following a single contingency.'' \14\ NERC stated that it did not eliminate the ability of an entity to plan for the loss of non-consequential load in the event of a single contingency but drafted a footnote that, according to NERC, ``meets the Commission's directive while simultaneously meeting the needs of industry and respecting jurisdictional bounds.'' \15\ NERC states that its proposed footnote `b' establishes the requirements for the limited circumstances when and how an entity can plan to interrupt Firm Demand for Category B contingencies. It allows for planned interruption of Firm Demand when ``subject to review in an open and transparent stakeholder process.'' \16\ NERC's proposed footnote `b' states:

\14\ NERC Petition at 10.

\15\ Id.
\16\ Id.

An objective of the planning process should be to minimize the likelihood and magnitude of interruption of firm transfers or Firm Demand following Contingency events. Curtailment of firm transfers is allowed when achieved through the appropriate redispatch of resources obligated to re-dispatch, where it can be demonstrated that Facilities, internal and external to the Transmission Planner's planning region, remain within applicable Facility Ratings and the re-dispatch does not result in the shedding of any Firm Demand. It is recognized that Firm Demand will be interrupted if it is: (1) Directly served by the Elements removed from service as a result of the Contingency, or (2) Interruptible Demand or Demand-Side Management Load. Furthermore, in limited circumstances Firm Demand may need to be interrupted to address BES performance requirements. When interruption of Firm Demand is utilized within the planning process to address [Bulk Electric System] performance requirements, such interruption is limited to circumstances where the use of Demand interruption are documented, including alternatives evaluated; and where the Demand interruption is subject to review in an open and transparent stakeholder process that includes addressing stakeholder comments.

D. Supplemental Information

8. On June 7, 2011, in response to a Commission deficiency letter, NERC explained that ``the approach proposed in footnote `b' is equally efficient because many of the stakeholder processes that will be used in footnote `b' planning decisions are already in place, as implemented by FERC in Order No. 890 and in state regulatory jurisdictions.'' \17\ NERC also pointed to state public utility commission processes or processes existing in local jurisdictions that address transmission planning issues that could serve to provide a case-specific review of the planned interruption of Firm Demand. NERC added that an ERO-sponsored planning process is not likely to be efficient or effective because of extensive jurisdictional issues between NERC, the Commission, and the many authorities having jurisdiction that would have to be resolved before implementation could occur. NERC added that an ERO-specific process would lead to conflicts among federal, provincial, state and local governing bodies that have jurisdiction over various parts of the planning, siting and construction process. NERC also believes that a NERC-centered process would duplicate planning actions occurring elsewhere (e.g., where resource allocation decisions are actually being made), and such a process could lead to inconsistent results. NERC concluded that a more reasonable and expeditious path would be to rely on existing stakeholder processes. According to NERC, such processes would more likely engage the appropriate local-level decision-makers and policy-makers.

\17\ NERC Data Response at 4.

---

9. With respect to review and oversight by NERC and the Regional Entities, NERC submitted that an ERO-specific process would place the ERO in the position of managing and actively participating in a planning process, which conflicts with its role as the compliance monitor and enforcement authority. NERC also stated that neither the ERO nor the Regional Entities will review decisions regarding planned interruptions. Their role will be limited to reviewing whether the registered entity participated in a stakeholder process when planning to interrupt Firm Demand. NERC explained that Regional Entities will have oversight after-the-fact by auditing the entity's implementation of footnote `b' to determine if the entity planned on interrupting Firm Demand and whether the decision by the entity to rely on planned interruption of Firm Demand was vetted through the stakeholder process and qualified as one of the situations identified in footnote b.

10. Furthermore, NERC stated that an objective of the planning process should be to minimize the likelihood and magnitude of planned Firm Demand interruptions. NERC recognizes that there may be topological or system configurations where allowing planned interruptions of Firm Demand may provide more reliable service. NERC contends that due to the wide variety of system configurations and regulatory compacts, it is not feasible for the ERO to develop a one-size-fits-all criterion for limiting the planned firm load interruptions for Category B events. According to NERC, the standards drafting team evaluated setting a certain magnitude of planned interruption of Firm Demand, but there was no analytical data to support a single value, and it would be viewed as arbitrary.

II. Discussion

11. The Commission proposes to remand NERC's proposal to modify Reliability Standard TPL-002-0a, Table 1, footnote `b.' The Commission believes that NERC's proposal does not meet the directives in Order No. 693 and the June 2010 Order and does not clarify or define the circumstances in which an entity can plan to interrupt Firm Demand for a single contingency. Specifically, the Commission is concerned that the procedural and substantive parameters of NERC's proposed stakeholder process are too undefined to provide assurances that the process will be effective in determining when it is appropriate to plan for interrupting Firm Demand, does not contain NERC-defined criteria on circumstances to determine when an exception for planned interruption of Firm Demand is permissible, and could result in inconsistent results in implementation. In proposing a stakeholder process without specification of any technical means by which exceptions are to be evaluated,

[[Page 66232]]

the proposed footnote effectively turns the processes into a reliability standards development process outside of NERC's existing procedures. Furthermore, the Commission believes that regardless of the process used, the result could lead to inconsistent reliability requirements within and across reliability regions. While the Commission recognizes that some variation among regions or entities is reasonable given varying grid topography and other legitimate considerations, there are no technical or other criteria to determine whether varied results are arbitrary or based on meaningful distinctions. While the Commission acknowledges that NERC has flexibility in developing alternative approaches, we believe that the proposed approach is not equally efficient or effective as the Commission's directives and that NERC has failed to provide a strong technical justification for its proposal.

12. As an initial matter, the Commission is concerned that the process lacks parameters. The standard requires that, when planning to interrupt Firm Demand, the Firm Demand interruption must be ``subject to review in an open and transparent stakeholder process that includes addressing stakeholder comments.'' \18\ However, without any substantive parameters governing the stakeholder process, the enforceability of this obligation by NERC and the Regional Entities' would be limited to a review to ensure only that a stakeholder process occurred. Indeed, NERC's explanation appears to confirm this concern, as NERC explained that Regional Entities' involvement is limited to oversight after-the-fact by auditing the entity's implementation of footnote `b' to determine if the entity planned on interrupting Firm Demand and whether the decision by the entity to rely on planned interruption of Firm Demand was vetted through the stakeholder process and qualified as one of the situations identified in footnote `b'.

\18\ NERC Petition at 10.

---

13. Further, the Commission is concerned that the NERC proposal leaves undefined the circumstances in which it is allowable to plan for Firm Demand to be interrupted in response to a Category B contingency. The TPL-002-0a Reliability Standard requires Planning Authorities and Transmission Planners to demonstrate through a valid assessment that the transmission system is planned and can be operated to supply projected Firm Demand at all demand levels over a range of forecasted system demands.\19\ Moreover, the planner must consider all single contingencies applicable to Table I, Category B and demonstrate that system performance is met. For those instances where system performance is not met, the planner must provide a written summary of its plans to achieve system performance including implementation schedules, in service dates of facilities and implementation lead times.\20\ In regard to NERC's proposal, the Commission is concerned that footnote `b' would function as a means to override the reliability objective and system performance requirements of the TPL Reliability Standard without any technical or other criteria specified to determine when planning to interrupt Firm Demand would be allowable. In this case NERC has provided no technically sound means of determining situations in which planning to interrupt Firm Demand would be allowable, and instead has removed such decision-making to an unspecified stakeholder process without any assurance that such processes will deploy technically sound means of approving or denying exceptions. Without any technical or other criteria specified to determine when planning to interrupt Firm Demand would be allowable, the Commission is concerned that multiple stakeholder processes across the country engaging in such determinations could lead to inconsistent and arbitrary exceptions

including, potentially, allowing entities to plan to interrupt any amount of Firm Demand in any location and at any voltage level. While the Commission recognizes that some variation among regions or entities is reasonable given varying grid topography and other legitimate considerations, there are no technical or other criteria to determine whether varied results are arbitrary or based on meaningful distinctions. The Commission is thus concerned that there may be a lack of consistency in determinations to allow the planned interruption of Firm Demand. The proposed stakeholder process does not have any parameters except for openness and transparency. As a result, multiple processes that could be adopted across the country would likely lead to inconsistent determinations to allow for the planned interruption of Firm Demand.

\19\ Reliability Standard TPL-002-0a, Requirement R1.
\20\ Reliability Standard TPL-002-0a, Requirements R1.5 and R2.

---

14. The Commission believes that a remand would give NERC and industry flexibility to develop an approach that would address the issues identified by the Commission with the proposed footnote `b' stakeholder process including, as discussed below, definition of the process and criteria or guidelines for the process.

A. Lack of Technical or Other Criteria

15. NERC's proposal does not prescribe the criteria that would define the parameters of permissible interruption of Firm Demand. In Order No. 693 the Commission expressed concern that, as a general rule, footnote `b' should not allow an entity to plan for the loss of non-consequential load in the event of a single contingency and directed NERC to clarify the standard. The Commission stated in the June 2010 Order that a regional difference or a case-specific exception process that could be technically justified would be acceptable. While the Commission allows NERC to propose an equally effective and efficient solution to a Commission's proposed solution, the Commission does not believe that the proposal is equally effective and efficient. First, NERC's proposed footnote `b' contains no constraints and could allow an entity to plan to interrupt any amount of Firm Demand, in any location or at any voltage level as needed for any single contingency, provided that it is documented and subjected to a stakeholder process. This result is contrary to the underlying standard and our prior orders.\21\ Further, NERC did not technically justify its proposal, instead relying on the benefit of having transparency in the process. The Commission does not believe transparency in this instance can substitute for a technical justification.

\21\ See Order No. 693, see also June 2010 Order.

---

16. In its supplemental filing, NERC states that it is not feasible for the ERO to develop a one-size-fits-all criterion for limiting the planned interruption of Firm Demand due to the wide variety of system configurations and regulatory compacts.\22\ NERC states that the standards drafting team believes there is no analytical data to support a single level and therefore any single value was viewed as arbitrary.

\22\ NERC Data Response at 6.

---

17. We are not persuaded by NERC's reasoning. First, both NERC and the Commission have developed thresholds in other reliability contexts that have overcome similar claims of arbitrariness. For example, the threshold for conducting vegetation management pursuant to Reliability Standard FAC-003-1 applies to all transmission lines operated at 200 kV and above.\23\ In the

[[Page 66233]]

same vein, NERC's Statement of Compliance Registry Criteria has numerous thresholds for determining eligibility for registration.\24\ The Commission did not suggest a one size fits all exceptions process. If the ERO were to perform an exception process, it might include flexibility in decisions based on disparate topology or on other matters since it could utilize its technical expertise to determine the reliability impact from one region to another. Moreover, the Commission's proposal to remand revised footnote `b' due to a lack of criteria does not preclude NERC from developing another alternative,

provided that it is equally ``efficient and effective.''

\23\ Reliability Standard FAC-003-1.

\24\ See, e.g., NERC Statement of Registry Criteria, Section III. The Commission approved Statement of Registry Criteria in Order No. 693.

18. Finally, the Commission understands that there are a wide variety of system configurations and regulatory compacts. NERC indicates that the standards drafting team considered a variety of limits; however, it is not clear whether NERC considered a blend of quantitative and qualitative thresholds. For example, a standard could require a process with a quantitative limitation on how much Firm Demand could be planned for interruption and that standard could provide an exception process where a registered entity would submit documents and explanation to the ERO or a Regional Entity for approval based upon certain considerations.\25\ In short, we believe that a more defined process would be needed but, by itself, would not be adequate without NERC-defined technical or other criteria to determine planned interruption of Firm Demand. The Commission seeks comment on these proposals.

\25\ While we encourage NERC to exercise flexibility in designing an appropriate standard, under this example, the exception process could consist of a stakeholder process that has some level of due process as long as that process does not allow the entity that proposes its exception to make the decision on whether to grant the exception.

B. Stakeholder Process

19. The Commission believes that NERC's proposed footnote `b' stakeholder process does not meet Order No. 693 and the June 2010 Order directive. According to NERC, the type of stakeholder process used under its proposed footnote `b' can vary from one planning entity to the next. NERC offers several stakeholder processes as examples, such as the Order 890-type process, a state public utility commission or local jurisdiction process, or a Regional Transmission Organization/ Independent System Operator (RTO/ISO) stakeholder process.

20. First, because NERC's proposed footnote `b' does not define the stakeholder process, the express terms of the standard would allow an applicable entity to form or participate in any stakeholder process and be compliant with the proposed standard. Second, as we have mentioned, NERC has offered no technical justification for exceptions to be granted through the stakeholder process and therefore no means for the Commission to judge whether the process will protect the reliability of the Bulk-Power System. Nothing in the proposed footnote `b' restricts the stakeholder process, other than that it must be an open and transparent stakeholder process that includes addressing stakeholder comments. The Commission is concerned that any meeting that is open to stakeholders could meet this standard. Further, because the stakeholder process is not defined, the proposal could allow a transmission planner to develop a process that provides insufficient process and transparency and still comply with the standard. The Commission believes that such process would be insufficient because it allows any stakeholder process to essentially become a reliability standards development processes outside of NERC's existing procedures. Furthermore, the Commission believes that regardless of the stakeholder process used, the outcome could lead to inconsistent results, with no technical or other criteria to determine whether varied results are arbitrary or based on meaningful distinctions. The Commission seeks comment on whether a stakeholder process is the appropriate vehicle to approve or deny exceptions to allow entities to plan to interrupt Firm Demand for a single contingency and if so, whether the proposed footnote `b' would require any stakeholder due process.

21. Nor does the standard describe what would be entailed in addressing the stakeholder comments. As described above, the process under the standard does not provide for any technical rigor to address stakeholder concerns. While the standard requires transparency and an opportunity for stakeholder comments on the transmission planner's proposed plan to interrupt Firm Demand, it does not mandate any particular stakeholder involvement, nor does it mandate that interested governmental authorities be afforded notice and an opportunity to comment. As we read the proposed standard, a responsible entity could define when it would plan to interrupt Firm Demand on its own, then ask for stakeholder input on that plan. While the standard requires the responsible entity to ``address'' stakeholder comments, the responsible

entity is not required to specify or support the technical basis upon which it rendered a decision. The Commission believes that the stakeholder process in proposed footnote `b' would allow the transmission planner to define the circumstances when it would rely on planned interruption of Firm Demand, provide that definition for review by regulators and other stakeholders, receive comments from regulators and stakeholders requesting a more narrow definition, and explain to the regulators and stakeholders why it is declining the request and maintaining the broader definition, even if every other transmission planner facing similar circumstances would reach the opposite conclusion.

22. In Order No. 693 and the June 2010 Order, the Commission stated that a regional difference or a case-specific exception process, among other things, would be an acceptable approach. With regard to a case-specific process, NERC replied it would ``create undesirable delays and uncertainty in the transmission planning process.'' \26\ However, the proposed footnote `b' does not provide a time limitation by which planning decisions to interrupt Firm Demand must be made. The Commission is not persuaded that NERC's proposed approach ameliorates this concern. The Commission seeks comment on whether an exceptions process that provides defined criteria, with some allowance or consideration for unique circumstances, could be crafted that would resolve NERC's concerns of ``undesirable delays'' and ``uncertainty.''

\26\ NERC Data Response at 2.

---

23. In sum, the Commission is concerned that the stakeholder process set forth in the NERC proposal is not sufficiently defined, rendering it potentially unenforceable. As mentioned above, the proposed stakeholder process includes no parameters other than openness and transparency. NERC states that it and the Regional Entities will review a responsible entity's decision to plan to interrupt Firm Demand using an after-the-fact audit, to determine if the entity's implementation of footnote `b' to plan Firm Demand interruption and whether the decision by the entity was vetted through the stakeholder process and qualified as one of the situations

[[Page 66234]]

identified in footnote `b.' \27\ The Commission believes that this could result in a transmission planner invoking a process that provides for minimal stakeholder involvement, providing scant reasons to reject any stakeholder input and then defending its decision by claiming that it has satisfied the provision. While the Compliance Enforcement Authority would verify that the process fulfilled the letter of NERC's proposed footnote `b'--that some open, transparent stakeholder process was involved and that the responsible entity in some way addressed stakeholder concerns--there is no mechanism for the ERO or a Regional Entity to enforce a finding that the evidence does not support an acceptable instance of planned interruption of Firm Demand. The Commission seeks comment on the concerns raised above.

\27\ NERC Data Response at 7-8.

C. Commission Proposal

24. The Commission believes that NERC's proposed footnote `b' does not meet the Commission's Order No. 693 directives, nor is it an equally effective and efficient alternative. On this basis, the Commission proposes to remand the proposal to NERC.

25. The Commission also proposes to provide further guidance on acceptable approaches to footnote `b'. We seek comment on all of the options below. In addition, while the Commission is proposing certain options for revising footnote `b', we also seek comment on other potential options to solve the concerns outlined in this NOPR. As noted above, the Commission understands that there are a wide variety of system configurations and regulatory compacts. We believe that a more defined process than that provided in the proposed footnote `b' would be needed but, by itself, would not be adequate without NERC-defined technical or other criteria to determine an acceptable planned interruption of Firm Demand at the fringes of the system.\28\

\28\ Any exceptions process to determine specific requests for planned interruption of Firm Demand may not necessarily be limited to the fringes of the system.

---

26. We acknowledge that the standards drafting team considered a variety of limits; however, setting some form of criteria within the standard itself for planning to interrupt Firm Demand may be an acceptable approach to setting criteria for footnote `b' and would be an option for NERC to consider. We also seek comment on whether existing protocols could provide guidance to NERC in devising criteria. For example, the Department of Energy's Electric Emergency Incident and Disturbance Report (Form OE-417) requires, among other things, an entity to report the uncontrolled loss of 300 Megawatts or more of firm system loads for more than 15 minutes from a single incident, load shedding of 100 Megawatts or more implemented under emergency operational policy, and the loss of service for more than 1 hour to 50,000 customers. While these are reporting requirements for the operational timeframe, and may include distribution level load shedding, the Commission requests comments on whether they could also serve as a basis for setting limits on when an entity can plan to interrupt Firm Demand on the Bulk-Power System. Another existing document that could provide guidance on how to set a limit on the planned interruption of Firm Demand is NERC's Statement of Compliance Registry Criteria, which uses, for example, 25 MW as a threshold in determining when a load-serving entity or distribution provider should register with NERC. We seek comments on this proposed option, and any other external documents that could be used to guide a revision to footnote `b.'

27. Second, as stated above, it is not clear whether NERC considered a blend of quantitative and qualitative thresholds. The Commission seeks comments on whether this would be an option for providing criteria that would be generally applicable, but also for allowing for certain cases that may exceed the criteria. For example, a standard could require a process with a quantitative limitation on how much Firm Demand could be planned for interruption and that standard could provide an exception process where a registered entity would submit documents and explanation to the ERO or a Regional Entity for approval based upon certain considerations. NERC has raised concerns about conflicts among federal, provincial, state and local governing bodies that have jurisdiction over various parts of the planning, siting and construction process. The Commission believes that this approach may satisfy the need for technical criteria that we have described, while accounting for NERC's concerns about the difficulty of developing a one-size-fits-all criterion for limiting planned Firm Demand interruptions and the appropriateness and feasibility of managing and actively participating in each planning process. As NERC states, the objective of footnote `b' should be to minimize the likelihood and magnitude of planned Firm Demand interruptions. The Commission believes that setting generally applicable criteria for when an applicable entity can plan to shed Firm Demand, coupled with an exceptions process overseen by NERC and the Regional Entities, could mean that few exception requests must be processed by NERC and the Regional Entities. We seek comment on this option, and which entities should be involved in the review and subsequent determination as to whether an exception should be allowed.

28. NERC has raised concerns about conflicts among federal, provincial, state and local governing bodies that have jurisdiction over various parts of the planning, siting and construction process. There also may be concerns about the costs of planning to avoid Firm Demand shedding. The Commission seeks comment on whether a feasible option would be to revise footnote `b' to allow for the planned interruption of Firm Demand in circumstances where the transmission planner can show that it has customer or community consent and there is no adverse impact to the Bulk-Power System. This presumably would not require affirmative consent by every individual retail customer, but we recognize that either term, customer or community, would need to be adequately defined. The Commission therefore seeks comments on who might be able to represent the customer or community in this option and how customer or community consent might be demonstrated. Additionally, we seek comment on how it would be determined that firm demand shedding with customer consent would not adversely impact the Bulk-Power System. However, we also seek comment on whether a customer who would otherwise consent to having its planning authority or transmission planner plan to interrupt Firm Demand pursuant to this option could instead select interruptible or conditional firm service under the tariff to address cost concerns.

29. Finally, regardless of how NERC revises footnote `b' to resolve the concerns outlined in this NOPR and in previous orders, the Commission notes that NERC will need to support the revision to footnote `b.' If there is a threshold component to the revised footnote, the Commission believes that NERC would need to support the threshold and show that instability, uncontrolled separation, or cascading failures of the system will not occur as a result of planning to shed Firm Demand up to the threshold. In addition, if there is an

individual exception option, the Commission

[[Page 66235]]

believes that the applicable entities should be required to find that there is no adverse impact to the Bulk-Power System from the exception and that it is considered in wide-area coordination and operations. Further, we believe that any exception should be subject to further review by the Regional Entity, NERC, and the Commission. This does not necessarily mean that the Regional Entity, NERC, or the Commission should have to approve the exception, but that any of the three could later audit its implementation.

30. In conclusion, while the Commission provides three options for revising footnote `b' in this Notice of Proposed Rulemaking, we seek comments on the feasibility of the options and on ways in which the options might be improved. In addition, we seek comment on whether there are other ways for NERC to solve the concerns outlined above in an equally effective and efficient manner.

III. Information Collection Statement

31. The Office of Management and Budget (OMB) regulations require that OMB approve certain reporting and recordkeeping (collections of information) imposed by an agency.\29\ The information contained here is also subject to review under section 3507(d) of the Paperwork Reduction Act of 1995.\30\

\29\ 5 CFR 1320.11.
\30\ 44 U.S.C. 3507(d).

---

32. As stated above, the subject of this NOPR is NERC's proposed modification to Table 1, footnote `b' applicable in four TPL Reliability Standards. This NOPR proposes to remand the footnote `b' modification to NERC. By remanding footnote `b' the applicable Reliability Standards and any information collection requirements are unchanged. Therefore, the Commission will submit this NOPR to OMB for informational purposes only.

33. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE. Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: data.clearance@ferc.gov, phone: (202) 502-8663, or fax: (202) 273-0873].

IV. Regulatory Flexibility Act

34. The Regulatory Flexibility Act of 1980 (RFA) \31\ generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The RFA mandates consideration of regulatory alternatives that accomplish the stated objectives of a proposed rule and that minimize any significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.\32\ The SBA has established a size standard for electric utilities, stating that a firm is small if, including its affiliates, it is primarily engaged in the transmission, generation and/or distribution of electric energy for sale and its total electric output for the preceding twelve months did not exceed four million megawatt hours.\33\ The RFA is not implicated by this NOPR because the Commission is remanding footnote' b' and not proposing any modifications to the existing burden or reporting requirements. With no changes to the Reliability Standards as approved, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities.

\31\ 5 U.S.C. 601-612.
\32\ 13 CFR 121.201.
\33\ Id. n.22.

V. Comment Procedures

35. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due 60 days from publication in the Federal Register. Comments must refer to Docket No. RM11-18-000, and must include the commenter's name, the organization they represent, if

applicable, and their address in their comments.

36. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's Web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

37. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE., Washington, DC 20426.

38. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VI. Document Availability

39. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through FERC's Home Page (http://www.ferc.gov) and in FERC's Public Reference Room during normal business hours (8:30 a.m. to 5 p.m. Eastern time) at 888 First Street, NE., Room 2A, Washington, DC 20426.

40. From FERC's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

41. User assistance is available for eLibrary and the FERC's Web site during normal business hours from FERC Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or e-mail at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission. Commissioner Spitzer is not participating.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2011-27624 Filed 10-25-11; 8:45 am]
BILLING CODE 6717-01-P

[Federal Register Volume 76, Number 225 (Tuesday, November 22, 2011)]
[Notices]
[Pages 72197-72202]
From the Federal Register Online via the Government Printing Office [www.gpo.gov]
[FR Doc No: 2011-30116]

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[137 FERC] 61,131; Docket No. RD11-3-000]

Before Commissioners: Jon Wellinghoff, Chairman; Philip D. Moeller, John R. Norris, and Cheryl A. LaFleur; North American Electric Reliability Corporation; Order Approving Reliability Standard

1. On January 28, 2011, the North American Electric Reliability Corporation (NERC) submitted a petition seeking approval of a revised Facilities Design, Connections, and Maintenance (FAC) Reliability Standard FAC-013-2--Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon, pursuant to section 215(d)(1) of the Federal Power Act (FPA) \1\ and section 39.5 of the Commission's regulations.\2\ The revised Reliability Standard requires planning coordinators to have a transparent methodology for, and to annually perform, an assessment of transmission transfer capability for the Near-Term Transmission Planning Horizon, as a basis for identifying system weaknesses or limiting facilities that could limit energy transfers in the future. NERC also requests approval of two new terms utilized in the proposed Reliability Standard, to be included in NERC's Glossary of Terms Used in NERC Reliability Standards (NERC Glossary or Glossary). Finally, NERC requests approval of its implementation plan for Reliability Standard FAC-013-2, setting an effective date that will allow planning coordinators a reasonable time, after certain related Modeling, Data, and Analysis (MOD) Reliability Standards have gone into effect, to meet the requirements of the revised Reliability Standard.

\1\ 16 U.S.C. 824o(d)(1) (2006).
\2\ 18 CFR 39.5 (2011).

---

2. As explained below, we find that revised Reliability Standard FAC-013-2 (including the associated new Glossary terms and implementation plan) is just, reasonable, not unduly discriminatory or preferential and in the public interest. We accept the violation risk factors and violation severity levels associated with the standard as proposed by NERC, with three exceptions described below. We also deny a request by the Electric Reliability Council of Texas (ERCOT) for an exemption from Reliability Standard FAC-013-2.

I. Background

3. The Commission certified NERC as the Electric Reliability Organization (ERO), as defined in section 215 of the FPA, in July 2006.\3\ In Order No. 693, the Commission reviewed an initial set of Reliability Standards as developed and submitted for review by NERC, accepting 83 standards as mandatory

[[Page 72198]]

and enforceable.\4\ In Order No. 693, the Commission, inter alia, accepted Reliability Standard FAC-013-1, which sets out requirements for communication of transfer capability calculations. In addition, the Commission directed NERC to modify FAC-013 so that it would apply to all reliability coordinators.\5\

\3\ North American Electric Reliability Corp., 116 FERC] 61,062, order on reh'g and compliance, 117 FERC] 61,126 (2006), order on compliance, 118 FERC] 61,190, order on reh'g 119 FERC] 61,046 (2007), aff'd sub nom. Alcoa Inc. v. FERC, 564 F.3d 1342 (DC Cir. 2009).
\4\ Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, FERC Stats. & Regs.] 31,242, order on reh'g, Order No. 693-A, 120 FERC] 61,053 (2007).
\5\ Id. P 790, 794.

4. Also related to NERC's immediate proposal, the Commission, in Order No. 693, neither approved nor remanded Reliability Standard FAC-012-1, which set out proposed requirements for documenting the methodologies used by reliability coordinators and planning authorities in determining transfer capability.\6\ Because additional information was needed regarding the standards' reference to regional implementation, the Commission did not act on proposed FAC-012-1, but directed certain changes to be included in a revised version of FAC-012-1. In particular, the Commission stated that the standard should provide a framework for the calculation of transfer capabilities, including data inputs and modeling assumptions.\7\ Further, the Commission stated that the process and criteria used to determine transfer capabilities must be consistent with the process and criteria used in planning and operating the system.\8\

\6\ Id. P 776, 782. See also id. P 287 (discussing ``fill-in-the-blank'' standards). NERC's proposed FAC-013-2 addresses directives pertaining to related to both FAC-013-1 and FAC-012-1.

\7\ Id. P 779.

\8\ Id. P 782.

5. Subsequently, as part of its submission of revised Modeling, Data, and Analysis (MOD) Reliability Standards, which govern the calculation of Available Transfer Capability (ATC), NERC requested that it be permitted to withdraw FAC-012-1 and retire FAC-013-1. In Order No. 729, the Commission found that FAC-012-1 and FAC-013-1 had not been wholly superseded by the revised MOD Reliability Standards because the revised MOD Reliability Standards did not address the calculation of transfer capabilities in the planning horizon.\9\ Moreover, the Commission found that the existing versions of FAC-012-1 (as adopted by NERC) and FAC-013-1 (as approved by FERC) were insufficient to address the Commission's concerns as stated in Order No. 693, and ordered NERC to develop specific modifications to comply with those outstanding directives.\10\

\9\ Mandatory Reliability Standards for the Calculation of Available Transfer Capability, Capacity Benefit Margins, Transmission Reliability Margins, Total Transfer Capability and Existing Transmission Commitment and Mandatory Reliability Standards for the Bulk-Power System, Order No. 729, 129 FERC] 61,155, at P 291 (2009); order on reh'g, Order No. 729-A, 131 FERC] 61,109, order on reh'g, Order No. 729-B, 132 FERC] 61,027 (2010).

\10\ Id.

6. The Commission explained in Order No. 729 the potential value of assessing transfer capabilities in the planning horizon, as a means of improving the long-term reliability of the Bulk-Power System:

The Commission recognizes that the calculation of transfer capabilities in the planning horizon (years one thorough five) may not be so accurate to support long-term scheduling of the transmission system but we do believe that such forecasts will be useful for long-term planning, in general, by measuring sufficient long-term capacity needed to ensure the reliable operation of the Bulk-Power System. Although regional planning authorities have developed similar efforts in response to Order No. 890, we believe that the requirements imposed by FAC-012 and FAC-013 need not be duplicative of those existing efforts and, by contrast, should be focused on improving the long-term reliability of the Bulk-Power System pursuant to the ERO's Reliability Standards.\11\

\11\ Id. P 290.

Thus, the Commission directed NERC to develop modifications to FAC-012-1 and FAC-013-1 to comply with the directives of Order No. 693 and to otherwise revise those Standards to be consistent with the revised MOD Reliability Standards.\12\

\12\ Id. P 291.

II. NERC's Petition

7. In its Petition, NERC explains that FAC-013-2 was developed in response to Commission directives in Order Nos. 693 and 729 (as discussed above) to require appropriate entities to perform an annual assessment of transfer capability in the planning horizon and to do so using data inputs and modeling assumptions that are consistent with other planning uses. Under Requirement R1, each planning coordinator must have a documented methodology for performing an annual assessment of transfer capability in the Near-Term Transmission Planning Horizon. Under Requirement R2, each planning coordinator must share its methodology with adjacent planning coordinators and transmission planners, and with other functional entities with a reliability-related need for the information. Under Requirement R3, planning coordinators must provide a documented response to comments made by an interested party about the methodology. Under Requirement R4, planning coordinators must conduct and document an annual simulation or assessment of transfer capability for at least one year in the Near-Term Transmission Planning Horizon. Under Requirement R5, planning coordinators must make the results of the assessment available to the same types of parties identified in Requirement R2. Finally, under Requirement R6, planning coordinators must provide data to support the assessment if requested by identified interested parties.\13\

\13\ See NERC Petition at 8-10, Ex. A.

---

8. NERC explains in its Petition that the proposed Reliability Standard addresses the Commission's directives by requiring planning coordinators to undertake an annual assessment of transfer capability in the planning horizon, and by requiring the use of certain data inputs and modeling assumptions to identify future transmission system weaknesses or limiting facilities.

9. NERC also requests approval of the terms ``Near-Term Transmission Planning Horizon'' and ``Year One'' to be added to the NERC Glossary. Finally, NERC proposes an implementation plan that includes an effective date for the revised Reliability Standard that is the later of (1) the first day of the calendar quarter twelve months after Commission approval of FAC-013-2, or (2) the first day of the calendar quarter six months after Reliability Standards MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-1 go into effect.\14\ At that time, the plan calls for the retirement of existing Reliability Standards FAC-012-1 and FAC-013-1.\15\

\14\ The relevant MOD Reliability Standards went into effect on April 1, 2011.

\15\ NERC Petition at Ex. B.

III. Notice of Filing and Responsive Pleading

10. Notice of NERC's Petition was issued on Feb. 2, 2011 and published on Feb. 10, 2011 in the Federal Register, with comments, protests and motions to intervene due on or before Feb. 28, 2011.\16\ Two sets of comments were received. The Midwest Independent Transmission System Operator, Inc. (MISO) and the New York Independent System Operator, Inc. (NYISO) filed a joint set of comments asking the Commission to reject FAC-013-2 as duplicative of the now-effective Transmission Planning (TPL) Standards. In addition, the ERCOT filed a motion to intervene out-of-time, asking the Commission to find that ERCOT should

[[Page 72199]]

be exempt from FAC-013-2's requirements.

\16\ 76 FR 7557 (2011).

---

11. MISO and NYISO state that Reliability Standard FAC-013-2 will not provide any reliability benefits beyond those conferred by the current TPL Reliability Standards, arguing that proposed Reliability Standard FAC-013-2 is ``substantially similar'' to the approved TPL Reliability Standards in purpose and in the assessments required.\17\ MISO and NYISO further argue that both the proposed Reliability Standard and the TPL Reliability Standards (particularly TPL-002) require an assessment of system conditions over the Near-Term Transmission Planning Horizon using similar assumptions or inputs, including contingencies, system conditions, projected firm transfers or transmission uses, and system demand levels.\18\

\17\ MISO and NYISO Comments at 3-4.
\18\ Id. at 4.

---

12. MISO and NYISO note that the TPL Reliability Standards require applicable entities not only to perform system simulations and related annual assessments to identify reliability issues based on current and projected firm transmission commitments, but also to take affirmative action to address any identified reliability issues based on those commitments. MISO and NYISO argue that the very similar assessment required under Reliability Standard FAC-013-2, which is intended ``to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliability transfer energy,'' does not provide a similar obligation to rectify any deficiencies identified from the assessment as is found in the TPL Standards, and therefore has questionable value.\19\ As an example, MISO and NYISO note that if an assessment performed under Reliability Standard FAC-013-2 found that incremental transfer capability was 0 MW at some point within the Near-Term Transmission Planning Horizon, FAC-013-2 does not provide any guidance about steps to be taken to address the identified weaknesses. Accordingly, MISO and NYISO argue that Reliability Standard FAC-013-2 is unnecessary and could lead to confusion with respect to the responsible entities' obligations to preserve the reliability of the BES.\20\

\19\ Id. at 5.
\20\ Id.

---

13. Finally, MISO and NYISO note that a calculation of transfer capability that is set one to five years in the future (i.e., the Near-Term Transmission Planning Horizon) does not provide any useful information for the future reliable operation of the system, because system conditions are likely to be significantly different than those assumed for the required assessment.\21\

\21\ Id. at 6.

---

14. ERCOT initially notes its support for MISO and NYISO's position that FAC-013-2 is unnecessary given its overlap with the requirements of the TPL Reliability Standards.\22\ However, if Reliability Standard FAC-013-2 is approved over MISO and NYISO's objections, ERCOT asks the Commission to provide an exemption for the ERCOT region. ERCOT notes that the revised Reliability Standard was developed in response to the Commission's directive to apply the transfer capability methodology requirements, as implemented in the MOD Reliability Standards, to the planning horizon.\23\ ERCOT states that the Commission has already found that the requirements of the MOD Reliability Standards governing the calculation of ATC provide no reliability benefit in the ERCOT region, essentially recognizing that ERCOT has no transmission market (and instead manages congestion through re-dispatch of generation), and that ERCOT has no interchange with neighboring regions. ERCOT argues that the same rationale applies for Reliability Standard FAC-013-2 with respect to the planning horizon, as ERCOT's reliability planning analyses are performed using the same assumptions as are used for operations.\24\

\22\ ERCOT Comments at 2.
\23\ Id. at 3.
\24\ Id. at 3-4 (noting that the Commission agreed with ERCOT's position that applying the MOD Reliability Standards to ERCOT would not provide any reliability benefits due to physical differences in ERCOT's transmission system (citing Order No. 729, 129 FERC] 61,155 at P 292-93, 296 and 298)).

---

15. ERCOT notes that the Texas Reliability Entity, Inc. (Texas RE) \25\ supported ERCOT's position on the propriety of an ERCOT exemption through comments submitted during NERC's Standards Development Process. Texas RE provided the following rationale for the exemption: ``ERCOT does not need to address transmission allocation issues either in the operating horizon or in the planning horizon. To the extent that ERCOT does planning studies to examine transfers, those studies are related more to economic planning than to reliability.'' \26\ ERCOT further argues that the Standards Drafting Team failed to draw a meaningful

distinction between the MOD requirements regarding calculation of transfer capabilities in the operating horizon, which are not applicable to ERCOT by virtue of a FERC-granted exemption, and FAC-013-2's requirements related to assessment of transfer capabilities in the planning horizon.\27\

\25\ Texas RE is the approved regional entity, as defined under FPA section 215(e)(4), for the ERCOT region, with delegated authority from NERC to develop, monitor, assess, and enforce compliance with NERC Reliability Standards within that region.

\26\ ERCOT Comments at 5 (quoting from Texas RE Comments submitted to NERC in the Standards Development Process).

\27\ Id. at 6.

IV. Discussion

16. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 CFR 385.214, the timely joint motion to intervene filed by MISO and NYISO serves to make them parties to this proceeding. Pursuant to Rule 214(d) of the Commission's Rules of Practice and Procedure, 18 CFR 385.214(d), the Commission will grant ERCOT's late-filed motion to intervene, given its interest in the proceeding, the early stage of the proceeding, and the absence of undue prejudice or delay.

A. Reliability Standard FAC-013-2

17. We approve Reliability Standard FAC-013-2 and find that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. We also approve the proposed implementation plan for Reliability Standard FAC-013-2, which would retire Reliability Standards FAC-012-1 and FAC-013-1 when FAC-013-2 becomes effective. We accept the addition of the terms ``Near-Term Transmission Planning Horizon'' and ``Year One'' to the NERC Glossary. Finally, we find that the proposed Reliability Standard satisfies our outstanding directives in Order Nos. 693 and 729 regarding the non-discriminatory assessment of transfer capability in the planning horizon.\28\

\28\ See Background Section above describing the pending Commission directives from Order No. 693 and Order No. 729.

---

18. Contrary to the arguments of MISO and NYISO, we find that Reliability Standard FAC-013-2 provides a unique reliability benefit beyond that conferred by the TPL Standards. Reliability Standard FAC-013-2 is designed to ensure that planning coordinators perform annual assessments to identify potential weaknesses and limiting facilities of the bulk electric system. Such potential weaknesses and limitations could ultimately affect reliable transfers of energy. Further, in performing the required annual assessment, the

[[Page 72200]]

planning coordinator must consider both current approved and projected transmission uses.\29\

\29\ See proposed Reliability Standard FAC-013-2 R.1.4.4.

---

19. By contrast, the TPL Reliability Standards set out specific performance requirements for all transmission planners (as well as planning authorities and coordinators), requiring among other things a demonstration that each transmission planner's portion of the bulk electric system is designed to maintain system stability and to stay within thermal and voltage limits, while serving forecast customer demand and all projected firm (non-recallable) reserved transmission services.\30\ Thus, the TPL Reliability Standards do not require a planning assessment that reflects all projected transmission uses but, rather, an assessment that reflects only projected firm reserved transmission uses. In other words, Reliability Standard FAC-013-2 differs from the TPL standards because the former focuses on identifying potential weaknesses that could limit energy transfers across a broader region and requires the planning coordinator to consider any expected transmission uses, regardless of whether they have been scheduled or otherwise reserved, and thereby allows for an assessment that may be more accurate in the outer years of the planning

horizon.

\30\ See Reliability Standard TPL-001-0.1 R1.

---

20. As MISO and NYISO note, Reliability Standard FAC-013-2 does not impose an obligation to develop a plan to address identified limitations in transfer capability in the Near-Term Transmission Planning Horizon. However, the lack of such an obligation does not detract from the Reliability Standard's value as an informational tool for the early identification of inter-regional or intra-regional limitations on transfers. In Order No. 729, the Commission recognized that the calculation of transfer capabilities in the planning horizon (years one through five) may not be accurate enough to support long-term scheduling of the transmission system.\31\ The Commission nonetheless determined that such forecasts would be useful ``for long-term planning, in general, by measuring sufficient long-term capacity needed to ensure the reliable operation of the Bulk-Power System.'' \32\

\31\ Order No. 729, 129 FERC] 61,155 at P 290.

\32\ Id.

---

21. Consistent with its purpose as a planning tool with a regional focus, rather than a mechanism for ensuring that individual systems are planned to reliably meet projected load and known transmission uses, Reliability Standard FAC-013-2 provides the planning coordinator flexibility in determining what transfers to assess. Moreover, an assessment conducted pursuant to FAC-013-2 may include transmission uses that are expected but which are not yet scheduled or reserved (e.g., expected interconnection of a large group of renewable generators), and can be used as a regional coordination tool rather than as a means of ensuring adequate planning for reliable system performance. Accordingly, we find that Reliability Standard FAC-013-2 does confer reliability benefits beyond those provided by the TPL Reliability Standards, and we are not persuaded by the arguments of MISO and NYISO on this issue.

22. We further find that Reliability Standard FAC-013-2 satisfies certain outstanding directives from Order Nos. 693 and 729 which are not satisfied by the TPL Reliability Standards. Reliability Standard FAC-013-2 requires the planning coordinator to perform an annual assessment of transfer capability for at least one year in the Near-Term Transmission Planning Horizon, and to document that the assumptions and criteria used to perform the assessment are consistent with the planning coordinator's planning practices. By contrast, the TPL Reliability Standards impose system performance requirements under various conditions, and do not require a specific assessment of transfer capabilities within a single system or across interconnected transmission systems. While we agree that Reliability Standard FAC-013-2 and the TPL Reliability Standards are designed primarily to encourage adequate longer-term planning rather than to generate accurate measures of ATC or total transfer capability (TTC), we believe that our outstanding directives regarding the review of transfer capability within the planning horizon are not satisfied by the TPL Reliability Standards.

B. Violation Risk Factors and Violation Severity Levels

23. We find that the violation risk factors (VRFs) assigned to Requirements R2, R3, R5 and R6 are consistent with the Commission's established guidelines and approve them as filed.\33\ However, we find that NERC has not adequately justified its proposed ``lower'' VRF designation for Requirements R1 and R4, and direct NERC to either provide additional justification for these VRF designations or propose a revised VRF designation that addresses our concerns.

\33\ See North American Electric Reliability Corp., 119 FERC] 61,145, order on reh'g, 120 FERC] 61,145, at P 8-13 (2007); North American Electric Reliability Corp., 123 FERC] 61,284, at P 20-35, order on reh'g & compliance, 125 FERC] 61,212 (2008); North American Electric Reliability Corp., 135 FERC] 61,166 (2011). Given the significant change in the scope of FAC-013-2 as compared to the original standards from which its requirements derive (FAC-012-1 and FAC-013-2), a reduction in the assigned VRF levels appears to be warranted for at least some of the requirements.

---

24. NERC states that Requirements R1 and R4 meet the definition of a ``lower'' risk requirement because they are ``strictly administrative in nature and are in the planning timeframe,'' and because ``it is not anticipated that under emergency, abnormal or restorative conditions violation of this requirement would affect the electric state or capability of the BES.'' \34\

\34\ NERC Petition at 33-34. The approved NERC definition for a ``lower'' VRF designation is as follows:

Lower Risk Requirement: Is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to effectively monitor and control the Bulk-Power System; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to effectively monitor, control, or restore the Bulk-Power System.

See North American Electric Reliability Corporation, 119 FERC] 61,145, at P9, order on compliance, 121 FERC] 61,179, at P 2 and Appendix A (2007).

---

25. Requirement R4 does not appear to be ``administrative in nature,'' in that it requires the planning coordinator to annually conduct a simulation assessing transfer capability on its system during at least one year in the near-term planning time frame. Requirement R4 requires an affirmative action by the applicable entity, and not merely documentation of the results of the study.

26. We have similar concerns with respect to R1, as it is a substantive requirement to adopt and document a methodology for assessing transfer capability that is consistent with the specific criteria set out in sub-requirements R1.1.2-1.5. This requirement goes further than mere documentation, and instead establishes the criteria that must be incorporated into a compliant methodology.

27. Finally, we approve the violation severity levels (VSLs) for FAC-013-2 as proposed, with the exception of the VSL triggers for R1, which appear to contain a typographical error. The VSL language for R1, as filed by NERC, uses the same description for ``medium,'' ``high,'' and ``severe'' violations, as follows:

The Planning Coordinator has a Transfer Capability methodology, but failed to

[[Page 72201]]

incorporate one of [sub-requirements 1.1 through 1.5] of Requirement R1 into that methodology.

It appears that these triggers were intended to be progressive, i.e., the failure to incorporate one component was intended to be a medium level violation, as is currently stated in NERC's filed version of FAC-013-2, but a high level violation should require a failure to incorporate two components, and so on. Accordingly, we will direct NERC to modify the VSL language for Requirement R1 to correct this apparent error.

28. For the reasons stated above, we direct NERC to submit a compliance filing within 60 days of issuance of this order, that (1) either proposes a ``medium'' VRF designation for Requirements R1 and R4, or provides additional justification for a ``lower'' VRF level; and (2) corrects the proposed VSL language for R1.

C. Applicability to ERCOT

29. For the reasons discussed below, we are not persuaded by ERCOT's arguments and, therefore, deny ERCOT's request for an exemption. ERCOT points out that the Commission granted an exemption to ERCOT regarding certain modeling, data and analysis, or MOD, Reliability Standards and believes that the Commission should grant ERCOT a similar exemption regarding compliance with FAC-013-2. Reliability Standard FAC-013-2, however, is distinguishable from the MOD Reliability Standards because the MOD Reliability Standards address methodologies for calculating ATC and total transfer capability (TTC) for the purpose of allocating transmission capacity. In Order No. 729, the Commission agreed that the MOD Reliability Standards would not provide any reliability benefit to ERCOT due to physical differences in ERCOT's transmission system.\35\

\35\ Order No. 729, 129 FERC] 61,155, at P 292-93, 296 (noting, inter alia, that ERCOT does not have a transmission market and manages transmission congestion through redispatch of generation).

---

30. In contrast to the MOD Reliability Standards, FAC-013-2 is not designed primarily to ensure non-discriminatory allocation of transmission capacity among transmission market participants, but is instead a planning tool, with a particular focus on identifying weaknesses or limitations in transfer capability between regions (including constrained regions within a single market such as ERCOT). We believe ERCOT, like other regions, will benefit from the assessment of potential limitations in transfer capability in the planning horizon over the Near-Term Transmission Planning Horizon that is required under FAC-013-2.

31. Moreover, ERCOT concedes that it currently has a planning process in place that allows it to address ``prospective weaknesses and limiting facilities that may arise under all probable prospective operating conditions.'' \36\ That ERCOT already undertakes these kinds of planning assessments leads to the conclusion that such assessments are in fact useful to ERCOT. Incorporating an obligation to continue performing such an assessment as part of a mandatory and enforceable Reliability Standard, especially one that will provide for greater levels of transparency as to how the assessments are done, will not only provide a meaningful reliability benefit but also would presumably impose little additional burden on ERCOT.

\36\ ERCOT Comments at 7.

V. Information Collection Statement

32. The Office of Management and Budget (OMB) regulations require approval of certain information collection requirements imposed by agency action.\37\ Upon approval of a collection(s) of information, OMB will assign an OMB control number and an expiration date. Respondents subject to the filing requirements of this Order will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

\37\ 5 CFR 1320.11.

---

33. The Commission will submit these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of the Paperwork Reduction Act. Comments are solicited within 60 days of the date this order is published in the Federal Register on the Commission's need for this information, whether the information will have practical utility, the accuracy of provided burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques. Comments should be submitted following the Commission's submission guidelines at http://www.ferc.gov/help/submission-guide.asp and should reference Docket No. RD11-3.

34. Rather than creating entirely new obligations with respect to the assessment of transfer capability for the near-term transmission planning horizon, Reliability Standard FAC-013-2 upgrades the existing planning requirements contained in FAC-013-1 and specifically requires planning coordinators to have a methodology for and to perform an annual assessment identifying potential future transmission system weaknesses and limiting facilities that could impact the bulk electric system's ability to reliably transfer energy in the near-term transmission planning horizon. Thus, this Order does not impose entirely new burdens on the affected entities. For example, FAC-013-1 requires each applicable entity to have a documented methodology for assessing transfer capability and to share the results of that assessment with specific entities. FAC-013-2 imposes relatively minimal new requirements regarding the information that must be included in the documented methodology, the frequency of the assessment and the number of days allocated to make the assessment results available to other entities.

35. Burden Estimate: Our estimate below regarding the number of respondents is based on the NERC compliance registry as of August 29, 2011. According to the registry, there are 80 planning authorities \38\ that will be involved in providing information. This Order will require applicable entities to review their transfer capability methodologies and document compliance with the Reliability Standard's requirements. For those planning coordinators that do not already comply with the

Standard's requirement for having a documented methodology for assessing transfer capability in the Near-Term Transmission Planning Horizon, they will be required to update their methodology documents and compliance protocols. In addition, planning coordinators must ensure that the required assessment will be performed at least once per calendar year.\39\ The estimated burden for the requirements in this Order follow:

\38\ The term ``planning coordinator'' is synonymous with the term ``planning authority,'' in the NERC Glossary.

\39\ While the document retention requirements are being increased under the new Reliability Standard (from one to three years), the usual and customary practice currently is to retain documentation needed to demonstrate compliance for the period since the last audit, which is on a three year schedule. In addition, while planning coordinators must ensure that they perform an appropriate transfer capability assessment at least once per year, they are already required to establish transfer capabilities and disseminate information about those capabilities. Thus, there should be no increase in burden other than the one-time cost of (1) setting up a procedure to ensure that the assessment will be performed at least once per year, and (2) adjusting the methodology (if needed) to comply with the more specific requirements set out in the new Reliability Standard.

[[Page 72202]]

Data collection	Number of respondents	Number of responses per respondent	Hours per respondent per response	Total annual hours
	(A)	(B)	(C)	(A x B x C)
Review and possible revision of methodology (one-time).....	\40\ 20	1	80	1,600
Procedure to perform the Transfer Capability Assessment annually (one-time).....	80	1	80	6,400
Total.....	.....	.....	.....	8,000

\40\ Requirement R1 applies to planning coordinators. We estimate that 25 percent of all planning coordinators will have to update their methodology documents.

Information Collection Costs: The Commission seeks comments on the costs to comply with these requirements and recordkeeping burden associated with Reliability Standard FAC-013-2.

Total Burden Hours for Collection: (Compliance/Documentation) = 8,000 hours.

Burden Hours Averaged Over Three Years \41\ = 2,667.

\41\ While this is a one-time burden, information collections tend to be on a three year approval cycle. Therefore, we are averaging the one-time burden estimate over three years.

Total One-Time Compliance Cost = 8,000 hours @ $120/hour = $960,000.

Total First Year Cost = $960,000.

Title: Order Approving Reliability Standard.

Action: Proposed Collection in FERC-725A.
OMB Control No: 1902-0244.
Respondents: Business or other for profit, and/or not for profit institutions.
Frequency of Responses: On occasion.
Necessity of the Information: Reliability Standard FAC-013-2 satisfies certain directives the Commission issued in Order No. 729 requiring applicable entities to specify the framework used for calculating transfer capabilities in the Near-Term Transmission Planning Horizon and to ensure that the framework is consistent with the processes and criteria used for other operating and planning purposes. It also requires some entities to update their Transfer Capability methodology documents and procedures to perform assessments annually.

36. Interested persons may obtain information on the reporting requirements by contacting: Federal Energy Regulatory Commission, 888 First Street NE., Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, email: DataClearance@ferc.gov, Phone: (202) 502-8663, fax: (202) 273-0873].

VI. Effective Date

37. This order will become effective January 23, 2012.

The Commission orders:

(A) Reliability Standard FAC-013-2 is hereby approved as just, reasonable, not unduly discriminatory, and in the public interest.

(B) NERC's addition of the terms ``Year One'' and ``Near-Term Transmission Planning Horizon'' to the NERC Glossary is hereby approved.

(C) NERC's proposed implementation plan for Reliability Standard FAC-013-2 is hereby approved, including the retirement of existing Reliability Standards FAC-012-1 and FAC-013-1 upon the effective date of Reliability Standard FAC-013-2.

(D) The VRF levels and VSL levels proposed for FAC-013-2 are approved with the exceptions discussed above, and NERC is directed to submit a compliance filing within 60 days of this order addressing the Commission's stated concerns with respect to the VRF levels of R1 and R4 and the VSL language of R1.

By the Commission. Commissioner Spitzer is not participating.

Dated: Issued November 17, 2011.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2011-30116 Filed 11-21-11; 8:45 am]
BILLING CODE 6717-01-P

137 FERC ¶ 61,131
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Philip D. Moeller, John R. Norris,
and Cheryl A. LaFleur.

North American Electric Reliability Corporation Docket No. RD11-3-000

ORDER APPROVING RELIABILITY STANDARD

(Issued November 17, 2011)

1. On January 28, 2011, the North American Electric Reliability Corporation (NERC) submitted a petition seeking approval of a revised Facilities Design, Connections, and Maintenance (FAC) Reliability Standard FAC-013-2 – Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon, pursuant to section 215(d)(1) of the Federal Power Act (FPA)[1] and section 39.5 of the Commission's regulations.[2] The revised Reliability Standard requires planning coordinators to have a transparent methodology for, and to annually perform, an assessment of transmission transfer capability for the Near-Term Transmission Planning Horizon, as a basis for identifying system weaknesses or limiting facilities that could limit energy transfers in the future. NERC also requests approval of two new terms utilized in the proposed Reliability Standard, to be included in NERC's Glossary of Terms Used in NERC Reliability Standards (NERC Glossary or Glossary). Finally, NERC requests approval of its implementation plan for Reliability Standard FAC-013-2, setting an effective date that will allow planning coordinators a reasonable time, after certain related Modeling, Data, and Analysis (MOD) Reliability Standards have gone into effect, to meet the requirements of the revised Reliability Standard.

2. As explained below, we find that revised Reliability Standard FAC-013-2 (including the associated new Glossary terms and implementation plan) is just, reasonable, not unduly discriminatory or preferential and in the public interest. We accept the violation risk factors and violation severity levels associated with the standard as proposed by NERC, with three exceptions described below. We also deny a request

[1] 16 U.S.C. § 824o(d)(1) (2006).

[2] 18 C.F.R. § 39.5 (2011).

by the Electric Reliability Council of Texas (ERCOT) for an exemption from Reliability Standard FAC-013-2.

I. Background

3. The Commission certified NERC as the Electric Reliability Organization (ERO), as defined in section 215 of the FPA, in July 2006.[3] In Order No. 693, the Commission reviewed an initial set of Reliability Standards as developed and submitted for review by NERC, accepting 83 standards as mandatory and enforceable.[4] In Order No. 693, the Commission, *inter alia*, accepted Reliability Standard FAC-013-1, which sets out requirements for communication of transfer capability calculations. In addition, the Commission directed NERC to modify FAC-013 so that it would apply to all reliability coordinators.[5]

4. Also related to NERC's immediate proposal, the Commission, in Order No. 693, neither approved nor remanded Reliability Standard FAC-012-1, which set out proposed requirements for documenting the methodologies used by reliability coordinators and planning authorities in determining transfer capability.[6] Because additional information was needed regarding the standards' reference to regional implementation, the Commission did not act on proposed FAC-012-1, but directed certain changes to be included in a revised version of FAC-012-1. In particular, the Commission stated that the standard should provide a framework for the calculation of transfer capabilities, including data inputs and modeling assumptions.[7] Further, the Commission stated that the process

---

[3] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,190, *order on reh'g* 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

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

[5] *Id.* P 790, 794.

[6] *Id*. P 776, 782. *See also id.* P 287 (discussing "fill-in-the-blank" standards). NERC's proposed FAC-013-2 addresses directives pertaining to related to both FAC-013-1 and FAC-012-1.

[7] *Id.* P 779.

and criteria used to determine transfer capabilities must be consistent with the process and criteria used in planning and operating the system.[8]

5. Subsequently, as part of its submission of revised Modeling, Data, and Analysis (MOD) Reliability Standards, which govern the calculation of Available Transfer Capability (ATC), NERC requested that it be permitted to withdraw FAC-012-1 and retire FAC-013-1. In Order No. 729, the Commission found that FAC-012-1 and FAC-013-1 had not been wholly superseded by the revised MOD Reliability Standards because the revised MOD Reliability Standards did not address the calculation of transfer capabilities in the planning horizon.[9] Moreover, the Commission found that the existing versions of FAC-012-1 (as adopted by NERC) and FAC-013-1 (as approved by FERC) were insufficient to address the Commission's concerns as stated in Order No. 693, and ordered NERC to develop specific modifications to comply with those outstanding directives.[10]

6. The Commission explained in Order No. 729 the potential value of assessing transfer capabilities in the planning horizon, as a means of improving the long-term reliability of the Bulk-Power System:

> The Commission recognizes that the calculation of transfer capabilities in the planning horizon (years one thorough five) may not be so accurate to support long-term scheduling of the transmission system but we do believe that such forecasts will be useful for long-term planning, in general, by measuring sufficient long-term capacity needed to ensure the reliable operation of the Bulk-Power System. Although regional planning authorities have developed similar efforts in response to Order No. 890, we believe that the requirements imposed by FAC-012 and FAC-013 need not be duplicative of those existing efforts and, by contrast, should be focused

[8] *Id.* P 782.

[9] *Mandatory Reliability Standards for the Calculation of Available Transfer Capability, Capacity Benefit Margins, Transmission Reliability Margins, Total Transfer Capability and Existing Transmission Commitment and Mandatory Reliability Standards for the Bulk-Power System*, Order No. 729, 129 FERC ¶ 61,155, at P 291 (2009); *order on reh'g*, Order No. 729-A, 131 FERC ¶ 61,109, *order on reh'g*, Order No. 729-B, 132 FERC ¶ 61,027 (2010).

[10] *Id.*

> on improving the long-term reliability of the Bulk-Power System pursuant to the ERO's Reliability Standards.[11]

Thus, the Commission directed NERC to develop modifications to FAC-012-1 and FAC-013-1 to comply with the directives of Order No. 693 and to otherwise revise those Standards to be consistent with the revised MOD Reliability Standards.[12]

II. NERC's Petition

7. In its Petition, NERC explains that FAC-013-2 was developed in response to Commission directives in Order Nos. 693 and 729 (as discussed above) to require appropriate entities to perform an annual assessment of transfer capability in the planning horizon and to do so using data inputs and modeling assumptions that are consistent with other planning uses. Under Requirement R1, each planning coordinator must have a documented methodology for performing an annual assessment of transfer capability in the Near-Term Transmission Planning Horizon. Under Requirement R2, each planning coordinator must share its methodology with adjacent planning coordinators and transmission planners, and with other functional entities with a reliability-related need for the information. Under Requirement R3, planning coordinators must provide a documented response to comments made by an interested party about the methodology. Under Requirement R4, planning coordinators must conduct and document an annual simulation or assessment of transfer capability for at least one year in the Near-Term Transmission Planning Horizon. Under Requirement R5, planning coordinators must make the results of the assessment available to the same types of parties identified in Requirement R2. Finally, under Requirement R6, planning coordinators must provide data to support the assessment if requested by identified interested parties.[13]

8. NERC explains in its Petition that the proposed Reliability Standard addresses the Commission's directives by requiring planning coordinators to undertake an annual assessment of transfer capability in the planning horizon, and by requiring the use of certain data inputs and modeling assumptions to identify future transmission system weaknesses or limiting facilities.

9. NERC also requests approval of the terms "Near-Term Transmission Planning Horizon" and "Year One" to be added to the NERC Glossary. Finally, NERC proposes

---

[11] *Id.* P 290.

[12] *Id.* P 291.

[13] *See* NERC Petition at 8-10, Ex. A.

an implementation plan that includes an effective date for the revised Reliability Standard that is the later of (1) the first day of the calendar quarter twelve months after Commission approval of FAC-013-2, or (2) the first day of the calendar quarter six months after Reliability Standards MOD-001-1, MOD-028-1, MOD-029-1, and MOD-030-1 go into effect.[14] At that time, the plan calls for the retirement of existing Reliability Standards FAC-012-1 and FAC-013-1.[15]

III. Notice of Filing and Responsive Pleading

10. Notice of NERC's Petition was issued on Feb. 2, 2011 and published on Feb. 10, 2011 in the *Federal Register*, with comments, protests and motions to intervene due on or before Feb. 28, 2011.[16] Two sets of comments were received. The Midwest Independent Transmission System Operator, Inc. (MISO) and the New York Independent System Operator, Inc. (NYISO) filed a joint set of comments asking the Commission to reject FAC-013-2 as duplicative of the now-effective Transmission Planning (TPL) Standards. In addition, the ERCOT filed a motion to intervene out-of-time, asking the Commission to find that ERCOT should be exempt from FAC-013-2's requirements.

11. MISO and NYISO state that Reliability Standard FAC-013-2 will not provide any reliability benefits beyond those conferred by the current TPL Reliability Standards, arguing that proposed Reliability Standard FAC-013-2 is "substantially similar" to the approved TPL Reliability Standards in purpose and in the assessments required.[17] MISO and NYISO further argue that both the proposed Reliability Standard and the TPL Reliability Standards (particularly TPL-002) require an assessment of system conditions over the Near-Term Transmission Planning Horizon using similar assumptions or inputs, including contingencies, system conditions, projected firm transfers or transmission uses, and system demand levels.[18]

12. MISO and NYISO note that the TPL Reliability Standards require applicable entities not only to perform system simulations and related annual assessments to identify reliability issues based on current and projected firm transmission commitments, but also

---

[14] The relevant MOD Reliability Standards went into effect on April 1, 2011.

[15] NERC Petition at Ex. B.

[16] 76 Fed. Reg. 7557 (2011).

[17] MISO and NYISO Comments at 3-4.

[18] *Id.* at 4.

to take affirmative action to address any identified reliability issues based on those commitments. MISO and NYISO argue that the very similar assessment required under Reliability Standard FAC-013-2, which is intended "to identify potential future Transmission System weaknesses and limiting Facilities that could impact the Bulk Electric System's (BES) ability to reliability transfer energy," does not provide a similar obligation to rectify any deficiencies identified from the assessment as is found in the TPL Standards, and therefore has questionable value.[19] As an example, MISO and NYISO note that if an assessment performed under Reliability Standard FAC-013-2 found that incremental transfer capability was 0 MW at some point within the Near-Term Transmission Planning Horizon, FAC-013-2 does not provide any guidance about steps to be taken to address the identified weaknesses. Accordingly, MISO and NYISO argue that Reliability Standard FAC-013-2 is unnecessary and could lead to confusion with respect to the responsible entities' obligations to preserve the reliability of the BES.[20]

13. Finally, MISO and NYISO note that a calculation of transfer capability that is set one to five years in the future (i.e., the Near-Term Transmission Planning Horizon) does not provide any useful information for the future reliable operation of the system, because system conditions are likely to be significantly different than those assumed for the required assessment.[21]

14. ERCOT initially notes its support for MISO and NYISO's position that FAC-013-2 is unnecessary given its overlap with the requirements of the TPL Reliability Standards.[22] However, if Reliability Standard FAC-013-2 is approved over MISO and NYISO's objections, ERCOT asks the Commission to provide an exemption for the ERCOT region. ERCOT notes that the revised Reliability Standard was developed in response to the Commission's directive to apply the transfer capability methodology requirements, as implemented in the MOD Reliability Standards, to the planning horizon.[23] ERCOT states that the Commission has already found that the requirements of the MOD Reliability Standards governing the calculation of ATC provide no reliability benefit in the ERCOT region, essentially recognizing that ERCOT has no transmission market (and instead manages congestion through re-dispatch of generation), and that

---

[19] *Id.* at 5.

[20] *Id.*

[21] *Id.* at 6.

[22] ERCOT Comments at 2.

[23] *Id.* at 3.

ERCOT has no interchange with neighboring regions. ERCOT argues that the same rationale applies for Reliability Standard FAC-013-2 with respect to the planning horizon, as ERCOT's reliability planning analyses are performed using the same assumptions as are used for operations.[24]

15. ERCOT notes that the Texas Reliability Entity, Inc. (Texas RE)[25] supported ERCOT's position on the propriety of an ERCOT exemption through comments submitted during NERC's Standards Development Process. Texas RE provided the following rationale for the exemption: "ERCOT does not need to address transmission allocation issues either in the operating horizon or in the planning horizon. To the extent that ERCOT does planning studies to examine transfers, those studies are related more to economic planning than to reliability."[26] ERCOT further argues that the Standards Drafting Team failed to draw a meaningful distinction between the MOD requirements regarding calculation of transfer capabilities in the operating horizon, which are not applicable to ERCOT by virtue of a FERC-granted exemption, and FAC-013-2's requirements related to assessment of transfer capabilities in the planning horizon.[27]

IV. Discussion

16. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214, the timely joint motion to intervene filed by MISO and NYISO serves to make them parties to this proceeding. Pursuant to Rule 214(d) of the Commission's Rules of Practice and Procedure, 18 C.F.R § 385.214(d), the Commission will grant ERCOT's late-filed motion to intervene, given its interest in the proceeding, the early stage of the proceeding, and the absence of undue prejudice or delay.

---

[24] *Id.* at 3-4 (noting that the Commission agreed with ERCOT's position that applying the MOD Reliability Standards to ERCOT would not provide any reliability benefits due to physical differences in ERCOT's transmission system (citing Order No. 729, 129 FERC ¶ 61,155 at P 292-93, 296 and 298)).

[25] Texas RE is the approved regional entity, as defined under FPA section 215(e)(4), for the ERCOT region, with delegated authority from NERC to develop, monitor, assess, and enforce compliance with NERC Reliability Standards within that region.

[26] ERCOT Comments at 5 (quoting from Texas RE Comments submitted to NERC in the Standards Development Process).

[27] *Id.* at 6.

A. Reliability Standard FAC-013-2

17. We approve Reliability Standard FAC-013-2 and find that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. We also approve the proposed implementation plan for Reliability Standard FAC-013-2, which would retire Reliability Standards FAC-012-1 and FAC-013-1 when FAC-013-2 becomes effective. We accept the addition of the terms "Near-Term Transmission Planning Horizon" and "Year One" to the NERC Glossary. Finally, we find that the proposed Reliability Standard satisfies our outstanding directives in Order Nos. 693 and 729 regarding the non-discriminatory assessment of transfer capability in the planning horizon.[28]

18. Contrary to the arguments of MISO and NYISO, we find that Reliability Standard FAC-013-2 provides a unique reliability benefit beyond that conferred by the TPL Standards. Reliability Standard FAC-013-2 is designed to ensure that planning coordinators perform annual assessments to identify potential weaknesses and limiting facilities of the bulk electric system. Such potential weaknesses and limitations could ultimately affect reliable transfers of energy. Further, in performing the required annual assessment, the planning coordinator must consider both current approved and *projected* transmission uses.[29]

19. By contrast, the TPL Reliability Standards set out specific performance requirements for all transmission planners (as well as planning authorities and coordinators), requiring among other things a demonstration that each transmission planner's portion of the bulk electric system is designed to maintain system stability and to stay within thermal and voltage limits, while serving forecast customer demand and all projected firm (non-recallable) reserved transmission services.[30] Thus, the TPL Reliability Standards do not require a planning assessment that reflects all projected transmission uses but, rather, an assessment that reflects only projected *firm reserved* transmission uses. In other words, Reliability Standard FAC-013-2 differs from the TPL standards because the former focuses on identifying potential weaknesses that could limit energy transfers across a broader region and requires the planning coordinator to consider any expected transmission uses, regardless of whether they have been scheduled or

---

[28] *See* Background Section above describing the pending Commission directives from Order No. 693 and Order No. 729.

[29] *See* proposed Reliability Standard FAC-013-2 R.1.4.4.

[30] *See* Reliability Standard TPL-001-0.1 R1.

otherwise reserved, and thereby allows for an assessment that may be more accurate in the outer years of the planning horizon.

20. As MISO and NYISO note, Reliability Standard FAC-013-2 does not impose an obligation to develop a plan to address identified limitations in transfer capability in the Near-Term Transmission Planning Horizon. However, the lack of such an obligation does not detract from the Reliability Standard's value as an informational tool for the early identification of inter-regional or intra-regional limitations on transfers. In Order No. 729, the Commission recognized that the calculation of transfer capabilities in the planning horizon (years one through five) may not be accurate enough to support long-term scheduling of the transmission system.[31] The Commission nonetheless determined that such forecasts would be useful "for long-term planning, in general, by measuring sufficient long-term capacity needed to ensure the reliable operation of the Bulk-Power System."[32]

21. Consistent with its purpose as a planning tool with a regional focus, rather than a mechanism for ensuring that individual systems are planned to reliably meet projected load and known transmission uses, Reliability Standard FAC-013-2 provides the planning coordinator flexibility in determining what transfers to assess. Moreover, an assessment conducted pursuant to FAC-013-2 may include transmission uses that are expected but which are not yet scheduled or reserved (*e.g.*, expected interconnection of a large group of renewable generators), and can be used as a regional coordination tool rather than as a means of ensuring adequate planning for reliable system performance. Accordingly, we find that Reliability Standard FAC-013-2 does confer reliability benefits beyond those provided by the TPL Reliability Standards, and we are not persuaded by the arguments of MISO and NYISO on this issue.

22. We further find that Reliability Standard FAC-013-2 satisfies certain outstanding directives from Order Nos. 693 and 729 which are not satisfied by the TPL Reliability Standards. Reliability Standard FAC-013-2 requires the planning coordinator to perform an annual assessment of transfer capability for at least one year in the Near-Term Transmission Planning Horizon, and to document that the assumptions and criteria used to perform the assessment are consistent with the planning coordinator's planning practices. By contrast, the TPL Reliability Standards impose system performance requirements under various conditions, and do not require a specific assessment of transfer capabilities within a single system or across interconnected transmission systems.

---

[31] Order No. 729, 129 FERC ¶ 61,155 at P 290.

[32] *Id.*

While we agree that Reliability Standard FAC-013-2 and the TPL Reliability Standards are designed primarily to encourage adequate longer-term planning rather than to generate accurate measures of ATC or total transfer capability (TTC), we believe that our outstanding directives regarding the review of transfer capability within the planning horizon are not satisfied by the TPL Reliability Standards.

B. Violation Risk Factors and Violation Severity Levels

23. We find that the violation risk factors (VRFs) assigned to Requirements R2, R3, R5 and R6 are consistent with the Commission's established guidelines and approve them as filed.[33] However, we find that NERC has not adequately justified its proposed "lower" VRF designation for Requirements R1 and R4, and direct NERC to either provide additional justification for these VRF designations or propose a revised VRF designation that addresses our concerns.

24. NERC states that Requirements R1 and R4 meet the definition of a "lower" risk requirement because they are "strictly administrative in nature and are in the planning timeframe," and because "it is not anticipated that under emergency, abnormal or restorative conditions violation of this requirement would affect the electric state or capability of the BES."[34]

---

[33] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,145, *order on reh'g*, 120 FERC ¶ 61,145, at P 8-13 (2007); *North American Electric Reliability Corp.*, 123 FERC ¶ 61,284, at P 20-35, *order on reh'g & compliance*, 125 FERC ¶ 61,212 (2008); *North American Electric Reliability Corp.*, 135 FERC ¶ 61,166 (2011). Given the significant change in the scope of FAC-013-2 as compared to the original standards from which its requirements derive (FAC-012-1 and FAC-013-2), a reduction in the assigned VRF levels appears to be warranted for at least some of the requirements.

[34] NERC Petition at 33-34. The approved NERC definition for a "lower" VRF designation is as follows:

> Lower Risk Requirement: is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to effectively monitor and control the Bulk-Power System; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the Bulk-Power System, or the ability to

(continued…)

25. Requirement R4 does not appear to be "administrative in nature," in that it requires the planning coordinator to annually conduct a simulation assessing transfer capability on its system during at least one year in the near-term planning time frame. Requirement R4 requires an affirmative action by the applicable entity, and not merely documentation of the results of the study.

26. We have similar concerns with respect to R1, as it is a substantive requirement to adopt and document a methodology for assessing transfer capability that is consistent with the specific criteria set out in sub-requirements R1.1.2 – 1.5. This requirement goes further than mere documentation, and instead establishes the criteria that must be incorporated into a compliant methodology.

27. Finally, we approve the violation severity levels (VSLs) for FAC-013-2 as proposed, with the exception of the VSL triggers for R1, which appear to contain a typographical error. The VSL language for R1, as filed by NERC, uses the same description for "medium," "high," and "severe" violations, as follows:

> The Planning Coordinator has a Transfer Capability methodology, but failed to incorporate one of [sub-requirements 1.1 through 1.5] of Requirement R1 into that methodology.

It appears that these triggers were intended to be progressive, i.e., the failure to incorporate one component was intended to be a medium level violation, as is currently stated in NERC's filed version of FAC-013-2, but a high level violation should require a failure to incorporate *two* components, and so on. Accordingly, we will direct NERC to modify the VSL language for Requirement R1 to correct this apparent error.

28. For the reasons stated above, we direct NERC to submit a compliance filing within 60 days of issuance of this order, that (1) either proposes a "medium" VRF designation for Requirements R1 and R4, or provides additional justification for a "lower" VRF level; and (2) corrects the proposed VSL language for R1.

> effectively monitor, control, or restore the Bulk-Power System.

See North American Electric Reliability Corporation, 119 FERC ¶ 61,145, at P9, *order on compliance*, 121 FERC ¶ 61,179, at P 2 and Appendix A (2007).

C. Applicability to ERCOT

29. For the reasons discussed below, we are not persuaded by ERCOT's arguments and, therefore, deny ERCOT's request for an exemption. ERCOT points out that the Commission granted an exemption to ERCOT regarding certain modeling, data and analysis, or MOD, Reliability Standards and believes that the Commission should grant ERCOT a similar exemption regarding compliance with FAC-013-2. Reliability Standard FAC-013-2, however, is distinguishable from the MOD Reliability Standards because the MOD Reliability Standards address methodologies for calculating ATC and total transfer capability (TTC) for the purpose of allocating transmission capacity. In Order No. 729, the Commission agreed that the MOD Reliability Standards would not provide any reliability benefit to ERCOT due to physical differences in ERCOT's transmission system.[35]

30. In contrast to the MOD Reliability Standards, FAC-013-2 is not designed primarily to ensure non-discriminatory allocation of transmission capacity among transmission market participants, but is instead a planning tool, with a particular focus on identifying weaknesses or limitations in transfer capability between regions (including constrained regions within a single market such as ERCOT). We believe ERCOT, like other regions, will benefit from the assessment of potential limitations in transfer capability in the planning horizon over the Near-Term Transmission Planning Horizon that is required under FAC-013-2.

31. Moreover, ERCOT concedes that it currently has a planning process in place that allows it to address "prospective weaknesses and limiting facilities that may arise under all probable prospective operating conditions."[36] That ERCOT already undertakes these kinds of planning assessments leads to the conclusion that such assessments are in fact useful to ERCOT. Incorporating an obligation to continue performing such an assessment as part of a mandatory and enforceable Reliability Standard, especially one that will provide for greater levels of transparency as to how the assessments are done, will not only provide a meaningful reliability benefit but also would presumably impose little additional burden on ERCOT.

---

[35] Order No. 729, 129 FERC ¶ 61,155, at P 292-93, 296 (noting, *inter alia*, that ERCOT does not have a transmission market and manages transmission congestion through redispatch of generation).

[36] ERCOT Comments at 7.

V. Information Collection Statement

32. The Office of Management and Budget (OMB) regulations require approval of certain information collection requirements imposed by agency action.[37] Upon approval of a collection(s) of information, OMB will assign an OMB control number and an expiration date. Respondents subject to the filing requirements of this Order will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

33. The Commission will submit these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of the Paperwork Reduction Act. Comments are solicited within 60 days of the date this order is published in the Federal Register on the Commission's need for this information, whether the information will have practical utility, the accuracy of provided burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques. Comments should be submitted following the Commission's submission guidelines at http://www.ferc.gov/help/submission-guide.asp and should reference Docket No. RD11-3.

34. Rather than creating entirely new obligations with respect to the assessment of transfer capability for the near-term transmission planning horizon, Reliability Standard FAC-013-2 upgrades the existing planning requirements contained in FAC-013-1 and specifically requires planning coordinators to have a methodology for and to perform an annual assessment identifying potential future transmission system weaknesses and limiting facilities that could impact the bulk electric system's ability to reliably transfer energy in the near-term transmission planning horizon. Thus, this Order does not impose entirely new burdens on the affected entities. For example, FAC-013-1 requires each applicable entity to have a documented methodology for assessing transfer capability and to share the results of that assessment with specific entities. FAC-013-2 imposes relatively minimal new requirements regarding the information that must be included in the documented methodology, the frequency of the assessment and the number of days allocated to make the assessment results available to other entities.

35. Burden Estimate: Our estimate below regarding the number of respondents is based on the NERC compliance registry as of August 29, 2011. According to the registry, there are 80 planning authorities[38] that will be involved in providing

[37] 5 CFR 1320.11.

[38] The term "planning coordinator' is synonymous with the term "planning authority," in the NERC Glossary.

information. This Order will require applicable entities to review their transfer capability methodologies and document compliance with the Reliability Standard's requirements. For those planning coordinators that do not already comply with the Standard's requirement for having a documented methodology for assessing transfer capability in the Near-Term Transmission Planning Horizon, they will be required to update their methodology documents and compliance protocols. In addition, planning coordinators must ensure that the required assessment will be performed at least once per calendar year.[39] The estimated burden for the requirements in this Order follow:

Data Collection	No. of Respondents (A)	No. of Responses Per Respondent (B)	Hours Per Respondent Per Response (C)	Total Annual Hours (A x B x C)
Review and possible revision of methodology (one-time)	20[40]	1	80	1,600
Procedure to perform the Transfer Capability Assessment	80	1	80	6,400

[39] While the document retention requirements are being increased under the new Reliability Standard (from one to three years), the usual and customary practice currently is to retain documentation needed to demonstrate compliance for the period since the last audit, which is on a three year schedule. In addition, while planning coordinators must ensure that they perform an appropriate transfer capability assessment at least once per year, they are already required to establish transfer capabilities and disseminate information about those capabilities. Thus, there should be no increase in burden other than the one-time cost of (1) setting up a procedure to ensure that the assessment will be performed at least once per year, and (2) adjusting the methodology (if needed) to comply with the more specific requirements set out in the new Reliability Standard.

[40] Requirement R1 applies to planning coordinators. We estimate that 25 percent of all planning coordinators will have to update their methodology documents.

annually (one-time)				
Total				8,000

Information Collection Costs: The Commission seeks comments on the costs to comply with these requirements and recordkeeping burden associated with Reliability Standard FAC-013-2.

- Total Burden Hours for Collection: (Compliance/Documentation) = 8,000 hours.
- Burden Hours Averaged over Three Years[41] = 2,667 .
- Total One-Time Compliance Cost = 8000 hours @ $120/hour = $960,000.
- Total First Year Cost = $960,000
- Title: Order Approving Reliability Standard
- Action: Proposed Collection in FERC-725A
- OMB Control No: 1902-0244
- Respondents: Business or other for profit, and/or not for profit institutions.
- Frequency of Responses: On occasion.
- Necessity of the Information: Reliability Standard FAC-013-2 satisfies certain directives the Commission issued in Order No. 729 requiring applicable entities to specify the framework used for calculating transfer capabilities in the Near-Term Transmission Planning Horizon and to ensure that the framework is consistent with the processes and criteria used for other operating and planning purposes. It also requires some entities to update their Transfer Capability methodology documents and procedures to perform assessments annually.

36. Interested persons may obtain information on the reporting requirements by contacting: Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, Phone: (202) 502-8663, fax: (202) 273-0873].

VI. Effective Date

37. This order will become effective [**insert date 60 days from publication in the Federal Register**].

[41] While this is a one-time burden, information collections tend to be on a three year approval cycle. Therefore, we are averaging the one-time burden estimate over three years.

The Commission orders:

(A) Reliability Standard FAC-013-2 is hereby approved as just, reasonable, not unduly discriminatory, and in the public interest.

(B) NERC's addition of the terms "Year One" and "Near-Term Transmission Planning Horizon" to the NERC Glossary is hereby approved.

(C) NERC's proposed implementation plan for Reliability Standard FAC-013-2 is hereby approved, including the retirement of existing Reliability Standards FAC-012-1 and FAC-013-1 upon the effective date of Reliability Standard FAC-013-2.

(D) The VRF levels and VSL levels proposed for FAC-013-2 are approved with the exceptions discussed above, and NERC is directed to submit a compliance filing within 60 days of this order addressing the Commission's stated concerns with respect to the VRF levels of R1 and R4 and the VSL language of R1.

By the Commission. Commissioner Spitzer is not participating.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

20111117-3021 FERC PDF (Unofficial) 11/17/2011

137 FERC ¶ 61,130
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Philip D. Moeller, John R. Norris,
and Cheryl A. LaFleur.

North American Electric Reliability Corporation Docket No. RR11-5-000

ORDER APPROVING AMENDMENTS TO RULES OF PROCEDURE

(Issued November 17, 2011)

1. On June 13, 2011, the North American Electric Reliability Corporation (NERC) filed a petition requesting approval of proposed amendments to the NERC Rules of Procedure. As discussed below, pursuant to section 215(f) of the Federal Power Act (FPA) and section 39.10(a) of the Commission's regulations, we approve the proposed amendments.[1]

I. Background

A. Section 215

2. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. The statute also requires, *inter alia*, that the ERO establish Rules that: (1) assure independence, while assuring fair stakeholder representation and balanced decision-making; (2) equitably allocate reasonable dues, fees and other charges; (3) provide fair and impartial procedures for enforcing Reliability Standards through imposition of penalties; and (4) provide reasonable notice and opportunity for public comment, due process and balance in developing Reliability Standards.

3. Section 215(f) provides that the ERO shall file with the Commission any proposed rule or proposed rule change, accompanied by an explanation of its basis and purpose. Similarly, the Commission, upon its own motion or complaint, may propose a change to the rules of the ERO. A proposed rule or proposed rule change shall take effect upon a finding by the Commission "after notice and opportunity for comment that the change is

[1] 16 U.S.C. § 824o(f)(2006) and 18 C.F.R. § 39.10(a) (2011).

20111117-3021 FERC PDF (Unofficial) 11/17/2011

just, reasonable, not unduly discriminatory or preferential, is in the public interest and satisfies the requirements of subsection (c)."[2]

B. Order No. 672 and NERC's Certification as the ERO

4. On February 3, 2006, the Commission issued Order No. 672 to implement the requirements of section 215 of the FPA.[3] Order No. 672, *inter alia*, sets forth the process for certifying an ERO to develop and enforce compliance with mandatory Reliability Standards, subject to Commission approval and oversight.

5. On July 20, 2006, the Commission certified NERC as the ERO under section 215(c) of the FPA.[4] The Commission found that NERC satisfies the criteria to be the ERO responsible for developing and enforcing mandatory Reliability Standards for the United States except for Alaska and Hawaii. Further, the Commission approved NERC's Rules of Procedure and, in addition, identified needed revisions to the NERC Rules. Through a series of subsequent filings, NERC refined its Rules of Procedure, including NERC's Reliability Standards Development Procedure, and Compliance Monitoring and enforcement program.[5]

II. Proposed Amendments to NERC Rules of Procedure

6. In its June 13, 2011 petition, NERC proposes to amend *Appendix 3B Election Procedure for Members of NERC Standards Committee* of the NERC Rules of Procedure. Specifically, NERC's proposed amendments: (1) require the Chair and Vice Chair of the NERC Standards Committee to serve as non-voting members; (2) add a criterion for the Canadian representative on the Standards Committee to require that the representative is an individual that has Canadian citizenship and resides in Canada; (3) simplify the process for managing special Standards Committee elections to fill vacant positions that

---

[2] 16 U.S.C. § 824o(f)(2006).

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

[4] *North American Electric Reliability Corp*., 116 FERC ¶ 61,062 (ERO Certification Order), *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom*. *Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[5] *E.g., North American Electric Reliability Corp.*, 118 FERC ¶ 61,030 (2007).

20111117-3021 FERC PDF (Unofficial) 11/17/2011

occur mid year by eliminating the need to collect petitions and hold a ratifying vote; and (4) make additional minor conforming changes.

7. Regarding the proposal to require the Chair and Vice Chair of the NERC Standards Committee to serve as non-voting members, NERC explains that during the past year, the elected officers on the Standards Committee faced a conflict of interest when determining whether to vote on behalf of the industry segment that elected them or on behalf of the industry as a whole. NERC states that the purpose of the proposed change is to eliminate this conflict of interest, to ensure that each industry segment maintains two representatives on the Standards Committee and to clarify that the officers of the Standards Committee are expected to act on behalf of the industry as a whole rather than on behalf of any particular industry segment.

8. NERC states that its clarification to add a criterion for the Canadian Representative of the Standards Committee is consistent with the definition of "Canadian" in section 200 of the NERC Rules of Procedure, and that the purpose of this change is to increase the likelihood that the Canadian Representative is familiar with Canadian issues. NERC further states that the purpose of its proposal is to simplify the process for managing special Standards Committee elections and to improve efficiency and result in shorter vacancies for these positions.

9. NERC also proposes to incorporate new *Appendix 3D Registered Ballot Body Criteria* into the NERC Rules of Procedure. NERC explains that on September 3, 2010, the Commission approved NERC's Standards Process Manual to replace the Reliability Standards Development Procedure Version 7, and that the Standards Process Manual did not include registered ballot body criteria.[6] NERC believes that it is appropriate to re-incorporate the Registered Ballot Body Criteria into the NERC Rules of Procedure with certain modifications that are intended to add clarity and bring the criteria up to date with changes in the industry.

10. The proposed changes include: (1) replacing the term "persons" (in addition to entities) with "individuals" in the criteria of potential Registered Ballot Body members for clarity purposes; (2) clarifying the segment qualification guidelines to state that after members of each segment are selected, registered participants may apply to change those segments annually on a schedule determined by the Standards Committee; (3) expanding the criteria for Regional Transmission Organizations to include Independent System Operators; (4) allowing agents or associations to represent groups of load serving entities; (5) allowing agents or associations to represent groups of electricity generators; and (6) allowing agents or associations to represent groups of electricity brokers, aggregators, or marketers, and also a new provision for inclusion of demand-side management providers.

[6] *North American Electric Reliability Corp.*, 132 FERC ¶ 61,200 (2010).

20111117-3021 FERC PDF (Unofficial) 11/17/2011

11. In addition, NERC proposes to add a provision to clarify that: (1) individuals or entities such as consultants, vendors, or trade associations, providing products or services related to Bulk-Power System reliability within the previous 12 months to another entity eligible to join Segments 1 through 7 (and that are therefore eligible to join one of these segments) are not eligible to join Segment 8; (2) individuals or entities that elect to participate in Segment 8 are not eligible to participate in multiple segments; and (3) individuals who are employed by an entity registered in another segment are not eligible to join Segment 8.[7] NERC also proposes to add a new criterion in Segment 5 – Electric Generators allowing agents or associations to represent groups of electric generators and, for clarity, to expand the language to expressly include variable and other renewable resources. Also, NERC proposes to replace the phrase Regional Reliability Organizations in Segment 10 with Regional Entities.[8]

III. Notice and Responsive Pleadings

12. Notice of NERC's June 13, 2011, Filing was published in the *Federal Register*, 76 Fed. Reg. 35,876 (2011), with interventions and protests due on or before July 5, 2011. A motion to intervene was timely filed by American Municipal Power, Inc. (AMP). Louisville Gas and Electric Company and Kentucky Utilities Company (LG&E) filed a timely comment but did not seek to intervene in this proceeding.

13. LG&E supports NERC's proposal except for two specific changes to the *Appendix 3D Registered Ballot Body Criteria*. LG&E indicates that it does not support the proposed language regarding Segment 5 – Electric Generators. Specifically, LG&E states that the phrase "including variable and other renewable resources" is unnecessary, only serves to make such generators a special class without justification, and believes the inclusion of this language creates the opportunity to discriminate against those generators

[7] In accordance with *Appendix 3D*, each participant chooses which of the Segments it wishes to join. NERC reviews the choices and makes a determination of whether the selection satisfies at least one of the guidelines to belong to that Segment. If a guideline is satisfied, the entity or individual will then be "credentialed" to participate as a voting member of that Segment. The Segments include: Segment 1 - Transmission Owners, Segment 2 - Regional Transmission Organizations and Independent System Operators, Segment 3 - Load-Serving Entities, Segment 4 - Transmission Dependent Utilities, Segment 5 - Electric Generators, Segment 6 - Electricity Brokers, Aggregators, and Marketers, Segment 7 - Large Electricity End Users, Segment 8 - Small Electricity Users, Segment 9 - Federal, State and Provincial Regulatory or other Government Entities, and Segment 10 - Regional Entities.

[8] NERC Petition at 5.

20111117-3021 FERC PDF (Unofficial) 11/17/2011

that do not fit within this special class. LG&E states that if such generators produce energy, then they fall into this segment without the additional language.

14. In addition, LG&E suggests that "agents or associations" representing groups of Segment-Eligible entities should be precluded from casting ballots where the agent or association's membership consists of entities eligible to cast their own individual ballots as a Segment-Eligible entity. LG&E suggests that this would prevent a registered ballot body member from having more than one vote. LG&E suggests that the provision should state that "(a) affiliated entities may collectively be registered only once within a segment; (b) agents and associations may not register within the same segment in which any entity or individual represented by the agent or association is also registered; and (c) consultants, employees and vendors providing services related to bulk power system reliability within the previous 12 months to another entity or individual may not register within the same segment in which the entity or individual receiving those products or services is also registered."[9]

IV. Discussion

A. Procedural Matters

15. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2011), the timely, unopposed motion to intervene filed by AMP serves to make it a party to this proceeding. In addition, we accept LG&E's timely filed comments.

B. Commission Determination

16. Pursuant to the Commission's authority under section 215(f) of the FPA and section 39.10(a) of the Commission's regulations, we approve the proposed modifications to the NERC Rules of Procedure. We agree with NERC that the modifications to *Appendix 3B* relative to the changes to the roles of the Chair and Vice Chair of the Standards Committee will eliminate the potential conflict of interest and ensure that each industry segment maintain the appropriate number of representative on the Standards Committee. In addition, we accept as reasonable NERC's addition of a criterion to ensure that each Canadian representative on the Standards Committee has Canadian citizenship and resides in Canada. We also agree with NERC that the amendments simplify the process for managing special elections to fill vacant positions that occur during the course of the year.

[9] LG&E Comments at 3-4.

20111117-3021 FERC PDF (Unofficial) 11/17/2011

17. With regard to LG&E's comment, we are not persuaded that the language "including variable and other renewable resources" creates the opportunity to discriminate against other generators who do not fit within this class. Rather, it is reasonably understood that this language helps to clarify the qualifications for membership in Segment 5 by providing one example of acceptable types of generation and additionally signals to variable and other renewable resource generators that they are able to participate in this voting Segment.

18. Further, we accept NERC's proposal to include "agents and associations" in the individual Segments in *Appendix 3D* of the NERC Rules of Procedure. While the Commission agrees that the addition of Agents or Trade Associations as voting members may impact several of the smaller segments, we are not persuaded that the proposed changes will have a material impact on the balance or fairness of those individual voting segments. Rather, NERC's addition of these entities is consistent with the Commission's general policy of inclusiveness with regard to the NERC Standards Development Process.[10] Recognizing that Agents and Trade Associations may provide additional perspectives of their members, some of which may not be participating in, or represented by the NERC Standards Development Process, we believe that the addition of these entities to the Registered Ballot Body Criteria may ultimately lead to the creation of more balanced Reliability Standards. For these reasons, we will not adopt LG&E's suggestions with regard to this issue.

The Commission orders:

NERC's petition is hereby approved, as discussed in the body of this order.

By the Commission. Commissioner Spitzer is not participating.

(S E A L)

Kimberly D. Bose,
Secretary.

[10] *See* Order No. 672 at P 268; *ERO Certification Order*, 116 FERC ¶ 61,062 at P 93.

20111117-3021 FERC PDF (Unofficial) 11/17/2011

Document Content(s)

RR11-5-000.DOC.....1-6

November 17, 2011

Commissioner Philip D. Moeller

STATEMENT

FEDERAL ENERGY REGULATORY COMMISSION

Docket Nos. AD12-1-000

Statement of Commissioner Philip D. Moeller on FERC's Upcoming Reliability Conference

"On Monday I released a comprehensive list of questions related to whether or not reliability might be impacted by upcoming rules of the EPA. While I am certain that all of my fellow Commissioners could have arrived at an equally comprehensive list, I wanted to circulate my thoughts on this topic well in advance of the technical conference.

By circulating these questions in advance, I hope to provide interested people with an opportunity to provide "hard" and "real" evidence of reliability problems. The debate over EPA and reliability is too often a debate lacking in substance, where one person might say this nation has a reliability problem, and another person will say the opposite. So the purpose of these detailed questions is to move the debate away from mere allegations, and into the substantive analysis of reliability issues and how to resolve them.

Just as I firmly believe that reliability issues associated with renewable energy can be adequately resolved, I believe that given enough time and study, any reliability issues associated with EPA rules can be resolved. Since its inception, electricity providers have been continuously addressing reliability issues and overcoming them. In the early days it was a debate between direct current and alternating current. During the Second World War transmission lines became one of the many solutions to the risk of sabotage and the problems of energy shortages that were fueled by wartime demand. After the war, the reliability problem of integrating increasingly large power plants, including nuclear plants, resulted in the development of many large pumped-storage facilities.

All of these earlier challenges to reliability were addressed successfully, and I have no doubt that any new challenges that we face can also be addressed. To clarify a few details on my list of questions:

> First, these are my questions alone, and not an official request by the Commission. Thus, as should be obvious, any response is optional and intended to help guide the public on the issues that could become important for the written record.
>
> Second, I have suggested no due date --- and that is intentional. To the extent that anybody can provide their responses before the technical conference, that would help me prepare for the conference. But given the importance of reliability to the power grid, I'd rather have complete and accurate responses than anything rushed or uncertain.
>
> Third, I don't expect, and would actually be surprised if anybody answered every question asked. I've asked a variety of questions that are based upon conversations that I've had over the past year or so on this topic. But a conversation is not evidence in the record that can be acted upon, and that's why decisions aren't based upon mere conversations. Thus, my questions are an opportunity to submit evidence into the record. And importantly, when evidence is submitted into the record, that evidence then provides people who have differing views an opportunity to challenge that evidence with their own evidence.

I look forward to the upcoming conference.

Document Content(s)

Moeller-statement.DOC.....1-1

20111114-4001 FERC PDF (Unofficial) 11/14/2011

UNITED STATES OF AMERICA
FEDRAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference	Docket No. AD12-1-000
North American Electric Reliability Corporation	Docket No, RC11-6-000
Public Service Commission of South Carolina and the South Carolina Office of Regulatory Staff	Docket No. EL11-62-000

(Not consolidated)

REQUEST FOR EVIDENCE OF COMMISSIONER PHILIP D. MOELLER ON EPA ISSUES FOR THE NOVEMBER 2011 RELIABILITY CONFERENCE

At the upcoming technical conference, the Commission will consider, among other things, how certain rules under consideration by the Environmental Protection Agency (EPA) could impact the reliability of electric supply in this nation.

Because of its responsibility for reliability and for wholesale electric markets, this Commission needs to both understand and take appropriate actions to ensure that prices for electricity are just and reasonable --- and that sufficient electricity is reliably available across our nation. Our effort to accommodate the changing power grid requires us to actively consider reliability issues that arise from actions of the EPA. In July of this year, we recognized that our acting on upcoming changes to the power grid is "critical":

> The need for additional transmission facilities is being driven in large part, by changes in the generation mix… early retirements of coal-fired generation, an increasing reliance on natural gas, and large-scale integration of renewable generation… It is therefore critical that the Commission act now to address deficiencies to ensure that more efficient or cost-effective investments are made as the industry addresses its challenges."[1]

In fact, the Commission has dedicated a substantial portion of our time to understanding the gradual integration of wind and other renewables onto the power grid, and we frequently issue orders and adopt regulations that relate to this topic.[2] In contrast to the

[1] Order No. 1000, 136 FERC ¶ 61,051, at P 45-46.

[2] In addition to the 600-plus pages of Order No. 1000, FERC staff recently issued a report on the "frequency response" of the power grid. This report, which was initiated and funded by FERC's Office of Electric Reliability, helps the public understand how renewable power sources such as

gradual integration of wind and solar, and our careful work studying that topic, upcoming EPA rules are expected to quickly remove, or "dis-integrate," significant amounts of coal power from the power grid.

For this reason, I am interested in receiving evidence on the following topics at our upcoming reliability conference:

1. Can the Commission agree that upcoming EPA rules, if enacted, would present a reliability problem? What evidence supports the assertion of a reliability problem? What evidence mitigates concerns about reliability? Some view the recent study by FERC staff as "informal" or as "irrelevant" --- but to the extent that staff's study is informal or irrelevant, then what other evidence available at this time can FERC rely upon to consider reliability issues?

2. Are the current tools and authority of the North American Electric Reliability Corporation (NERC) sufficient to assess and act upon reliability issues raised by upcoming EPA rules and regulations? What other resources does NERC need to fulfill its oversight role for reliability?

3. In general, are NERC's mandatory reliability standards sufficient? Should any new standards be considered under the NERC process as a result of EPA rules?

4. Will financial issues create risks of "mothballing" power plants that would otherwise be retrofitted to comply with upcoming EPA regulations? In particular, are market prices for energy and capacity sufficient at this time to attract investors to risk their capital on projects designed to meet EPA standards? Has the economy recovered sufficiently for investors to consider an investment in power plants as a good long-term investment? To what extent would reliability be impacted if power plants are "mothballed"?

5. Will it make more sense for investors to "mothball" power plants until the full scope of the upcoming EPA regulations is known? In other words, will significant numbers of investors prefer to retire power plants now, as a means to lower the risk that investments into pollution controls will be stranded by future EPA regulations? More broadly, do investors perceive regulators at either EPA or FERC as increasing or decreasing their investment risk? To what extent would reliability be impacted if power plants are "mothballed"?

---

wind and solar can be integrated into the power grid at the same time that coal and older fuel sources are retired. As stated in a press release issued by FERC on January 20, 2011, "[t]his study is valuable in that it gives us the tools to help determine how to manage operation and expansion of the grid, regardless of which resources the electric industry uses to generate power."

6. Given the findings in the recent report that was issued by FERC staff on the "frequency response" of the power grid, are the NERC standards related to frequency response sufficient to ensure adequate voltage support given the expected retirements of coal plants across the power grid?

7. Will the loss of the system inertia that is supplied by coal plants impact the power grid in unforeseen ways? Does the topic of inertia require further study?

8. Because "blackstart" power plants are needed to re-start the power grid after a blackout, will blackstart standards and planning require further study before the retirement of blackstart units?

9. Are the NERC modeling and planning standards robust enough to ensure that the nation understands how simultaneous retirements of longstanding power plants will impact the power grid?

10. Are the models used for contingency planning capable of accommodating the different types of power plants that are expected to remain on the power grid after small coal plants are retired? That is, do the models need to be modified to handle the bigger contingencies that would be expected if the remaining power plants tend to be larger plants? Do the contingency models need to be modified because of the differing reliability characteristics of a resource base with more renewable power?

11. To the extent that the operating characteristics at power plants change as a result of EPA rules, how would changes in those characteristics impact how the operators of the system dispatch power plants? In particular, how would changes to start-up and malfunction procedures at generating plants impact operational decisions?

12. Do any policies in the Commission's recent Order No. 1000 merit further consideration with respect to how planners of the transmission grid should work together with those who are investing in generation resources? Specifically, since modifying the transmission network can impact whether a power plant should retire, and since modifying which power plants retire can impact whether to invest in certain transmission assets, are the planning approaches in Order No. 1000 sufficient to address the simultaneous retirement of large numbers of power plants?

13. What knowledge do the regional operators of the power system, including Regional Transmission Organizations (RTOs), need so that they can make decisions on whether to invest in transmission assets? Would they be helped if they had more advance notice of a decision to retire a power plant?

14. What knowledge do the owners of generation plants need so that they can make decisions on whether to retire a power plant? Would they be helped if they had more advance notice of a decision to invest in new transmission?

15. What existing legal and policy obstacles prevent generators and transmission owners from coordinating their work more closely? Given the interdependence of decisions to invest in generation with decisions to invest in transmission, does a "safety-valve" approach help or hinder the needed coordination of investment?

16. With respect to ramping the system up or down after many smaller coal-powered generators are retired, how should ramping procedures change to reflect larger sizes of operating units?

17. Should NERC consider any new standards with respect to minimum voltage? What is the expected impact of EPA rules on voltage support?

18. Given the economic weakness over the past several years, how would the demand for electricity differ under a rapidly growing economy? That is, if the economy begins to recover over the next few years, can the generation fleet serve demand if significant numbers of existing power plants are retired?

19. The EPA apparently made statements that appear to question whether "fracking" of natural gas will be permitted in the future,[3] which raises the question of whether future regulatory requirements imposed on fracking will allow access to sufficient quantities of natural gas to replace coal. Does this issue present a reliability concern?

20. Do investors and managers who are expecting to replace coal plants with new gas-powered plants believe that natural gas pipelines can be authorized and built in a manner that will allow new gas plants to enter service when needed for reliability? Has this matter been studied sufficiently?

---

[3] See a 41-page document identified as EPA-HQ-OAR-2009-0234- 3003.2, a "Response to 03/04/11 Interagency Comments" and a 7-page document identified as EPA-HQ-OAR-2009-0234-3025.1, "Response to 03/09/11 Interagency Comments". These documents contain the following two statements, apparently made by EPA:

> *"EPA could remove this from the justification for the rejecting the beyond-the-floor analysis if FERC believes there is sufficient gas for all coal- and oil-fired electric generation to be replaced by natural gas without the use of hydraulic fracturing."*
>
> *"We presented the discussion in addition to our concerns with the costs of fuel switching and about the available supply of natural gas (which FERC contests)."*

21. Are any regions of this nation expecting particularly harsh impacts from the retirement of generating plants? That is, are some parts of the nation largely served by one or two critical power plants, which if retired, would present reliability problems that impose extreme hardship on the economic vitality of a community or region?

22. Should the Commission consider any other evidence related to EPA matters?

To the extent that the public has evidence to offer for the record on these issues, please file that evidence, together with any comments, in the above-listed dockets and in accordance with usual FERC procedures. In addition, please send a courtesy copy to my office:

The Honorable Philip D. Moeller
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8852

November 14, 2011

Document Content(s)

MoellerTechConf.PDF.....1-5

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

VERSION 4 CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS	**Docket No. RM11-11-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

November 21, 2011

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	NOTICES AND COMMUNICATIONS	2
III.	DISCUSSION	2
IV.	CONCLUSION	15

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby provides these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR")[2] regarding the Version 4 Critical Infrastructure Protection ("CIP") Reliability Standards. In the NOPR, the Commission proposed to approve eight modified CIP Reliability Standards (CIP-002-4 through CIP-009-4), the accompanying Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") with modifications, the implementation plan, and the effective date developed and approved by NERC. The Commission seeks comments from interested parties on the proposed approval of the Version 4 CIP standards.

The purpose of the Version 4 CIP Reliability Standards is to provide a cybersecurity framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the Bulk Power System.

By this filing, NERC submits its response to the NOPR.

[1] The Federal Energy Regulatory Commission ("FERC" or "Commission") certified NERC as the electric reliability organization ("ERO") in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (July 20, 2006).

[2] *Version 4 Critical Infrastructure Protection Reliability Standards, Notice of Proposed Rulemaking*, 136 FERC ¶ 61,184 (September 15, 2011) ("NOPR").

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.Phillips@nerc.net

III. DISCUSSION

A. The Proposed Reliability Standards

In a February 10, 2011 filing,[3] NERC requested Commission approval of the proposed Version 4 CIP Reliability Standards to replace the currently effective Version 3 CIP Reliability Standards. The Version 4 CIP Reliability Standards were developed in response to directives in Order No. 706[4] and propose to modify CIP-002-4 to include "bright line" criteria for the identification of Critical Assets, replacing the current entity-developed risk-based assessment methodology. NERC also developed conforming changes to the seven remaining Version 3 CIP Reliability Standards.

[3] *See Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4*, Docket No. RM011-11-000 (February 10, 2011) ("NERC Petition").
[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008).

NERC recognized in its original petition for approval that the Version 4 CIP Reliability Standards serve as an "interim step"[5] to addressing the complete set of directives in Order No. 706. NERC has not yet addressed all of the directives in Order No. 706 in the Version 4 CIP Reliability Standards but anticipates responding to all of the Order No. 706 directives in the Version 5 CIP Reliability Standards. The standard drafting team continues to develop solutions to the directives in a "phased" approach.

By this filing, NERC responds to the NOPR and urges the Commission to promptly approve the Version 4 CIP Reliability Standards.

B. Responses to Specific Matters Identified by the Commission

1. Whether Additional Critical Assets Can be Identified

In the NOPR, FERC is requesting comments on whether, under CIP Version 4, a responsible entity retains the flexibility to identify assets that, although outside of the bright line criteria, are essential to bulk power system reliability.[6] Additionally, FERC is requesting comments on whether NERC and/or the Regional Entities will have the ability, either in an event-driven investigation or compliance audit, to identify specific assets that fall outside the bright-line criteria yet are still essential to Bulk-Power System reliability and should be subject prospectively to compliance with the CIP standards.[7]

FERC is also requesting that NERC provide a method for review and approval of Critical Cyber Asset lists from external sources such as the Regional Entities or NERC.[8] FERC notes that the Regional Entities must have a role in the external review to ensure that there is sufficient

[5] NERC Petition at p. 6
[6] CIP V4 NOPR at P 31.
[7] *Id.*
[8] *Id.* at P 45.

accountability in the process and because the Regional Entities and NERC are ultimately responsible for ensuring compliance with Reliability Standards.[9] FERC states that, looking forward, it will be essential for NERC and the Regional Entities to actively review the designation of cyber assets that are subject to the CIP Reliability Standards, including those which span regions, in order to determine whether additional cyber assets should be protected.[10]

The proposed Version 4 CIP Reliability Standards present a bright-line for defining Critical Assets that provides certainty and clarity regarding those assets that should be identified as critical. In developing the proposed CIP-002-4 standard, the drafting team considered adding criteria that would allow entities to identify additional facilities falling outside of the bright-line criteria that they believe are essential to bulk power system reliability. Because of potential variances in application of additional facilities subject to the CIP standards, the drafting team made a determination not to add additional criteria beyond the bright-line criteria. However, responsible entities are permitted to apply any or all of the requirements in the CIP standards to assets that do not meet the bright-line thresholds.

The development of CIP Version 4 is an interim step to addressing all of the remaining Order No. 706 directives. The drafting team has used some post-version 4 information (*e.g.*, the results of the FERC-requested survey[11] and further industry discussions) to further refine the bright-line criteria with the intent to categorize assets as being of low, medium, or high impact that are "critical" to bulk power system reliability. NERC anticipates this will be reflected in the proposed CIP Version 5 standards scheduled to be filed for Commission approval in 2012.

[9] *Id.* at P 59.
[10] *Id.* at P 61.
[11] *See*, FERC's April 12, 2011 data request to NERC regarding the CIP V4 Reliability Standards, and NERC's May 27, 2011 response to the FERC data request, filed in FERC Docket No. Rm11-11-000.

In the interim period, if there are assets that NERC and the Regional Entities later determine should be treated as critical but do not meet the CIP Version 4 criteria, NERC has the authority under Section 810 of the NERC Rules of Procedure to issue a Level 2 (Recommendation) or Level 3 (Essential Action) Alert. Section 810 of the NERC Rules of Procedure provides the following:

> **810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions**
>
> 1. Members of NERC and bulk power system owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.
> 2. In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and other information will be used to guide the reliability assessment program.
> 3. When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:
>
>   3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the bulk power system of findings and lessons learned;
>
>   3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the bulk power system according to each entity's facts and circumstances;
>
>   3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system to take to ensure the reliability of the bulk power system. Such Essential Actions require NERC board approval before issuance.
>
> 4. The bulk power system owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such bulk power system owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.
>
> 5. NERC will advise the Commission and other applicable governmental authorities of its intent to issue all Level 1 Advisories, Level 2 Recommendations, and Level 3

> Essential Actions at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other applicable governmental authorities no later than thirty (30) days following the date by which NERC has requested the bulk power system owners, operators, and users to which a Level 2 Recommendation or Level 3 Essential Action issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other applicable governmental authorities will describe the actions taken by the relevant owners, operators, and users of the bulk power system and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for confidential or critical infrastructure information.

Level 3 Alerts, issued pursuant to NERC Rule of Procedure Section 810, allow NERC (following NERC Board of Trustees approval) to recommend that specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system be taken to ensure the reliability of the bulk power system. Additionally, Rule 810 states that bulk power system owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) Alerts apply shall provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions consistent with reporting dates specified by NERC. Therefore, NERC can use Level 2 Recommendations and Level 3 Essential Actions as a tool to address assets that NERC and Regional Entities later determine should be treated as critical but do not fall into the CIP Version 4 criteria.

In Order No. 706-A,[12] FERC states "that oversight of a responsible entity's identification of critical cyber assets would occur at the compliance audit stage." The Version 4 standards work within that framework by providing the bright-line criteria for the identification of Critical Assets and providing for further oversight at the compliance audit stage.

[12] Order No. 706 at P. 50.

The Version 5 standards modify this approach by characterizing "BES Cyber Systems" as "High Impact," "Medium Impact," or "Low Impact" based on the impact of the cyber system to the reliable operation of the bulk power system. This characterization makes use of a bright-line concept similar to Version 4, but requires responsible entities to determine the impact of loss, compromise or misuse of a given BES Cyber System using a bright-line impact filter.

1. Whether the VSLs for CIP-002-4, Requirements R1 and R2 Should be Modified

In the NOPR, FERC expresses concern that the proposed Version 4 VSLs for CIP-002-4, Requirements R1 and R2 do not adequately address the purpose of NERC's proposed bright-line criteria: to ensure accurate and complete identification of all Critical Assets, so that all associated Critical Cyber Assets become subject to the protections required by the CIP Standards.[13] FERC states that neither set of VSLs address the failure to properly identify either Critical Assets or Critical Cyber Assets in the first place.[14] FERC therefore proposes to direct NERC to modify the VSLs for CIP-002-4, Requirements R1 and R2, to address a failure to identify either Critical Assets or Critical Cyber Assets, as shown in Appendix 1 of the NOPR.[15]

NERC agrees with FERC that the VSLs for CIP-002-4, Requirements R1 and R2 should be modified, and proposes to add the word "complete" in the front of the list in the VSL language to ensure that the list of identified Critical Assets from each Responsible Entity is a complete list. The new language would read as follows: "The Responsible Entity did not

[13] NOPR at P 35.
[14] *Id.* at P 36.
[15] *Id.* at P 37.

develop a complete list of its identified Critical Assets even if such list is null." This would keep the requirements binary, consistent with FERC's guidance on this issue.[16]

In order to modify the VSLs for CIP-002-4, Requirements R1 and R2, NERC will have to conduct a non-binding poll, present the proposed changes to the NERC Board of Trustees for approval, and then file the proposed changes with FERC for approval, which could take NERC several months to complete.

2. Proposed CIP Version 4 Implementation Plan

In the NOPR, FERC proposes to approve the proposed Implementation Plan for CIP V4 as filed.[17]

NERC agrees with FERC's proposal to approve the proposed Implementation Plan for the Version 4 CIP Reliability Standards as filed.

3. Deadline to Respond to Order No. 706 Directives

FERC is proposing in the NOPR to direct NERC to submit modified CIP Reliability Standards that address the outstanding directives from Order No. 706, using NERC's development timeline included in the petition.[18] This timeline specifies that NERC submit a modified set of CIP Reliability Standards to the NERC Board for approval by the end of second quarter 2012, and file with FERC by the end of third quarter 2012.[19]

NERC appreciates FERC's acknowledgement that Version 4 is an interim step in addressing outstanding directives from Order No. 706, and is working to develop the CIP Version 5 Reliability Standards by the timeline NERC proposed in the petition. As long as a

[16] *See, Mandatory Reliability Standards for Critical Infrastructure Protection, Order Addressing Violation Severity Level Assignments for Critical Infrastructure Protection Reliability Standards,* 130 FERC ¶61,211, at P 14 (March 18, 2011).
[17] NOPR at PP 38-39.
[18] *Id.* at P 41.
[19] *Id.* at PP 41, 66-67.

FERC Order on the CIP Version 4 standards does not add to or expand directives from Order No. 706 or include directives that add to that timeline, the proposed deadline to file the Version 5 standards by third quarter 2012 is acceptable to NERC, subject to the discussion that follows. A FERC Order must be conditioned upon NERC's use of the FERC-approved standards development process as implemented, which requires industry approval and NERC Board of Trustees approval, before filing with FERC.

FERC is correct that, under the timeline to address all outstanding Order No. 706 directives, NERC anticipates a filing of Version 5 with FERC by the end of the third quarter of 2012. These projected timelines for standards development projects are routinely prepared to assist in resource planning within its standards development process, and by general practice, they do not include more than one successive ballot period

A 60-day initial posting period for formal comment and initial ballot of the Version 5 CIP Reliability Standards began November 7, 2011, and ends on January 6, 2012. In recognition of the volume of standards requirements and the scope of changes in Version 5 from Version 4, that posting period is longer than the more common 45-day initial posting period for formal comment. A second formal posting for comment and successive ballot period is scheduled to begin on March 26, 2012. However, the timing of that formal posting and successive ballot period depends on the number of industry comments received in response to the November 7 posting and the number of changes that may need to be made to the language in the standards as a result of those comments. In the event there is strong stakeholder opposition to the proposed standards, resulting in a failed ballot of any or all of the Version 5 CIP standards, NERC may not be able to file the Version 5 CIP standards by the third quarter 2012. Even though the drafting team has removed standard-to-standard dependencies in Version 5, the Version 5 standards must

be filed together because they collectively represent a significant change from previous versions. While NERC will make every effort to address stakeholder concerns before the successive ballot, the nature of the standards development process, and ultimately a favorable outcome on the proposed standards, is in the hands of the registered ballot body, which will in turn, affect the final delivery of the proposed CIP Version 5 standards to FERC for approval.

Thus, if a deadline must be established, NERC urges FERC to consider that a filing resulting from the FERC-approved standards development process by the end of the third quarter 2012 is only possible if the implementation of the standards development process requires only one successive ballot.

NERC notes that its anticipated timeline to file the Version 5 CIP Standards, in conjunction with the Implementation Plan proposed in the initial draft of Version 5, may present the opportunity to suggest an extension of Version 3 until Version 5 can be implemented, thereby eliminating the need for implementing Version 4, to be followed only a short time later by implementation of Version 5. That suggestion is not being made now, and it could be considered only if the industry moves promptly on Version 5. If Version 5 is not approved by the industry, filed by NERC, and approved by the Commission within that anticipated schedule, or reasonably thereafter, it is unlikely that Version 3 could be extended in a manner that eliminates the need for implementation of Version 4.

4. Identification of Critical Cyber Assets Based Upon a Cyber Asset's Connectivity and Potential to Compromise the Reliable Operation of the Bulk Power System

In the NOPR, FERC states that, in light of recent cybersecurity vulnerabilities and threats and attacks that have exploited the interconnectivity of cyber system, FERC is seeking comments regarding the method of identification of Critical Cyber Assets to ensure sufficiency and

accuracy.[20] FERC states that it believes that any criteria adopted for the purposes of identifying a Critical Cyber Asset under CIP-002 should be based upon a Cyber Asset's connectivity and its potential to compromise the reliable operation of the bulk power system, rather than focusing on the operation of any specific Critical Assets.[21] FERC is requesting comments on this approach.[22]

The Version 5CIP Reliability Standards drafting team is aware of recent cybersecurity vulnerabilities that may have the potential to exploit the interconnectivity of cyber systems. While the Version 5 CIP Reliability Standards drafting team recognizes the importance of the connectivity issue and is looking at this in the development of the Version 5 standards, this issue was not raised in FERC's Order No. 706. The drafting team is assessing FERC's suggested approach. However, it is unlikely that this work can be completed before the Version 5 CIP Reliability Standards are presented to the NERC Board of Trustees for approval.

Importantly, the proposed Version 5 CIP Reliability Standards remove the blanket exemption for non-routably connected cyber systems, and instead move the connectivity attribute to specific requirements. Additionally, the draft standard proposes to apply electronic perimeter protections of some form to all BES Cyber Systems.

5. NIST Risk Management Framework

FERC is requesting comments on whether NERC should consider applicable features of the National Institute of Standards and Technology (NIST) Risk Management Framework to ensure protection of all cyber systems connected to the bulk power system, including

[20] *Id.* at P 43.
[21] *Id.*
[22] *Id.*

establishing CIP requirements based on entity functional characteristics rather than focusing on Critical Asset size.[23]

In Paragraph 25 of Order No. 706, the Commission stated:

> 25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

Consistent with this direction, NERC is considering applicable features of the NIST Risk Management Framework in the development of the Version 5 CIP Reliability Standards. One of the fundamental differences between CIP Version 4 and CIP Version 5 is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change resulted from the standard drafting team's review of the NIST Risk Management Framework and the use of an analogous term of "information system" as the target for categorizing and applying security controls.

However, although the standard drafting team is considering changes in the Version 5 CIP Reliability Standards that are reflective of the NIST Risk Management Framework, it is important to highlight differences between NERC's and NIST's approaches. At the root of these differences are divergent responsibilities and goals between NERC and NIST. NIST develops standards and guidance for U.S. Federal Agencies to manage risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to prevent or protect against in order to achieve the

[23] *Id.* at PP 45-52.

reliability of the BES. In contrast, NIST is developing standards for almost two hundred different organizations, each with vastly different missions. The advantage of the NERC standards is a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC standards can be more tailored to the industry than a wholesale adoption of the NIST Risk Management Framework.

Four key features of the NIST Risk Management Framework were incorporated into the proposed CIP Version 5 Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function and impact, receive some level of protection; (2) customizing protection to the mission of the cyber systems subject to protection; (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System; and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled.

The criteria defined in Attachment 1 of the proposed CIP-002-5 standard are used to categorize BES Cyber Systems and their BES Cyber Assets into impact categories, resulting in all BES Cyber Systems and BES Cyber Assets being included in scope. Requirement R1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the "High" and "Medium" categories. All other BES Cyber Systems are deemed to be "Low" impact. This general process of categorization of BES Cyber Systems and BES Cyber Assets based on impact to the reliability of the BES is consistent with risk management approaches for the purpose of application of cyber security controls in the rest of the Version 5 CIP standards.

In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to its specific environment and make modifications to those controls. However, in the NERC compliance

framework, all requirements are mandatory and enforceable. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of bulk power system reliability.

While it may appear that the standard drafting team's approach to categorization is based on an asset's "size," in reality, the characterization is based on the "impact" of a misuse or compromise, or of the scope of control, of the BES Cyber System. Additionally, because electronic perimeter protections are now required surrounding all BES Cyber Systems (with specific requirements for High Impact, Medium Impact, and programmatic requirements for Low Impact), the connectivity issue FERC discussed in the NOPR should be largely addressed.

6. Potentially Unprotected Control Centers

In the NOPR, FERC expresses concern that the proposed CIP-002-4 bright line criteria do not adequately address FERC's Order No. 706 directive regarding the classification of control centers or take the potential misuse of control systems into account in the identification of Critical Assets.[24] FERC states as an example that the proposed bright line criteria leave a number of Critical Assets with potentially unprotected cyber assets, including a total of 222 control centers, with no legal obligation to apply cybersecurity measures.[25] FERC states that these potentially unprotected control centers involve an unknown number of associated control systems, and that therefore "[i]t is critical…that the Commission's concerns regarding the

[24] *Id.* at 56.
[25] *Id.*

potential misuse of control centers and associated control systems be addressed in the CIP Reliability Standards." [26]

Under the Version 5 CIP Reliability Standards, every control center will be covered by either the "Medium" or "High" criteria, which requires a greater level of protection. Because of their impact and size, no control center will qualify under the "Low" criteria. Version 5 also includes a responsibility entity's consideration of cyber misuse as part of its BES Cyber System classification. Furthermore, several of the Version 5 standards' requirements are specifically made applicable to not only "High" impact BES Cyber Systems, but also to "Medium" impact BES Cyber Systems at Control Centers. Through the use of both classification and applicability, certain requirements apply to all Control Centers, regardless of classification.

Additionally, there is not a universally accepted definition of "control center" (although the Version 5 CIP Reliability Standards drafting team has proposed one). However, by the current working definition, particularly for generation, some "control centers" have a span of control that is below the NERC Registration criteria for generators (*i.e.*, 20 MVA unit, 75 MVA plant) that only communicate with the other generators within its control. Therefore, it is difficult to imagine scenarios where cyber assets at these locations have a greater impact to reliability, simply because they meet the definition of "control center," than much larger, single-unit generators that do not meet the bright-line criteria for medium impact.

IV. CONCLUSION

For the reasons stated above, NERC respectfully requests that the Commission take prompt action in approving the proposed Version 4 CIP Reliability Standards consistent with these comments when it issues its Final Rule in this proceeding.

[26] *Id.* at PP 56, 58.

Respectfully submitted,

/s/ Holly A. Hawkins

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 21st day of November, 2011.

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

TRANSMISSION RELAY LOADABILITY RELIABILITY STANDARD	**)** **)**	**Docket No. RM11-16-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew M. Dressel
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
andrew.dressel@nerc.net

November 21, 2011

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	NOTICES AND COMMUNICATIONS	2
III.	DISCUSSION	2
IV.	CONCLUSION	6

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby provides these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR")[1] regarding a proposed Reliability Standard PRC-023-2 — Transmission Relay Loadability.[2] In the NOPR, the Commission proposed to approve Reliability Standard PRC-023-2 and the NERC Rules of Procedure Section 1700 – Challenges to Determinations. The Commission sought comments from interested parties on the proposed standard.

The purpose of PRC-023-2 is to ensure that protective relay settings shall: not limit transmission loadability; not interfere with system operators' ability to take remedial action to protect system reliability; and be set to reliably detect all fault conditions and protect the electrical network from these faults. The NERC Rules of Procedure Section 1700 – Challenges to Determinations was formed in response to the Commission directive to develop a mechanism for entities to challenge critical determinations and provides an appeals process for determinations made by Planning Coordinators under the PRC-023-2 Reliability Standard. The Commission proposes to approve both the PRC-023-2 Reliability Standard and NERC Rules of Procedure Section 1700. NERC supports the Commission's proposals in the September 15, 2011 NOPR.

By this filing, NERC submits its response to the NOPR.

[1] *Transmission Relay Loadability Reliability Standard*, 136 FERC ¶ 61,187 (September 15, 2011) ("NOPR").
[2] FERC certified NERC as the electric reliability organization ("ERO") in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (July 20, 2006).

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins*
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew M. Dressel*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
andrew.dressel@nerc.net

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

III. DISCUSSION

NERC has committed to applying the test set forth in Attachment B to PRC-023-2 to a representative sample of utilities from each of the three Interconnections and will file the results of these tests in a report on or before February, 2013 ("NERC Report").[3] FERC seeks comments regarding three issues for the ERO to address in the NERC Report related to the test to determine critical sub-200 kV facilities in Attachment B to PRC-023-2.

Responses to Specific Matters Identified by the Commission

[3] The Commission directed NERC:

> to specify the test that planning coordinators must use to determine whether a sub-200kV facility is critical to the reliability of the Bulk-Power System [and to] file its test, and the results of applying the test to a representative sample of utilities from each of the three Interconnections for Commission approval.

Transmission Relay Loadability Reliability Standard. 130 FERC ¶ 61,221, (2010) ("Order No. 733") at P 69. This directive was later modified in *Transmission Relay Loadability Standard*, 134 FERC ¶ 61,127, (2011) ("Order No.733-A") at P 78, which extended the deadline for filing the test and results to twenty-four months from the date of Order No. 733-A.

Issue 1

In the NOPR, the Commission identifies concern with "the rigor of the simulations" in criterion B4, noting that Planning Coordinators are required to apply their engineering judgment.[4] Therefore, the Commission proposes that the NERC Report address:

> whether the power system assessment proposed in criterion B4 includes the critical system conditions utilized under Reliability Standard TPL-003-0 Requirement R1.3.2 and whether applicable entities evaluate relay loadability under the B4 criterion consistent with Requirement R1 which requires, in part, that they 'evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees' in addition to applicable current criteria. If the evaluation uses other per unit voltage and power factor angle assumptions, [the Commission] propose[d] that the Report include a comparison of results obtained from those that would be achieved were the assumptions consistent with Requirement R1.[5]

NERC Response:

The intent of the power flow analysis, defined in Attachment B to PRC-023-2, is to have Planning Coordinators utilize the base cases that are used for demonstrating compliance with the TPL standards. NERC proposes to include in the NERC Report a summary of the base cases used in applying the criteria to a representative sample of utilities and an assessment of how the base cases used related to the TPL-003-0, Requirement R1.3.2.

While the measures in Criterion B4 of Attachment B do not explicitly reference voltage or power factor, the measures were derived from the conditions in PRC-023-2, Requirement R1 – specifically, 0.85 per unit voltage and 30 degree power factor angle. This allows the Planning Coordinators to make a comparison of the loading in the power flow simulation against a threshold based on the Facility Rating assigned for that circuit, without regard to the simulated voltage and power factor angle. This achieves two purposes: (i) it simplifies the test - because entities can efficiently perform the assessment using standard screening tools provided in the

[4] NOPR at P 43.
[5] *Id.*

power flow software, and (ii) it provides for a conservative test - because the measures are based on 0.85 per unit voltage and 30 degree power factor angle. A more detailed assessment that accounts for simulated voltage and power factor angle would demonstrate a greater margin against undesired tripping because the simulated apparent impedance will be a higher value when simulated voltage is greater than 0.85 per unit, and the trip threshold for a phase distance relay will be a lower value when power factor angle is less than 30 degrees. It is therefore unnecessary for NERC to include in the NERC Report a comparison of results obtained to those that would be achieved based on assumptions consistent with Requirement R1.

Issue 2

The NOPR proposes that the NERC Report should comment on what other types of technical studies or assessments the Planning Coordinators may use to identify critical facilities in Criterion B5. Specifically, the Commission states:

> Criterion B5 of Attachment B requires compliance with the proposed Reliability Standard with respect to a "circuit … selected by the Planning Coordinator based on technical studies or assessments, other than those specified in criteria B1 through B4, in consultation with the Facility owner." The Commission proposes that the Report comment on what "technical studies or assessments" planning coordinators use to identify critical facilities.[6]

NERC Response:

NERC included Criterion B5 in Attachment B to address situations where Criteria B1 through B4 do not identify a circuit for compliance with PRC-023-2, but the Planning Coordinator can demonstrate, based on other technical studies or assessments, that PRC-023-2 should apply to the circuit. Attachment B does not specify a finite list to avoid unnecessarily limiting the technical studies or assessments the Planning Coordinators may use to identify

[6] *Id.* at P 44.

circuits. However, NERC proposes to discuss in the NERC Report the types of studies that Planning Coordinators may use.

Issue 3

In the NOPR, the Commission proposes:

> Notwithstanding the various phrases used to describe the reliability objective, the NERC Petition indicates that the test is intended to identify all circuits in a planning coordinator's area that could have an operational impact on the reliability of the bulk electric system. The Commission proposes that the Report assess whether Attachment B is sufficiently comprehensive to capture all such circuits.[7]

NERC Response:

NERC proposes to include in the NERC Report an assessment that demonstrates whether Attachment B is sufficiently comprehensive to capture all circuits in a Planning Coordinator's area that could have an operational impact on the reliability of the Bulk Electric System in the context of transmission relay loadability.

[7] *Id.* at P 45.

IV. CONCLUSION

For the reasons stated above, NERC respectfully requests that the Commission take action consistent with these comments when it issues its Final Rule regarding the proposed Reliability Standard PRC-023-2.

Respectfully submitted,

/s/ Andrew M. Dressel

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road N.E.
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew M. Dressel
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
andrew.dressel@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 21st day of November, 2011.

/s/ Andrew M. Dressel
Andrew M. Dressel
Attorney for North American Electric Reliability Corporation

[Federal Register Volume 76, Number 225 (Tuesday, November 22, 2011)]
[Notices]
[Pages 72203-72204]
From the Federal Register Online via the Government Printing Office [www.gpo.gov]
[FR Doc No: 2011-30125]

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. AD12-5-000]

Voltage Coordination on High Voltage Grids; Notice of Reliability Workshop Agenda

As announced in the Notice of Staff Workshop issued on November 8, 2011, the Commission will hold a workshop on Thursday, December 1, 2011, from 9 a.m. to 4:30 p.m. to explore the interaction between voltage control, reliability, and economic dispatch. In addition, the Commission will consider how improvements to dispatch and voltage control software could improve reliability and market efficiency. This event will consist of two panels of industry participants. The first panel will address how entities currently coordinate economic dispatch and voltage control. The second panel will address the capability of existing and emerging software to improve coordination and optimization of the Bulk-Power System from a reliability and economic perspective. The agenda for this workshop is attached. Members of the Commission may attend the workshop.

Commission conferences are accessible under section 508 of the Rehabilitation Act of 1973. For accessibility accommodations, please send an email to accessibility@ferc.gov or call toll free 1-(866) 208-3372 (voice) or (202) 208-1659 (TTY), or send a FAX to (202) 208-2106 with the required accommodations.

Information on this event will be posted on the Calendar of Events on the Commission's Web site, http://www.ferc.gov, prior to the event.

For more information about this conference, please contact: Sarah McKinley, Office of External Affairs, Federal Energy Regulatory Commission, 888 First Street NE., Washington, DC 20426, (202) 502-8368, sarah.mckinley@ferc.gov.

Dated: November 16, 2011.
Kimberly D. Bose,
Secretary.
[GRAPHIC] [TIFF OMITTED] TN22NO11.003

Staff Workshop on Voltage Coordination on High Voltage Grids

December 1, 2011

9 a.m.-4:30 p.m.

Agenda

9-9:15 a.m.--Greeting and Opening Remarks by David Andrejcak.

9:15-11:30 a.m.--Current approaches and challenges to analyzing voltage support and reactive margin during operations planning and real-time.

Presentations: Panelists will be asked to describe how their companies currently coordinate the dispatch of reactive resources to support forecasted loads, generation and interchange transactions during operations planning and real-time. Panelists should address the following in their presentations:

a. Describe the pre-scheduling and real-time processes that involve the commitment or dispatch of reactive resources from a reliability perspective. What applications or tools are used to evaluate reactive or voltage support needs from this perspective?

b. Describe the pre-scheduling and real-time processes that involve the commitment or dispatch of reactive resources from an economic perspective. What applications or tools are used to evaluate reactive or voltage support needs from this perspective?

c. Explain whether and how pre-scheduling, real-time and post analysis evaluations are performed on the bulk electric system or on lower voltage systems to maximize opportunities for additional reliability or economic transactions.

d. Describe the situations where the dispatch of reactive resources may limit System Operating Limits or whether and how more transactions could be supported.

e. Describe how reactive power needs of the distribution system or loads are coordinated or optimized.

Panelists:

Khaled Abdul-Rahman, California Independent System Operator

Xiaochuan Luo, ISO New England

Wes Yeomans, New York Independent System Operator

Dave Zwergel, Midwest ISO

Chantal Hendrzak, PJM Interconnection

Bruce Rew, Southwest Power Pool

11:30 a.m.-1 p.m.--Lunch Break.

1-4 p.m.--The next generation of voltage support and reactive margin applications used during operations planning and real-time.

Presentations: Panelists will be asked to describe capabilities of the present and anticipated future software that can be used as decision tools to help system operators optimize voltage support resources to preserve and protect

[[Page 72204]]

reliability and support market-based economic transactions. Panelists should address the following in their presentations:

a. What are the objectives of software products available to industry that optimize the system for operations planning and real-time? (Minimize losses, maximize transfer capability, and/or minimize production costs?)

b. Describe the system optimization software products currently used or tested in industry. Discuss how widely these are used in industry.

c. Describe how these software products are evaluated and validated using a post analysis process.

d. What effort is involved in implementing the application for use in industry?

e. Discuss whether the application can be used on an interconnection-wide, Balancing Authority or local distribution system basis and, if so, how the application would be utilized.

f. Discuss whether the applications can be used to optimize reactive power resources in the distribution system or loads and coordinate with higher voltage systems.

Panelists:

Kedall Demaree, Alstom

Rod Sulte, GE

Soorya Kuloor, Gridiant

Marija Ilic, New Electricity Transmission Software Solutions (NETSS)

Dan French, Siemens

4:00-4:30 p.m.--Summary Remarks by David Andrejcak.

[FR Doc. 2011-30125 Filed 11-21-11; 8:45 am]
BILLING CODE 6717-01-P

Critical Energy Infrastructure Information Has Been Redacted From This Public Version

November 23, 2011

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: ***North American Electric Reliability Corporation,***
Docket No. RM06-16-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this filing in compliance with Paragraph 629 of the Federal Energy Regulatory Commission's ("FERC") Order No. 693. Order No. 693 requires that NERC provide a quarterly informational filing regarding the timeframe to restore power to the auxiliary power systems of U.S. nuclear power plants following a blackout as determined during simulations and drills of system restoration plans. This filing contains the referenced material pertaining to the third quarter of 2011.

NERC's filing consists of the following:

- This transmittal letter;
- A table of contents for the entire filing;
- A narrative description summarizing the data collected;
- Official Data Request to Fulfill FERC Order No. 693 Requirements: Restoration of Nuclear Power Plant Off-site Power Sources (**Exhibit A**); and
- Restoration of Nuclear Power Plant Off-site Power Sources Data: 3rd Quarter 2011 (**Exhibit B**).

Please contact the undersigned if you have any questions.

Respectfully submitted,

/s/ Andrew M. Dressel
Andrew M. Dressel

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

MANDATORY RELIABILITY STANDARDS FOR THE BULK POWER SYSTEM	**Docket No. RM06-16-000**

THIRD QUARTER 2011 COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO PARAGRAPH 629 OF ORDER No. 693

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road N.E.
Suite 600, North Tower
Atlanta, GA 30326-1001
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew M. Dressel
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
andrew.dressel@nerc.net

November 23, 2011

Critical Energy Infrastructure Information Has Been Redacted From This Public Version

TABLE OF CONTENTS

I.	Introduction	1
II.	Notices and Communications	2
III.	Summary of Restoration of Nuclear Power Plant Off-site Power Sources Data	2
IV.	Conclusion	9

EXHIBIT A – Official Data Request to Fulfill FERC Order No. 693 Requirements: Restoration of Nuclear Power Plant Off-site Sources

EXHIBIT B – Restoration of Nuclear Power Plant Off-site Power Sources Data: 3rd Quarter 2011

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

MANDATORY RELIABILITY STANDARDS FOR THE BULK POWER SYSTEM	**)** **)**	**Docket No. RM06-16-000**

THIRD QUARTER 2011 COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO PARAGRAPH 629 OF ORDER No. 693

I. INTRODUCTION

In its March 16, 2007 Order,[1] the Federal Energy Regulatory Commission ("FERC" or "Commission") directed the North American Electric Reliability Corporation ("NERC") to provide a quarterly informational filing regarding the timeframe to restore power to the auxiliary power systems of U.S. nuclear power plants following a blackout as determined during simulations and drills of system restoration plans. This filing includes information for the third quarter of 2011.

[1] *Mandatory Reliability Standards for the Bulk-Power System*, 118 FERC ¶ 61,218, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *Order on reh'g, Mandatory Reliability Standards for the Bulk-Power System*, 120 FERC ¶ 61,053 (Order No. 693-A) (2007).

II. NOTICES AND COMMUNICATIONS

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

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road N.E.
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

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

Holly A. Hawkins*
Assistant General Counsel for Standards and Critical Infrastructure Protection

Andrew M. Dressel*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
andrew.dressel@nerc.net

III. SUMMARY OF RESTORATION OF NUCLEAR POWER PLANT OFF-SITE POWER SOURCES DATA

Background

In response to comments offered by the U.S. Nuclear Regulatory Commission during the Notice of Proposed Rulemaking process, FERC expressed, in Order No. 693, its concern regarding the role and priority that nuclear power plants should have in bulk power system restoration plans. FERC addressed the concern in the discussion of the EOP-005-1 — System Restoration Plans Reliability Standard. Specifically, in Paragraph 629 of Order No. 693, FERC directed NERC as follows:

> The Commission directs the ERO to gather data, pursuant to §39.5(f) of the Commission's regulations, from simulations and drills of system restoration on the time it takes to restore power to the auxiliary power

> systems of nuclear power plants under its data gathering authority and report that information to the Commission on a quarterly basis.

EOP-005-1, Requirement R11 and sub-requirement R11.4 identify the expected priority for restoring off-site power to nuclear stations. They state:

> **R11.** Following a disturbance in which one or more areas of the Bulk Electric System become isolated or blacked out, the affected Transmission Operators and Balancing Authorities shall begin immediately to return the Bulk Electric System to normal.
>
> **R11.4.** The affected Transmission Operators shall give high priority to restoration of off-site power to nuclear stations.

Importantly, while the requirement provides the instruction to give high priority to off-site power restoration, it does not specify target timeframes.

NERC, in its role as the Electric Reliability Organization ("ERO") and in accordance with 18 C.F.R. § 39.2(d), is required to provide information as necessary to FERC in order to implement section 215 of the Federal Power Act. That same regulation obligates users, owners and operators of the bulk power system to provide the ERO with information in support of this same objective.

To collect the data necessary to respond to the FERC directive for nuclear power plant off-site power source data, NERC issued a data request following a process that was, at that time, drafted as a proposed rule of procedure. That procedure required NERC to post a proposed ERO data request for industry comment, followed by NERC Board of Trustees approval, before issuing it as a formal data request.[2] NERC posted the "nuclear data request" for a 30-day industry comment period that began on June 26, 2007. NERC reviewed the comments received and presented a final version of the data request that was adopted by the NERC Board of Trustees at its August 2, 2007 meeting.

[2] FERC has since approved Section 1600 of the Rules of Procedure, known as the Data Rule, which establishes the process for issuing ERO data requests.

The data presented in **Exhibit B** to this filing contain critical energy infrastructure information. Specifically, the information set forth in **Exhibit B** to the instant filing includes critical energy infrastructure information as defined by FERC Rules of Practice and Procedure (18 C.F.R. Part 388), FERC Orders, and NERC Rules of Procedure. The information pertains to proprietary or business design information, including design information related to vulnerabilities of critical energy infrastructure information that is not publicly available. Accordingly, the information set forth in **Exhibit B** has been redacted from the public filing. In accordance with the FERC Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided separately. NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

The ERO data request for nuclear power plant off-site power source restoration data, as approved by the NERC Board of Trustees, is found in **Exhibit A**. Following Board of Trustees approval, NERC began to collect nuclear data from U.S. Transmission Operators during the fourth quarter 2007 and will continue to collect the data quarterly until otherwise directed by FERC. This filing represents data captured for the third quarter of 2011.

The specific data requested of the Transmission Operators requests the following information:

- Reporting entity;
- Name of exercise, drill or simulation;
- Date of exercise, drill or simulation;
- Name of nuclear plant;
- Unit designation (each unit must be included separately);
- Identifier of off-site power source;

- Time duration when off-site power sources are lost to the restoration of first off-site power source (For this request, the loss of off-site power sources is the simulated physical interruption of power in support of EOP-005-1 requirements); and
- Discussion of scenario assumptions or constraints impacting the restoration of the initial off-site power source to the nuclear power plant.

In addition, the following clarifying language was included in the data request to guide the Transmission Operators when supplying the requested data.

> Simulations, drills, or exercises that are implemented for individualized operator training requirements are not included in this request. Simulations, drills, and exercises conducted to support the requirements of EOP-005-1 are included in this request. This request is not intended to require additional simulations or studies to those conducted to satisfy EOP-005-1 requirements.

It is important to note that EOP-005 focuses on restoration plans and does not contain any requirement for restoration plans specific to nuclear plants. Hence, the reporting conducted under this data request so far will not result in a tabulation resulting in reports for each US nuclear plant.

Exhibit B presents the raw data collected through this period of observation. As noted above, for the public version of this report, **Exhibit B** has been redacted to remove the actual raw data collected through the period of observation, in accordance with the data survey, and in recognition that the information requested constitutes confidential critical energy infrastructure information. Specifically, **Exhibit B** contains information that, if released, could identify system weaknesses and pose a risk of attack on existing infrastructure. NERC respectfully requests that the critical energy infrastructure information be protected consistent with national energy security objectives and in accordance with the cited regulation.

NERC has not analyzed this data to identify the impact of the reported off-site power source restoration times relative to the ability of the U.S. nuclear power plants to remain in a mode that permits a timely return to service. NERC will utilize the information contained herein to ensure applicable entities are supporting their reliability standard obligations as defined in EOP-005-1 relative to the priority of off-site power source restoration to nuclear power plants in plans for system restoration.

Summary of Data

There are 104 nuclear units in the U.S. All of these units have reported the requested information as directed. In the third quarter of 2011, Transmission Operators conducted eighteen (18) individual exercises, drills, or simulations during this period that included the restoration of off-site power sources to eighteen (18) units, with many events impacting more than one nuclear unit.[3] Transmission Operators conduct these exercises, drills, and simulations in support of EOP-005-1 and report their results to their respective Regional Entities. The Regional Entities then report their findings to NERC.

In total, sixty-two (62) off-site power source restoration "events" are included in the raw data presented in **Exhibit B** of this filing. Of the sixty-two (62) events, there were forty-four (44)[4] potential initial off-site source restorations (some units have multiple off-site sources). NERC categorized the restoration of first off-site sources in two-hour windows. Fifty (50) percent (22 of 44) of the initial off-site power source restorations occurred within the first four hours following the simulated blackout event,

[3] For example, an entity conducted one system restoration exercise on September 27, 2011 that involved the restoration of offsite power sources to three nuclear units. In the summary chart that follows below, each offsite power source restoration "event" is reported separately for purposes of data analysis.

[4] Not all units provided data for off-site sources beyond the first source restored. The data included represents only the units that provided the data and does not include the entire spectrum of off-site sources beyond the initial source for the rest of the units.

with over forty (40) percent (18 of 44) occurring in two hours or less. Four (4) sources were simulated to be restored in the 2 to 4 hour window. The data shows nineteen (19) of the potential initial sources were restored in over 10 hours.

Several Transmission Operators that reported data provided explanations of the time to restore off-site sources. For example, one (1) entity reported restoration time of eleven (11) hours and nineteen (19) minutes for the primary source. This time includes one (1) hour and forty-nine (49) minutes of measured simulation time during the exercise plus ninety (90) minutes to account for initial assessment and manning/start-up of the blackstart units plus eight (8) hours for field switching to sectionalize and reconnect circuits. Three (3) sources did not have a restoration time reported.

Total Number Offsite Power Source Restoration Events Included in EOP-005-1 Exercises, Drills or Simulations	62
Potential first off-site source restorations	44
Exercises, Drills, or Simulations in which the first off-site source was restored in 2 hours or less following the loss of power	18
Exercises, Drills, or Simulations in which the first off-site source was restored 2-4 hours following the loss of power	4
Exercises, Drills, or Simulations in which the first off-site source was restored 4-6 hours following the loss of power	0
Exercises, Drills or Simulations in which the first off-site source was restored 6-8 hours following the loss of power	0
Exercises, Drills, or Simulations in which the first off-site source was restored 8-10 hours following the loss of power	0
Exercises, Drills or Simulations in which the first off-site source was restored more than 10 hours following the loss of power	19
Exercises, Drills, or Simulations that did not achieve the restoration of the first off-site power source to a nuclear	3

power plant or that did not report a time for source restoration	

The remaining eighteen (18) events included in the data involved the restoration of a subsequent off-site source beyond the first source restored. Of those eighteen (18) events involving the restoration of a subsequent off-site source beyond the first source restored, three (3) subsequent sources were simulated to be restored in two hours or less, three (3) sources were simulated to be restored in the two to four hour window and three (3) sources were simulated to be restored in the four to six hour window. Five (5) subsequent off-site sources were restored in more than ten hours and four (4) or did not have a time reported for restoration.

IV. CONCLUSION

NERC respectfully requests that FERC accept this informational filing for the third quarter of 2011 in accordance with FERC's directive that NERC provide information regarding the time it takes to restore off-site power sources to nuclear power plants following a blackout as determined by drills and simulations.

Respectfully submitted,

/s/ Andrew M. Dressel

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road N.E.
Suite 600, North Tower
Atlanta, GA 30326-1001
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew M. Dressel
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 23rd day of November, 2011.

/s/ Andrew M. Dressel
Andrew M. Dressel

Attorney for North American Electric Reliability Corporation

Critical Energy Infrastructure Information Has Been Redacted From This Public Version

Exhibit A

Official Data Request to Fulfill FERC Order No. 693 Requirements: Restoration of Nuclear Power Plant Off-site Power Sources

Critical Energy Infrastructure Information Has Been Redacted From This Public Version

Gerry Adamski
Vice President and
Director of Standards

August 24, 2007

TRANSMISSION OPERATOR CONTACT
TITLE
COMPANY
ADDRESS
CITY, STATE ZIP CODE (TNR, 12pt)

Dear XXXXX:

Official Data Request to Fulfill FERC Order No. 693 Requirements
Restoration of Nuclear Power Plant Off-site Power Sources

Pursuant to the authority granted by FERC Order 672 and as implemented in Title 18, Section 39.2 of the Code of Federal Regulations, NERC as the appointed electric reliability organization issues this official data request as described in **Attachment 1**.

The legal basis in the United States for this authority is explained in FERC's Order 672, paragraph 114:

> 114. The Commission agrees with commenters that, to fulfill its obligations under this Final Rule, the ERO or a Regional Entity will need access to certain data from users, owners and operators of the Bulk-Power System. Further, the Commission will need access to such information as is necessary to fulfill its oversight and enforcement roles under the statute. Section 39.2 of the regulations will include the following requirement:
>
> > (d) Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.

Within the United States, failure to comply with an official data request would constitute a violation of FERC regulations. Enforcement action is available to FERC to deal with

violations of its regulations. This is authority FERC could exercise, not authority available to NERC. NERC's Compliance Monitoring and Enforcement Program, including the ability to impose penalties and sanctions, is limited to violations of reliability standards.

Please note the following additional pieces of information relative to this data request:

- An Excel spreadsheet (attached) to serve as a template for providing the requested information.
- Regional entities are requested to submit the requested information to sarcomm@nerc.net.

Thank you for your support of this effort. Please contact me should you have any questions.

Sincerely,

Enclosure

cc: James D. Castle, Chairman, Operating Reliability Subcommittee
Regional Entity Management Group

Exhibit A
Restoration of Nuclear Power Plant Offsite Power Source Data Request

Background
In paragraph 629 of Order No. 693, FERC directs NERC to provide an informational filing regarding the timeframe to restore auxiliary power to nuclear power plants following a blackout as determined during simulations and drills of system restoration plans:

> 629. "In addition the Commission directs the ERO to gather data, pursuant to § 39.5(f) of the Commission's regulations, from simulations and drills of system restoration on the time it takes to restore power to the auxiliary power systems of nuclear power plants under its data gathering authority and report that information to the Commission on a quarterly basis."

Description of Data Requested
This request is an ongoing request that begins in the fourth quarter of 2007. If an exercise, drill, or simulation includes the restoration of one or more offsite power sources to a nuclear power plant, the following information is to be prepared and provided *for each offsite power source* in a format developed and provided by NERC:

- Reporting entity
- Name of exercise, drill, or simulation
- Date of exercise, drill, or simulation
- Name of nuclear plant
- Unit designation (each unit must be included separately)
- Identifier of offsite power source
- Time duration when offsite power sources are lost to the restoration of first offsite power source. (For this request, the loss of offsite power sources is the simulated physical interruption of power in support of EOP-005-1 requirements.)
- Discussion of scenario assumptions or constraints impacting the restoration of the initial offsite power source to the nuclear power plant

Simulations, drills, or exercises that are implemented for individualized operator training requirements are not included in this request. Simulations, drills, and exercises conducted to support the requirements of EOP-005-1 are included in this request. This request is not intended to require additional simulations or studies to those conducted to satisfy EOP-005-1 requirements.

The individual data submissions should be submitted to the regional entity who will compile the data in a consolidated format. The regional entity will then forward the complied data to NERC's director of standards on a quarterly basis.

To comply with FERC directives, NERC will make a quarterly filing with FERC that includes the compiled data.

How the Data Will Be Used

The data will be provided to FERC per its directive in Order 693. FERC agrees with issues raised by the Nuclear Regulatory Commission (NRC) concerning the role and priority nuclear power plants should have in system restorations, and directs the collection of this data to aid in its review of this issue.

How the Data Will Be Collected and Validated

The regional entities are requested to coordinate the collection and composite presentation of the requested data from its member participants. Transmission operators responsive to this request are expected to validate the data to be correct prior to submittal.

Reporting Entities

Each transmission operator in the United States who has a nuclear power plant tied to a transmission line that it controls and who is participating in an exercise, drill, or simulation in support of the EOP-005-1 standard will report. Transmission operators that do not have a nuclear power plant tied to a transmission line it controls are exempt from this request.

Transmission operators outside the United States subject to EOP-005-1 are voluntarily encouraged to submit this information as well. NERC will seek permission from these non-U.S. entities for inclusion of its data in the information filed with FERC.

Due Date for the Information

If a transmission operator subject to this data request conducts a drill, simulation, or exercise that includes restoration of the initial offsite power source to a nuclear power plant, the transmission operator is to submit the requested information to its regional entity by the fifteenth of the month; following the end of the previous three-month quarter. The regional entity is to provide a quarterly report of all such submissions by April 30, July 31, October 31, and January 31 for the three-month period that concludes on these dates. This data request begins in the fourth quarter of 2007.

If no drill, exercise, or simulation meeting the criteria described above is conducted during a quarter, no submission by the transmission operator and regional entity is required. This data request does not direct transmission operators to conduct quarterly exercises, drills, or simulations to satisfy this data request. It does require the data to be reported if such a simulation, drill, or exercise is conducted.

Restrictions on Disseminating Data (Confidential/CEII)

NERC will provide this data to FERC per its Order No. 693 directives. This information will be treated as critical energy infrastructure information when submitted to FERC.

Estimate on Burden Imposed to Collect Data

There will be ongoing costs for the staff of responsible entities to respond and for regional entities to collect, compile, and report to NERC the requested data.

Exhibit B

Restoration of Nuclear Power Plant Off-site Source Data: 3rd Quarter 2011

Critical Energy Infrastructure Information Has Been Redacted From This Public Version

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RM08-13-001**
	)	

MOTION FOR AN EXTENSION OF TIME
OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 212 and 2008 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure, 18 C.F.R. §§ 385.212 and 385.2008 (2011), the North American Electric Reliability Corporation ("NERC") hereby requests an extension of time to submit a filing in the above referenced proceeding.

I. BACKGROUND

On July 30, 2008, NERC filed a Petition for Approval of Reliability Standard PRC-023-1 – Transmission Relay Loadability.[1] On May 21, 2009, the Commission issued a Notice of Proposed Rulemaking ("NOPR") that proposed to approve PRC-023-1 and to direct NERC to develop modifications to the standard.[2] NERC submitted comments in response to the NOPR on August 17, 2009.

On March 18, 2010, FERC issued Order No. 733 approving PRC-023-1 and directing several modifications:[3]

> In light of the ERO's statement that within two years it expects to submit to the Commission a proposed Reliability Standard addressing generator relay loadability, we direct the ERO to submit to the Commission an updated and specific timeline explaining when it expects to develop and submit this proposed Standard. While we recognize that generator relay loadability is a complex issue that presents different challenges than

[1] *Petition of the North American Electric Reliability Corporation for Approval of PRC-023-1 Reliability Standard*, Docket No. RM08-13-000 (July 30, 2008).
[2] *Transmission Relay Loadability Reliability Standard*, 127 FERC ¶ 61,175 (May 21, 2009).
[3] *Transmission Relay Loadability Reliability Standard*, 130 FERC ¶ 61,221 (2010) ("Order No. 733").

> transmission relay loadability, we note that more than six years have passed since the August 2003 blackout and there is still no Reliability Standard that addresses generator relay loadability. With this in mind, the Commission will not hesitate to direct the development of a new Reliability Standard if the ERO fails to propose a Standard in a timely manner...[4]

Order No. 733 also directed NERC to develop new Reliability Standards to address issues related to generator relay loadability and the operation of protective relays due to power swings. [5]

NERC filed a request for clarification and, in the alternative, rehearing of Order No. 733 on April 19, 2010.[6] On February 17, 2011, FERC issued Order No. 733-A granting clarification and, in part, rehearing of Order No. 733.[7] Specifically, Order No. 733-A clarified that certain "mandatory language" regarding Order No. 733 directives "conflicts with the Commission's references to Order No. 693 and creates the impression that the Commission prohibited NERC from developing an equally effective and efficient approach to the approach the Commission laid out in the order." Moreover, Order No. 733-A affirmed that the Commission "did not intend to prohibit NERC from exercising its technical expertise to develop a solution to an identified reliability concern that is *equally effective and efficient* as the one proposed in Order No. 733."[8] The Commission also granted a twenty-four month extension for NERC to comply with the Final Rule.[9]

On August 19, 2010, NERC posted a Standards Authorization Request ("SAR") and draft standard for Project 2010-13 — Relay Loadability Order for public comment.[10] The SAR for Project 2010-13 subdivided standard development related to Order No. 733 directives into three

---

[4] Order No. 733 at P 105.
[5] *Id*. at PP 106, 150.
[6] *Request of the North American Electric Reliability Corporation for Clarification and, in the Alternative, Rehearing of Order No. 733*, Docket No. RM08-13-001 (April 19, 2010).
[7] *Order on Rehearing, Clarification, and Request for an Extension of Time*, 134 FERC ¶ 61,127 (February 17, 2011) ("Order No. 733-A").
[8] Order No. 733-A at P 11 (*emphasis added*).
[9] Order No. 733-A at P 5.
[10] NERC Project 2010-13 SAR, Standards Announcement, available at: http://www.nerc.com/docs/standards/sar/Standards%20Announcement_final.pdf.

phases. Phase I focused on the directives requiring modifications to various elements within PRC-023-1. Phase II focused on the directives associated with development of a new standard to address generator relay loadability. Phase III focused on directives associated with developing requirements to address protective relay operations due to power swings.

II. MOTION FOR EXTENSION

By this motion, NERC is requesting an extension of time to address the directive in Order No. 733 to develop a new generator relay loadability standard, in accordance with NERC's Reliability Standards Development Plan 2012-2014.[11] As set forth in NERC's April 5, 2011 informational filing ("April 5 Informational Filing"),[12] NERC adopted a prioritization tool to assist in determining the relative priorities of projects within the NERC Standards Development portfolio. The generator relay loadability standard was not identified as a high priority project in the prioritization analysis. Therefore, NERC is requesting that the generator relay loadability project be postponed in order to focus industry resources on projects that have higher overall reliability impact. As NERC stated in the April 5 Informational Filing:

> This [prioritization] tool consider[s] various factors, including regulatory actions, overall reliability impact, stakeholder and staff experience, and project logistics. Assisted by that prioritization tool, the [NERC] Standards Committee identified a set of projects to which the majority of NERC and industry resources are being assigned. Projects already in progress that are not within this set are being moved into an "informal development" phase, where the industry may continue to perform research and analysis expected to aid in future standards development. Additionally, several projects that have not yet started have had their initiation postponed.[13]

Based on the results of NERC's 2012-2014 prioritization effort and associated work plan development, the proposed Phase II of Project 2010-13— Relay Loadability Order is expected to

[11] NERC's Board of Trustees approved the Reliability Standards Development Plan 2012-2014 on November 3, 2011.
[12] *North American Electric Reliability Corporation Reliability Standards Development Plan 2011-2013 Informational Filing Pursuant to Section 310 of the NERC Rules of Procedure*, Docket Nos. RM05-17-000, RM05-25-000, RM06-16-000 (April 5, 2011).
[13] April 5 Informational Filing at p. 2.

be moved from informal development back into formal development in the fourth quarter of 2012. This expectation relies on an assumption that current standards development project forecasts are correct, and that project priorities will not change before commencement of this project. However, under NERC's current processes, NERC's Standards Committee considers the regulatory, reliability, and logistical issues associated with projects to create or modify NERC standards, then determines the manner in which industry resources and NERC staff are deployed to create or modify those standards. Changes in resources, priorities, or other factors may result in an earlier or later expected date of initiation. Additionally, all new and modified standards must be developed following the steps outlined in the current NERC Standard Processes Manual, which ensures an open and inclusive stakeholder process through adherence to ANSI standards development principles. Accordingly, NERC's development of consensus support may also affect the initiation date.

Given the above, NERC currently forecasts that the standard or standards associated with this project will be completed and filed by the end of the third quarter of 2014. However, because development of this project has been continued on an informal basis for much of 2011, it may be that the project is completed sooner. As the April 5 Informational Filing anticipated, future prioritizations may vary and "new priorities may be created as our experience grows, as new risks are identified, that will create an ongoing need to be flexible in work planning to ensure the activities most in the interest of bulk power system reliability are given appropriate resources and priority."[14] NERC will continue to provide status updates to the Commission through the annual filings of the *Reliability Standards Development Plan* regarding the estimated start and completion dates of this project.

[14] *Id.*

NERC has agreed in the past and continues to agree that generator relay loadability is an issue that needs to be addressed. However, there are limits to how many projects may be undertaken at any one time by NERC staff and the industry volunteers that NERC relies upon to bring these projects to a successful conclusion.

III. CONCLUSION

WHEREFORE, in consideration of the foregoing, NERC respectfully requests that an extension of time be granted until the end of the third quarter of 2014 to complete this project, consistent with the results of the Reliability Standards Development Plan 2012-2014 and the associated results of the NERC prioritization tool.

Respectfully submitted,

/s/ *Willie L. Phillips*

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins @nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 22nd day of November, 2011.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RM09-25-000**
	)	

MOTION FOR AN EXTENSION OF TIME
OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 212 and 2008 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure, 18 C.F.R. §§ 385.212 and 385.2008 (2011), the North American Electric Reliability Corporation ("NERC") hereby requests an extension of time to submit a filing in the above referenced proceeding.

I. BACKGROUND

On March 16, 2007, FERC issued Order No. 693 in which it approved 83 Reliability Standards developed by NERC.[1] Additionally, FERC directed NERC to make modifications to the Personnel Performance, Training, and Qualifications ("PER") Reliability Standards.[2] On September 30, 2009, NERC submitted a petition for approval of Reliability Standards PER-005-1 and PER-004-2.[3] In that petition, NERC committed to addressing the question of whether personnel that support EMS applications should be included in mandatory training as described in the *Reliability Standards Development Plan: 2009-2011* in Project 2010-01 — Support Personnel Training.

---

[1] *Mandatory Reliability Standards for the Bulk-Power* System, Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007), *order on reh'*g Order No. 693-A, 120 FERC ¶ 61,053 (2007) ("Order No. 693").
[2] *See* Order No. 693 at P 1372-1375. *See also* Order No. 693 1342-1417.
[3] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards Regarding System Personnel Training*, Docket No. RM09-25-000 (September 30, 2009).

On June 17, 2010, FERC issued a Notice of Proposed Rulemaking ("NOPR") on proposed Reliability Standards PER-005-1 and PER-004-2 in which it sought comments from NERC and other interested persons on whether completion of the expansion of the training standard in Project 2010-01 – Support Personnel Training by the fourth quarter of 2011 is reasonable, or whether, for good cause, another timeline for completion of this work would be necessary.[4] NERC submitted comments in response to the NOPR[5] on August 23, 2010, in which NERC proposed to "resolve the directive to consider whether Generator Operators and personnel who support EMS applications should be included in a mandatory training standard within twenty-four (24) months from the date of this filing."[6]

On November 18, 2010, FERC issued Order No. 742 in which the Commission approved PER-005-1 and PER-004-2 and accepted NERC's proposal to satisfy the directive by August 23, 2012.[7] Order No. 742 provided, "…With respect to the Order No. 693 directive to consider whether personnel that support EMS applications should be included in the training Reliability Standard, we accept NERC's commitment to satisfy this directive by August 23, 2012."[8]

II. MOTION FOR EXTENSION

By this motion, NERC is requesting an extension of time to address the directive in Order No. 742, in accordance with NERC's Reliability Standards Development Plan 2012-2014.[9] As set forth in NERC's April 5, 2011 Informational Filing ("April 5 Informational Filing"),[10] NERC

[4] *System Personnel Training Reliability Standards*, 131 FERC ¶ 61,254 (June 17, 2010) ("NOPR").
[5] Comments of the North American Electric Reliability Corporation in Response to Notice of Proposed Rulemaking, Docket No. RM09-25-000 (August 23, 2010) ("Comments").
[6] Comments, p. 21.
[7] *System Personnel Training Reliability Standards*, 133 FERC ¶ 61,159 (2010) ("Order No. 742").
[8] Order No. 742 at P 86.
[9] NERC's Board of Trustees approved the Reliability Standards Development Plan 2012-2014 on November 3, 2011.
[10] *North American Electric Reliability Corporation Reliability Standards Development Plan 2011-2013 Informational Filing Pursuant to Section 310 of the NERC Rules of Procedure*, Docket Nos. RM05-17-000, RM05-25-000, RM06-16-000, (April 5, 2011).

adopted a prioritization tool to assist in determining the relative priorities of projects within the NERC Standards Development portfolio. During the prioritization effort, the project to consider whether personnel that support EMS applications should be included in the training Reliability Standard was not determined to be the highest priority on the tool's resultant priority list in either the 2011-2013 Reliability Standards Development Plan or the 2012-2014 Reliability Standards Development Plan. Therefore, NERC has postponed the start of this project in order to focus industry resources on projects that have higher overall reliability impact. As NERC stated in the April 5 Informational Filing:

> This tool consider[s] various factors, including regulatory actions, overall reliability impact, stakeholder and staff experience, and project logistics. Assisted by that prioritization tool, the [NERC] Standards Committee identified a set of projects to which the majority of NERC and industry resources are being assigned. Projects already in progress that are not within this set are being moved into an "informal development" phase, where the industry may continue to perform research and analysis expected to aid in future standards development. Additionally, several projects that have not yet started have had their initiation postponed.[11]

Based on the results of NERC's 2012-2014 prioritization effort and associated work plan development, the proposed Project 2010-01— Support Personnel Training is expected to be initiated in the fourth quarter of 2012, pending further research in early 2012 to properly define the scope of the project. This expectation relies on an assumption that current standards development project forecasts are correct, and that priorities will not change before commencement of this project. Under NERC's current processes, NERC's Standards Committee considers the regulatory, reliability, and logistical issues associated with projects to create or modify NERC standards, then determines the manner in which industry resources and NERC staff are deployed to create or modify those standards. Changes in resources, priorities, or other factors may result in an earlier or later expected date of initiation. Additionally, all new and

[11] April 5 Informational Filing at p. 2.

modified standards must be developed following the steps outlined in the current NERC Standard Processes Manual, which ensures an open and inclusive stakeholder process through adherence to ANSI standards development principles. Accordingly, NERC's development of consensus support may also affect the initiation date.

Given the above, NERC currently forecasts that the standard or standards associated with this project will be completed and filed by the end of the third quarter of 2014. However, as the April 5 Informational Filing anticipated, future prioritizations may vary, and "new priorities may be created as our experience grows, as new risks are identified, that will create an ongoing need to be flexible in work planning to ensure the activities most in the interest of bulk power system reliability are given appropriate resources and priority."[12] NERC will continue to provide status updates to the Commission though the annual filings of the *Reliability Standards Development Plan* regarding the estimated start and completion dates of this project.

NERC has agreed in the past and continues to agree that proper training of support personnel is an issue that needs to be addressed. However, there are limits to how many projects may be undertaken at any one time by NERC staff and the industry volunteers that NERC relies upon to bring these projects to a successful outcome.

III. CONCLUSION

WHEREFORE, in consideration of the foregoing, NERC respectfully requests that an extension of time be granted until the end of the third quarter of 2014 to complete the project to consider whether personnel that support EMS applications should be included in the training Reliability Standard, consistent with the Reliability Standards Development Plan 2012-2014 and the associated results of the NERC prioritization tool.

[12] *Id.*

Respectfully submitted,

/s/ *Andrew M. Dressel*

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
North American Electric Reliability Corporation
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
Andrew Dressel
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins @nerc.net
andrew.dressel@nerc.net

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 22nd day of November, 2011.

/s/ Andrew M. Dressel
Andrew M. Dressel
Attorney for North American Electric Reliability Corporation

Attachment A

BAL-003-1 Frequency Response & Frequency Bias Setting Standard

Supporting Document

Background

This document outlines the ERO process for supporting the Frequency Response Standard (FRS).

Event Selection Criteria

The ERO will use the following criteria to select FRS frequency excursion events for analysis.

1. The evaluation period for performing the annual Frequency Bias Setting and the Frequency Response Measure (FRM) calculation is December 1 of the prior year through November 30 of the current year.
2. The ERO will identify at least 25 frequency excursion events in each Interconnection for calculating the Frequency Bias Setting and the FRM. If the ERO cannot identify in a given evaluation period 25 frequency excursion events satisfying the limits specified in criteria 3 below, then similar acceptable events from the previous evaluation period also satisfying listed criteria will be included with the data set by the ERO for determining FRS compliance.
3. The ERO will use two limits to determine if an acceptable frequency excursion event for determining FRM has occurred:
    a. The change in frequency (delta F) and the arresting frequency (Point C) must exceed the excursion threshold values specified for the Interconnection in Table 1 below. Point C is the arrested value of frequency observed within 8 seconds following the start of the excursion.

		Point C	
Interconnection	**Delta F**	**Under Frequency**	**Over Frequency**
East	0.04Hz	< 59.97	> 60.03
West	0.05Hz	< 59.97	> 60.03
Texas	0.15Hz	< 59.90	> 60.10
HQ	0.20Hz	< 59.85	> 60.15

Table 1: Interconnection Frequency Excursion Threshold Values

    b. The time from the start of the rapid change in frequency until the point at which Frequency has stabilized within a narrow range should be less than 18 seconds.

4. Pre-disturbance frequency should be relatively steady and near 60.000 Hz. The A Value is computed as an average over the period from -16 seconds to 0 seconds before the frequency transient begins to decline.
5. Events that coincide with a second event that does not stabilize before the first scan used in the B-Value will not be considered.
6. Frequency excursion events occurring during periods when large interchange schedule ramping or load change is happening, and frequency excursion events occurring within 5 minutes of the top of the hour, should be excluded from consideration if other acceptable frequency excursion events can be used for analysis.
7. Select the cleanest 2 or 3 frequency excursion events occurring monthly that satisfy selection criteria. If there are not 2 frequency excursion events satisfying selection criteria occurring during the month, then other frequency excursion events from the same season of the year satisfying selection criteria should be considered for use if necessary.

To assist Balancing Authority preparation for complying with this standard, the ERO will provide quarterly posting of candidate frequency excursion events for the current year FRM calculation. The ERO will post the final list of frequency excursion events used for standard compliance by December 15 each year. Balancing Authorities are encouraged to develop scanning tools that identify candidate frequency excursion events so they are ready to access data files when needed.

NOTE: *The ERO may use for analysis of Interconnection frequency performance, but not for Balancing Authority Frequency Response, additional frequency excursion events not satisfying the criteria specified.*

Frequency Response Obligation (FRO) for the Interconnection

Each Interconnection will establish target contingency protection criteria. The default target listed in Table 2 is based on the largest category C (N-2) event identified. However, this contingency protection criterion includes a safety margin to prevent Point C from encroaching on the interconnection's highest Under Frequency Load Shed (UFLS) step for credible contingencies.

	Eastern	Western	Texas	HQ	
Starting Frequency	60	60	60	60	Hz
*Highest UFLS	59.6	59.5	59.3	58.5	Hz
Contingency Protection Criteria	4500	2740	2750	1700	MW
**Base Obligation	1125	548	229	113	MW/0.1Hz
With 25% Safety Margin	1406	685	286	141	MW/0.1Hz

Table 2: Interconnection Frequency Response Obligations

*The Eastern Interconnection set point listed is a compromise value for the highest UFLS step setting of 59.5Hz used in the east and the special protection scheme's highest UFLS step setting of 59.7Hz used in Florida. It is extremely unlikely that an event elsewhere in the Eastern Interconnection would cause the Florida UFLS special protection scheme to "false trip".

**In the Base Obligation measure for Texas, 1150 MW (Load Resources triggered by Under Frequency Relays at 59.70 Hz) was reduced from its Contingency Protection Criteria level of 2750 MW to get 229 MW/0.1 Hz. This was reduced to accurately account for designed response from Load Resources within 30 cycles.

An Interconnection may propose alternate FRO protection criteria to the ERO. The ERO will confirm the proposed alternate FRO protection criteria.

Balancing Authority Frequency Response Obligation (FRO) and Frequency Bias Setting

The ERO will manage the administrative procedure for annually assigning an FRO and Frequency Bias Setting to each Balancing Authority.

For a multiple Balancing Authority interconnection, the Interconnection Frequency Response Obligation is allocated based on either the Balancing Authority Peak Demand or peak generation. Initial FRO allocation will be based on the following method:

$$\left[\frac{\text{Projected BA Peak Load + BA installed capacity}}{\text{Projected Interconnection Peak Load + Interconnection installed capacity}}\right] \times \text{Interconnection FRO}$$

Each Balancing Authority shall report its previous year's Frequency Response Measure (FRM), Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO on FRS Form 1 by January 10 each year. If the ERO posts the official list of events after December 10, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1.

Once the ERO validates the data for all Balancing Authorities, the ERO will use FRS Form 1 data to post the following information for each Balancing Authority for the upcoming year:

- Frequency Bias Setting
- Frequency Response Obligation (FRO)

Frequency Bias Setting will be the greater of (in absolute terms) the FRM or the Interconnection minimum (as defined in Attachment B). FRS Form 1 will automatically calculate the Balancing Authority's Bias Settings. Balancing Authorities that provide Overlap Regulation will submit a FRS Form 1 that represents both the provider's and the recipient(s)' footprint. Once the data listed above is fully posted, the ERO will announce the implementation date for changing the Frequency Bias Setting.

Frequency Response Measure (FRM)

The FRM will be computed from Single Event Frequency Response Data (SEFRD), defined as: "the data from an individual event from a Balancing Authority that is used to calculate its Frequency Response, expressed in MW/0.1Hz" as calculated on FRS Form 2. The SEFRD for a typical Balancing Authority in an Interconnection with more than one Balancing Authority is basically the change in its Net Actual Interchange on its tie lines with its adjacent Balancing Authorities divided by the change in Interconnection frequency. (Some Balancing Authorities may choose to apply corrections to their Net Actual Interchange values to account for factors such as nonconforming loads. FRS Form 1 shows the types of adjustments that are allowed.) The ERO will use a standardized sampling interval of 20 to 52 seconds in the computation of SEFRD values.

Assuming data entry is correct FRS Form 1 will automatically calculate the Balancing Authority's FRM for the past 12 months as the median of the SEFRD values. A Balancing Authority electing to report as an RSG or a provider of Overlap Regulation Service will provide an FRS Form 1 for the aggregate of its participants.

BAL-003-1 Frequency Response & Frequency Bias Setting Standard
Attachment B

Process for Adjusting Minimum Frequency Bias Setting

Interconnection frequency performance is improved the closer all Balancing Authorities' (BAs') natural Frequency Response is to Frequency Bias Setting (Cohn, 1966).

The BA calculates its natural Frequency Response based on the events in FRS Form 1. The BA will set its Frequency Bias Setting to the greater of (in absolute value):

- Natural Frequency Response
- Interconnection Minimum (initially 1% of peak in BAL-003-0.1b).

For purposes of calculating the minimum Frequency Bias Setting, a Reserve Sharing Group or a Balancing Authority providing Overlap Regulation will report the projected peak demand and generation of its combined BAs' areas on FRS Form 1.

This attachment outlines the process the ERO is to use for modifying minimum Frequency Bias Settings to better meet reliability needs. The ERO may adjust the Frequency Bias Setting minimum in accordance with this Attachment B.

The ERO will post the minimum Frequency Bias Setting values on the ERO website along with other balancing standard limits.

The initial minimum Frequency Bias Settings are outlined in the following table.

Interconnection	Minimum Frequency Bias Setting (in MW/0.1Hz)
Eastern	0.8% of peak load or generation
Western	0.8% of peak load or generation
Texas	0.8% of peak load or generation
HQ	0.8% of peak load or generation

Table 1. Initial Frequency Bias Setting Minimums

The ERO will annually review Frequency Bias Setting data submitted by BAs. If an Interconnection's total minimum Frequency Bias Setting exceeds (in absolute value) the Interconnection's total natural Frequency Response by more (in absolute value) than 0.2 percentage points (of peak load expressed in MW/0.1Hz), the ERO may reduce (in absolute value) the minimum Frequency Bias Setting for BAs within that Interconnection, by 0.1 percentage point to better match that Frequency Bias Setting and natural Frequency Response.

A. Introduction

1. **Title:** **Frequency Response and Bias**
2. **Number:** BAL-003-0.1b
3. **Purpose:** This standard provides a consistent method for calculating the Frequency Bias component of ACE.
4. **Applicability:**
   - **4.1.** Balancing Authorities.
5. **Effective Date:** Immediately after approval of applicable regulatory authorities.

B. Requirements

R1. Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area.

- **R1.1.** The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change.
- **R1.2.** Each Balancing Authority shall report its Frequency Bias Setting, and method for determining that setting, to the NERC Operating Committee.

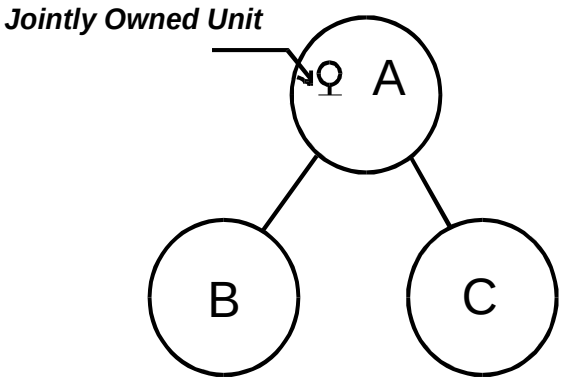
R2. Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:

- **R2.1.** The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.
- **R2.2.** The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.

R3. Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.

R4. Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting.

- **R4.1.** Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing Authorities that have fixed schedules (B and C). See the diagram below.
- **R4.2.** The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting.



R5. Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.

R5.1. Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.

R6. A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.

C. Measures

M1. Each Balancing Authority shall perform Frequency Response surveys when called for by the Operating Committee to determine the Balancing Authority's response to Interconnection Frequency Deviations.

D. Compliance

Not Specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R3 (October 23, 2007).

2. Appendix 2 — Interpretation of Requirements R2, R2.2, R5, and R5.1 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	March 16, 2007	FERC Approval — Order 693	New

0a	December 19, 2007	Added Appendix 1 — Interpretation of R3 approved by BOT on October 23, 2007	Addition
0a	July 21, 2008	FERC Approval of Interpretation of R3	Addition
0b	February 12, 2008	Added Appendix 2 — Interpretation of R2, R2.2, R5, and R5.1 approved by BOT on February 12, 2008	Addition
0.1b	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial; updated version number to "0.1b"	Errata
0.1b	October 29, 2008	BOT approved errata changes	Errata
0.1a	May 13, 2009	FERC Approved errata changes – version changed to 0.1a (Interpretation of R2, R2.2, R5, and R5.1 not yet approved)	Errata
0.1b	May 21, 2009	FERC Approved Interpretation of R2, R2.2, R5, and R5.1	Addition

Appendix 1

Interpretation of Requirement 3

Request: *Does the WECC Automatic Time Error Control Procedure (WATEC) violate Requirement 3 of BAL-003-0?*

Interpretation:

Requirement 3 of BAL-003-0 — Frequency Response and Bias deals with Balancing Authorities using Tie-Line Frequency Bias as the normal mode of automatic generation control.

> **BAL-003-0**
> **R3.** Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.

- Tie-Line Frequency Bias is one of the three foundational control modes available in a Balancing Authority's energy management system. (The other two are flat-tie and flat-frequency.) Many Balancing Authorities layer other control objectives on top of their basic control mode, such as automatic inadvertent payback, CPS optimization, time control (in single BA Interconnections).
- As long as Tie-Line Frequency Bias is the underlying control mode and CPS1 is measured and reported on the associated ACE equation, there is no violation of BAL-003-0 Requirement 3:

$$ACE = (NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME}$$

Appendix 2

Interpretation of Requirements R2, R2.2, R5, R5.1

Request: *ERCOT specifically requests clarification that a Balancing Authority is entitled to use a variable bias value as authorized by Requirement R2.2, even though Requirement 5 seems not to account for the possibility of variable bias settings.*

Interpretation:

The consensus of the Resources Subcommittee is that BAL-003-0 — Frequency Response and Bias — Requirement R2 does not conflict with BAL-003-0 Requirement R5.

BAL-003-0 — Frequency Response and Bias Requirement 2 requires a Balancing Authority to analyze its response to frequency excursions as a first step in determining its frequency bias setting. The Balancing Authority may then choose a fixed bias (constant through the year) per Requirement 2.1, or a variable bias (varies with load, specific generators, etc.) per Requirement 2.2.

BAL-003-0

R2. Each Balancing Authority shall establish and maintain a Frequency Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways:

- **R2.1.** The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours.
- **R2.2.** The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.

BAL-003-0 — Frequency Response and Bias Requirement 5 sets a minimum contribution for all Balancing Authorities toward stabilizing interconnection frequency. The 1% bias setting establishes a minimum level of automatic generation control action to help stabilize frequency following a disturbance. By setting a floor on bias, Requirement 5 also helps ensure a consistent measure of control performance among all Balancing Authorities within a multi-Balancing Authority interconnection. However, ERCOT is a single Balancing Authority interconnection. The bias settings ERCOT uses do produce, on average, the best level of automatic generation control action to meet control performance metrics. The bias value in a single Balancing Authority interconnection does not impact the measure of control performance.

BAL-003-0

R5. Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change.

- **R5.1.** Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequency Response Standard Background Document

October 2011

RELIABILITY | ACCOUNTABILITY

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

Table of Contents

Contents

Table of Contents 1

Introduction 3

Background and Rationale by Requirement 3

Requirement 1 3

Background and Rationale 3

Requirement 2 6

Background and Rationale 7

Requirement 3 7

Background and Rationale 7

Requirement 4 8

Background and Rationale 8

Requirement 5 8

Background and Rationale 9

How this Standard Meets the FERC Order 693 Directives 10

FERC Directive 10

Levels of Non-Compliance 10

Determine the appropriate periodicity of frequency response surveys necessary to ensure that Requirement R2 and other Requirements of the Reliability Standard are met 10

Define the necessary amount of Frequency Response needed for Reliable Operation for each Balancing Authority with methods of obtaining and measuring that the frequency response is achieved 10

Necessary Amount of Frequency Response 10

Methods of Obtaining Frequency Response 11

Measuring that the Frequency Response is Achieved 11
Going Beyond the Directive 12
Good Practices and Tools 13
Good Practices 13
Tools 14
Field Trial 15

Introduction

This document provides background on the development, testing and implementation of BAL-003-1 - Frequency Response Standard (FRS). The intent is to explain the rationale and considerations for the Requirements and their associated compliance information. The document also provides good practices and tips for Balancing Authorities with regard to Frequency Response.

In Order No. 693, the FERC directed additional changes to BAL-003-0.1b. This document explains how those directives are met by BAL-003-1.

The original Standards Authorization Request (SAR), finalized on June 30, 2007~~, assumed~~, assumed the Frequency Response currently available to be adequate in all the North American Interconnections. The goal of the SAR was to update the Standard to make the measurement process more objective and to provide this objective data to Planners and Operators for improved modeling. The improved models will improve understanding of the trends in Frequency Response to determine if reliability limits were being approached. The Standard would also lay the process groundwork for a transition to a performance-based Standard if reliability limits were approached.

This document will be periodically updated by the FRS Drafting Team until the Standard is approved (expected to occur during ~~Spring~~spring of 2012). Once approved, this document will then be maintained and updated by the ERO and the NERC Resources Subcommittee.

Background and Rationale by Requirement

Requirement 1

R1. Each Balancing Authority (BA) or Reserve Sharing Group (RSG) shall achieve an annual Frequency Response Measure (FRM) (as detailed in Attachment A and calculated on FRS Form 1) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each BA or RSG to maintain an adequate level of Frequency Response in the Interconnection.

Background and Rationale

R1 is intended to meet the following primary objectives:

- Determine whether a Balancing Authority (BA) has sufficient Frequency Response for reliable operations.
- Provide the feeder information needed to calculate CPS limits and Frequency Bias Settings.

With regard to the first objective, FRS Form 1 and the process in Attachment A provide the method for determining the Interconnections' necessary amount of Frequency Response and allocating it to the Balancing Authorities. The field trial for BAL-003-1 is testing an allocation methodology based on the amount of load and generation in the BA. This is to accommodate the wide spectrum of BAs from generation-only all the way to load-only.

The basic Frequency Response Obligation is based on non-coincident peak load and generation data reported in FERC Form 714 for the previous full calendar year. The basic allocation formula used by NERC is:

$$FRO_{BA} = FRO_{Int} \times \frac{Peak\ Gen_{BA} + Peak\ Load_{BA}}{Peak\ Gen_{Int} + Peak\ Load_{Int}}$$

Where:

- Peak GenBA is the average of monthly "Output of Generating Plants", FERC Form 714, column f of Part II - Schedule 3.
- Peak LoadBA is the average of "Monthly Peak Demand (MW)", FERC Form 714, column j of Part II - Schedule 3.
- Peak GenInt is the sum of all BAs' in that interconnection reported average monthly peak generation.
- Peak LoadInt is the sum of all BAs in that interconnection reported average monthly peak demand.

Balancing Authorities can approximate their FRO by multiplying their Interconnection's FRO by their share of Interconnection bias.

Balancing Authorities that merge or that transfer load or generation need to notify the ERO of the change in footprint and corresponding changes in allocation such that the net obligation for the Interconnection remains the same.

Note: The methodology for determining the Interconnection's Frequency Response Obligation and allocating it to BAs may change on the basis of field trial results. The drafting team is evaluating a risk-based approach for basing the Interconnection Frequency Response Obligation on an historic probability density of frequency error, and for allocating the obligation on the basis of the Balancing Authority's average annual ACE share of frequency error.

Attachment A proposes the following Interconnection event criteria as a basis to determine an Interconnection's Frequency Response Obligation:

- Largest category C loss-of-resource (N-2) event
- Largest total generating plant with common voltage switchyard
- Largest loss of generation in the interconnection in the last 10 years

Given the fact that the Interconnections currently have sufficient Frequency Response, few BAs should encounter problems meeting R1, particularly with the options the Standard provides with regard to obtaining Frequency Response.

With regard to the second objective above (determining Frequency Bias Settings and CPS limits), Balancing Authorities have been asked to perform annual reviews of their Frequency Bias Settings by measuring their Frequency Response, dating back to Policy 1. This obligation

was carried forward into BAL-003-01.b. While the associated training document provided useful information, it left many of the details to the judgment of the person doing the analysis. The FRS Form 1 and FRS Form 2 provide a consistent, objective process for calculating Frequency Response to develop an annual measure, the FRM.

The FRM will be computed from Single Event Frequency Response Data (SEFRD), defined as: "the data from an individual event from a Balancing Authority that is used to calculate its Frequency Response, expressed in MW/0.1Hz". The SEFRD for a typical Balancing Authority in an Interconnection with more than one Balancing Authority is basically the change its Net Actual Interchange on its tie lines with its adjacent Balancing Authorities divided by the change in Interconnection frequency. (Some Balancing Authorities may choose to apply corrections to their Net Actual Interchange values to account for factors such as nonconforming loads. FRS Form 1 shows the types of adjustments that are allowed.)

A standardized sampling interval of 20 to 52 seconds will be used in the computation of SEFRD values. Microsoft Excel® spreadsheet interfaces for EMS scan rates of 2 through 6 seconds will be provided to support the computation. During the field trial, other sampling intervals will be evaluated as well to determine if another sampling interval is more appropriate.

In an attempt to balance the workload of Balancing Authorities with the need for accuracy in the FRM, the field trial will require at least 25 samples selected during the course of the year to compute the FRM. Research conducted by the Frequency Responsive Reserve Standard Drafting Team (FRSDT) indicated that a Balancing Authority's FRM will converge to a reasonably stable value with 20 to 25 samples. The FRSDT will re-evaluate the required number of samples during the field trial.

The FRSDT also evaluated different approaches for "averaging" individual event observations to compute a technically sound estimate of Frequency Response Measure (FRM). The MW contribution for a single BA in a multi-BA Interconnection is small compared to the minute to minute changes in load, interchange and generation. For example, a 3000 MW BA in the east may only be called on to contribute 10MW for the loss of a 1000MW. The 10 MW of governor and load response may easily be masked ay a coincident change in load. Because of this large "noise to signal" ratio, the mean did not prove to be an appropriate measure of true typical performance.

In general, statisticians use the median as the best measure of central tendency when a population has outliers. Two independent reviews by the FRSDT has shown the Median to be less influenced by noise in the measurement process and the team has chosen the median as the initial metric for calculating the BAs' Frequency Response Measure.
In addition, The FRSDT is evaluating the linear regression as a means to estimate the BA's typical frequency response. This calculation is embedded in FRS Form 1 and will be evaluated during the field trial. Initial review implies that the linear regression tends to skew calculated FRM due to the influence of outliers. The outliers are being evaluated by the FRSDT as they may point to needed improvements in the measurement process or training issues for the BA in question.

In order to support field trial evaluations of sample size, sampling intervals, and aggregation techniques, the FRSDT will be retrieving scan rate data from the Balancing Authorities for each SEFRD. Additional frequency events may also be requested for research purposes, though they will not be included in the FRM computation.

FERC Order No. 693 directed the ERO to define the number of Frequency Response surveys that were conducted each year and to define a necessary amount of Frequency Response. R1 addresses both of these directives:

- There is a single annual survey of at least 25-30 events each year.
- The FRM calculated on FRS Form 1 is compared by the ERO against the FRO determined 12 months earlier (when the last FRS Form 1 was submitted) to verify the Balancing Authority provided its share of Interconnection Frequency Response.

FERC Order No. 693 also directed that the Standard should identify methods for Balancing Authorities to obtain Frequency Response. Requirement R1 allows Balancing Authorities to participate in Reserve Sharing Groups (RSGs) to provide or obtain Frequency Response. These may be the same RSGs that cooperate for BAL-002-0 or may be RSGs that form for the purposes of BAL-003-1.

If BAs participate as an RSG for BAL-003-1, compliance is based on the sum of the participants' performance.

Two other ways that BAs could obtain Frequency Response are through Supplemental Service or Overlap Regulation Service:

- No special action is needed if a BA provides or receives supplemental regulation. If the regulation occurs via Pseudo Tie, the transfer occurs automatically as part of Net Actual Interchange (NIA) and in response to information transferred from recipient to provider.
- If a BA provides overlap regulation, its FRS Form 1 will include the Frequency Bias setting as well as peak load and generation of the combined Balancing Authority Areas. The FRM event data will be calculated on the sum of the provider's and recipient's performance.

In the Violation Severity Levels for Requirement R1, the impact of a BA not having enough frequency response depends on two factors:

- Does the Interconnection have sufficient response?
- How short is the BA in providing its FRO?

The VSL takes these factors into account.

Requirement 2

R2. Each Balancing Authority not participating in Overlap Regulation Service shall implement the Frequency Bias Setting (fixed or variable) validated by the ERO, into its Area Control Error

(ACE) calculation beginning on the date specified by the ERO to ensure effectively coordinated Tie Line Bias control.

Background and Rationale

Attachment A of the Standard discusses the process the ERO will follow to validate the BA's FRS Form 1 data and publish the official Frequency Bias Settings. Historically, it has taken multiple rounds of validation and outreach to confirm each BA's data due to transcription errors, misunderstanding of instructions, and other issues. While BAs historically submit Bias Setting data by January 1, it often takes one or more months to complete the process.

The target is to have BAs submit their data by January 10. The BAs are given 30 days to assemble their data since the BAs are dependent on the ERO to provide ~~them with~~them with FRS Form 1, and there may be process delays in distributing the forms since they rely on identification of frequency events through November 30 of the preceding year.

Frequency Bias Settings generally change little from year to year. Given the fact that BAs can encounter staffing or EMS change issues coincident with the date the ERO sets for new Frequency Bias Setting implementation, the standard provides a 24 hour window on each side of the target date.

To recap the annual process:

1. The ERO posts the official list of frequency events to be used for this Standard in early December. The FRS Form 1for each Interconnection will be posted shortly thereafter.
2. The Balancing Authority submits its revised annual Frequency Bias Setting value to NERC by January 10.
3. The ERO and the Resources Subcommittee validate Frequency Bias Setting values, perform error checking, and calculate, validate, and update CPS2 L10 values. This data collection and validation process can take as long as two months.
4. Once the L10 and Frequency Bias Setting values are validated, The ERO posts the values for the upcoming year and also informs the Balancing Authorities of the date on which to implement revised Frequency Bias Setting values. Implementation typically would be on or about March 1st of each year.

Requirement 3

R3. Each Balancing Authority not receiving Overlap Regulation Service shall operate its Automatic Generation Control (AGC) in Tie Line Bias mode to ensure effectively coordinated control, unless such operation would have an Adverse Reliability Impact on the Balancing Authority's Area.

Background and Rationale

This requirement serves several functions. The primary reason for operating in Tie Line Bias is so ACE is calculated properly for performance purposes. Even if a BA temporarily operated in manual mode, as long as CPS is properly calculated and the BA met CPS, it is operating reliably.

There are legitimate reasons for taking AGC out of Tie Line Bias or operating manually including:

- Telemetry problems that lead the operator to believe ACE is significantly in error.
- The frequency input to AGC is not reflective of the BA's true frequency (such as if the control center were operating a local generator and disconnected from the Interconnection).
- During restoration (where one BA might be controlling frequency while another to which it is connected is managing interchange between them).
- For training purposes.
- Many AGC systems will automatically switch to an alternate mode if the EMS determines Tie Line Bias control could lead to problems.
- For single BA Interconnections, Flat Frequency and Tie Line Bias are equivalent.

Because it is rare that temporary operation out of Tie Line Bias can lead to reliability problems, the VSLs for this requirement are structured accordingly.

Requirement 4

R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify its Frequency Bias Setting in its ACE calculation to be equivalent to the sum of the Frequency Bias Settings of the participating Balancing Authorities as validated by the ERO or calculate the Frequency Bias Setting based on the entire area being combined and thereby represent the Frequency Response for the combined area being controlled.

Background and Rationale

This requirement reflects the operating principles first established by NERC Policy 1 and is similar to Requirement R6 of the approved BAL-003-0.1b standard. Overlap Regulation Service is a method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing Authority's actual interchange, frequency response, and schedules into the providing Balancing Authority's AGC/ACE equation.

As noted earlier, a BA that is providing Overlap Regulation will report the sum of the Bias Settings in its FRS Form 1. Balancing Authorities receiving Overlap Regulation Service have an ACE and Frequency Bias Setting equal to zero (0).

Requirement 5

R5. In order to ensure adequate control response each Balancing Authority shall use a monthly average Frequency Bias Setting whose absolute value is at least equal to one of the following:

- *The minimum percentage of the Balancing Authority Area's estimated yearly Peak Demand within its metered boundary per 0.1 Hz change as specified by the ERO in accordance with Attachment B.*

- *The minimum percentage of the Balancing Authority Area's estimated yearly peak generation for a generation- only BA, per 0.1 Hz change as specified by the ERO in accordance with Attachment B.*

Background and Rationale

BAL-003-0.1b standard requires a minimum Frequency Bias Setting equal in absolute value to one percent of the Balancing Authority's estimated yearly peak demand (or maximum generation level if native load is not served). For most Balancing Authorities this calculated amount of Frequency Bias is significantly greater in absolute value than their actual Frequency Response characteristic (which represents an over-bias condition) resulting in over-control since a larger magnitude response is realized. This is especially true in the Eastern Interconnection where this condition requires excessive secondary frequency control response which degrades overall system performance and increases operating cost as compared to requiring an appropriate balance of primary and secondary frequency control response.

Balancing Authorities were given a minimum Frequency Bias Setting obligation because there had never been a mandatory Frequency Response Obligation. This historic "one percent of peak per 0.1Hz" obligation, dating back to NERC's predecessor, NAPSIC, was intended to ensure all BAs provide some support to Interconnection frequency.

The ideal system control state exists when the Frequency Bias Setting of the Balancing Authority exactly matches the actual Frequency Response characteristic of the Balancing Authority. If this is not achievable, over-bias is significantly better from a control perspective than under-bias with the caveat that Frequency Bias is set relatively close in magnitude to the Balancing Authority actual Frequency Response characteristic. Setting the Frequency Bias to better approximate the Balancing Authority natural Frequency Response characteristic will improve the quality and accuracy of ACE control, CPS & DCS and general AGC System control response. This is the technical basis for recommending an adjustment to the long standing "1% of peak/0.1Hz" Frequency Bias Setting. Attachment B is intended to bring the Balancing Authorities' Frequency Bias Setting closer to their natural Frequency Response. Attachment B balances the following objectives:

- Bring the Frequency Bias Setting and Frequency Response closer together.
- Ensure there is no negative impact on other Standards (CPS, BAAL and to a lesser extent DCS) by adjustments in the minimum Frequency Bias Setting, by accommodating only minor adjustments.
- Do not allow the Frequency Bias Setting minimum to drop below natural Frequency Response, because under-biasing could affect an Interconnection adversely.

Finally, for BAs using variable bias, FRS Form 1 has a data entry location for the previous year's average monthly bias. The Balancing Authority and the ERO can compare this value to the previous year's Frequency Bias Setting minimum to ensure R5 has been met.

How this Standard Meets the FERC Order 693 Directives

FERC Directive

The following is the relevant paragraph of Order No. 693.

> *Accordingly, the Commission approves Reliability Standard BAL-003-0 as mandatory and enforceable. In addition, the Commission directs the ERO to develop a modification to BAL-003-0 through the Reliability Standards development process that: (1) includes Levels of Non-Compliance; (2) determines the appropriate periodicity of frequency response surveys necessary to ensure that Requirement R2 and other requirements of the Reliability Standard are being met, and to modify Measure M1 based on that determination and (3) defines the necessary amount of Frequency Response needed for Reliable Operation for each balancing authority with methods of obtaining and measuring that the frequency response is achieved.*

1. Levels of Non-Compliance

VRFs and VSLs are an equally effective way of assigning compliance elements to the standard.

2. Determine the appropriate periodicity of frequency response surveys necessary to ensure that Requirement R2 and other Requirements of the Reliability Standard are met

BAL-003 V0 R2 (the basis of Order No. 693) deals with the calculation of Frequency Bias Setting such that it reflects natural Frequency Response.

The drafting team has determined that a sample size on the order of at least 25-30 events is necessary to have a high confidence in the estimate of a BA's Frequency Response. Selection of the frequency excursion events used for analysis will be done via a method outlined in Attachment A to the Standard.

On average, these events will represent the largest 2-3 "clean" frequency excursions occurring each month.

Since Frequency Bias Setting is an annual obligation, the survey of the at least 25-30 frequency excursion events will occur once each year.

3. Define the necessary amount of Frequency Response needed for Reliable Operation for each Balancing Authority with methods of obtaining and measuring that the frequency response is achieved

Necessary Amount of Frequency Response

The drafting team has proposed the following approach to defining the necessary amount of frequency response. In general, the goal is to avoid triggering the first step of under-frequency load shedding (UFLS) in the given Interconnection for reasonable contingencies expected. The

methodology for determining each Interconnection's and Balancing Authority's obligation is outlined in Attachment A to the Standard.

It should be noted that the standard cannot guarantee that there will never be a triggering of UFLS as the magnitude of "point C" differs throughout an interconnection during a disturbance and there are local areas that see much wider swings in frequency.

The contingency protection criterion is the largest reasonably expected contingency in the Interconnection. This can be based on the largest observed credible contingency in the previous 10 years or the largest Category C event for the Interconnection.

The Safety Margin included addresses the difference between Points B and C and accounts for variables.

For multiple BA interconnections, the Frequency Response Obligation is allocated to BAs based on size. This allocation will be based on the following calculation:

$$FRO_{BA} = FRO_{Int} \times \frac{\text{Peak Gen}_{BA} + \text{Peak Load}_{BA}}{\text{Peak Gen}_{Int} + \text{Peak Load}_{Int}}$$

Methods of Obtaining Frequency Response

The drafting team believes the following are valid methods of obtaining Frequency Response:

- Supplemental regulation.
- Overlap regulation.
- Contractual service (The drafting team has developed an approach to obtain a contractual share of Frequency Response from Adjacent Balancing Authorities. See FRS Form 1). While the final rules with regard to contractual services are being defined, the current expectation is that the ERO and the associated Region(s) should be notified beforehand and that the service be at least 6 months in duration.
- Through a tariff (e.g. Frequency Response and regulation service).
- From generators through an interconnection agreement.
- Contract with an internal resource or loads (The drafting team encourages the development of a NAESB business practice for Frequency Response service for linear (droop) and stepped (e.g. LaaR in Texas) response).

Measuring that the Frequency Response is Achieved

FRS Form 1 and the underlying data retained by the BA will be used for measuring whether Frequency Response was provided. FRS Form 1 will provide the guidance on how to account for and measure Frequency Response.

Going Beyond the Directive

Based on the combined operating experience of the SDT, the drafting team believes each Interconnection has sufficient Frequency Response. If margins decline, there may be a need for additional standards or tools. The drafting team and the Resources Subcommittee are working with the ERO on its Frequency Response Initiative to develop processes and good practices so the Interconnections are prepared. These good practices and tools are described in the following section.

The drafting team is also evaluating a risk-based approach for basing the Interconnection Frequency Response Obligation on an historic probability density of frequency error, and for allocating the obligation on the basis of the Balancing Authority's average annual ACE share of frequency error. This allocation method uses the inverse of the rationale for allocating the CPS1 epsilon requirement by Bias share.

Good Practices

Knowing the quantity and depth of frequency responsive reserves in real time is a possible next step to being better prepared for the next event. The challenge in achieving this is having the knowledge of the capabilities of all sources of frequency response. Presently the primary source of frequency response remains with the generation resources in our fleets. Understanding how each of these sources performs to changes in system frequency and knowing their limitations would improve the BA's ability to measure frequency responsive reserves. Presently there are only guidelines, criteria and protocols in some regions of the industry that identify specific settings and performance expectations of primary frequency response of resources. One method of gaining better understanding of performance is to measure performance during actual events that occur on the system. This approach would only provide feedback for performance during that specific event and would not provide insight into depth of response or other limitations. Repeated measurements will increase confidence in expected performance. NERC modeling standards are in process to be revised that will improve the BA's insight into predicting available frequency responsive reserves. However, knowing how resources are operated, what modes of operation provide sustained primary frequency response and knowing the operating range of this response would give the BA the knowledge to accurately predict frequency response and the amount of frequency responsive reserves available in real time.

Some benefits on several interconnections have been realized by communicating to generation resources (GO) the importance of operating in modes that allow primary frequency response to be sustained by the control systems of the resource. Other improvements in implementation of primary frequency response have been achieved through improved settings on turbine governors through the elimination of "step" frequency response with the simultaneous reduction in governor dead-band settings. Improvements in the full AGC control loop of the

generating resource, which accounts for the expected primary frequency response, have improved the delivery of quality primary frequency response while minimizing secondary control actions of generators. Some of these actions can provide quick improvement in delivery of primary frequency response.

Once primary frequency response sources are known the BA could calculate available reserves that are frequency responsive. Planning for these reserves during normal and emergency operations could be developed and added to the normal planning process.

Tools

Single generating resource primary frequency response performance evaluation tools for steam turbine, combustion turbine (simple cycle or combined cycle) and for intermittent resources are available at the following link.
http://texasre.org/standards_rules/standardsdev/rsc/sar003/Pages/Default.aspx.

These tools and the regional standard associated with them are in their final stages of development in the Texas region.

These tools will be posted on the NERC website.

Field Trial

This section is a summary of the Field Trial activities that have been or will be conducted by the ERO, the Resources Subcommittee and the FRS Drafting Team.

1. The NERC BA recommendation (alert) and observations.√
2. The NERC governor recommendation (alert) and observations.√
3. The 2011 bias calculation √
    1. Evaluate measurement methodology√
    2. Serve as initial training for BAs√
    3. Evaluate median, mean, regression and possibly other measures√
    4. Evaluate sample size (to address the directive of frequency of surveys) √
    5. Evaluate impact of inclusion/exclusion of internal contingencies √
    6. Improve FRS Form 1√
4. Create supporting process for FRS Form 1 √
    1. For Interconnection benchmarking (proving adequacy of frequency response)
    2. Evaluating trend
    3. Test process for developing candidate list for FRS Form 1
5. 2012 bias calculation
    1. Further refinement of items in 2011 bias calculation
    2. Test the FRO allocation methodology
    3. Test approach for handling variable bias
    4. Evaluate 12 month vs. 24 month rolling average approach to performance
6. Evaluate reduction in bias setting floor below 1% (initially 0.8% in 2012) to evaluate impact on frequency and calculated CPS and BAAL performance.
7. Evaluate effectiveness of administrative process to support the standard.
8. Evaluate a risk-based approach for basing the Interconnection Frequency Response Obligation on an historic probability density of frequency error, and for allocating the obligation on the basis of the Balancing Authority's average annual ACE share of frequency error.

Body content goes here. Body content goes here. Body content goes here. Body content goes here.

DRAFT:DNC:March 2, 2005

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Interconnection for Wind Energy And Other Technologies	Docket No. RM05-4-000

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

The North American Electric Reliability Council, a New Jersey non-profit corporation ("NERC")[1], is pleased to provide these comments in response to the issues and questions raised in the Commission's January 24, 2005 Notice of Proposed Rulemaking, Interconnection for Wind Energy and Other Alternative Technologies. NERC supports the Commission's initiatives to assure that wind generation plays an appropriate role in the Nation's mix of generation resources. NERC believes that significant amounts of wind generation can reliably be added to the bulk electric system, so long as all those involved in the planning and operation of these wind plants (generator owners, generator operators, transmission owners, transmission planners and transmission operators) adhere to established reliability standards.

[1] NERC was formed after the Northeast blackout in 1965 to promote the reliability of the interconnected electric systems in North America. Its mission is to ensure that the bulk electric systems that serve North America are adequate, reliable, and secure. It works with all segments of the electric industry as well as customers to "keep the lights on" by developing and encouraging compliance with rules for the reliable operation and adequacy of supply of these systems. NERC comprises ten regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC's comments address several technical questions[2] raised in the NOPR:

1. Low Voltage Ride Through Standard
2. Supervisory Control and Data Acquisition ("SCADA") Capability
3. Power Factor Design Criteria (Reactive Power)
4. Other Generating Technologies

As a general matter, NERC believes that standards for the reliable planning and operation of bulk electric system facilities should be contained in the standards set by NERC and the regional reliability councils. Such standards may then be incorporated by reference into various agreements. The Commission has already followed that approach in the pro forma Large Generator Interconnection Agreement adopted in Order No. 2003, by including provisions requiring the Parties to abide by Good Utility Practice. The Commission recently concluded that the term Good Utility Practice includes compliance with NERC's new reliability standards. [3]

1. Low Voltage Ride Through Standard

The NOPR would require wind generator plants to have the low voltage ride through capabilities described in Figure 1 of the proposed Appendix G of the Interconnection Requirements for Wind Generators. NERC agrees with a requirement that wind generator plants have the ability to ride through low-voltage transients, but NERC does not agree that Figure 1 properly states the requirement.

NERC Reliability Standard TPL–002-0, System Performance Following Loss of a Single BES [Bulk Electric System] Element, requires the Planning Authority and the Transmission Planner to ensure that the bulk electric system will remain stable with

[2] NERC is not providing comments on the questions related to requiring the transmission provider to participate in updating the models for assessing the interconnection impacts and the wind plant's self-study of the feasibility of an interconnection.

[3] Supplement to Policy Statement on Matters Relating to Bulk Power System Reliability, Docket No. PL04-5-001, issued February 9, 2005.

thermal and voltage limits within applicable ratings, and with no loss of demand or curtailed firm transfers, for a normally cleared fault on a single element (an interval of several cycles). If a fault occurs on a transmission line near a wind plant, the voltage measured at that point could drop instantaneously to 0 for the short interval required to clear the fault. Figure 1 would permit a wind generator to trip offline if voltage drops below 15 % of nominal voltage. Unless the wind plant stays on line through a normally cleared fault, its capacity will be lost to the system, in effect creating a double contingency (loss of the line and loss of the plant) and a violation of TPL-002-0.

Including Figure 1 in the Commission's regulations has other disadvantages. NERC understands that the intent of Figure 1 is to have a reasonable requirement for system reliability and also meet the physical capabilities of existing generation technology. But wind technology is advancing rapidly. If Figure 1 is included in the Commission's rule, it is likely to be static over time and may limit technological development. Figure 1 also may not be appropriate for every application of wind generation at every wind plant location, because reliability needs may require different engineering or operating procedures over the North American electric system. Protection schemes especially must be coordinated across regional areas.

For these reasons, NERC does not believe that Figure 1 should be part of Appendix G. Instead, it should be replaced with a requirement that wind plants directly connected to the bulk transmission system meet the requirements of NERC and regional council reliability standards.

2. Supervisory Control and Data Acquisition ("SCADA") Capability

The NOPR would require the Transmission Provider[4] and the wind generator owner to determine the SCADA requirements for each interconnection of a wind generator to the transmission system. SCADA capability is necessary to facilitate the required exchange of data and control between the wind generation plant and the Transmission Provider. SCADA also provides critical information that the balancing authority needs to minimize the balancing area's area control error and that the transmission operator needs to maintain transmission voltage within acceptable limits. NERC agrees with the requirement that the wind generator owner provide SCADA information to the Transmission Provider and the balancing authority. The specific SCADA requirements should be established between the wind generator owner and the Transmission Provider and the balancing authority, which would make it unnecessary to establish a minimum SCADA requirement for Appendix G.

3. Power Factor Design Criteria (Reactive Power)

The NOPR would require a wind generator (1) to maintain a power factor range from 0.95 lagging to 0.95 leading, measured at the high voltage side of the substation transformer, and (2) to have sufficient dynamic reactive support to interconnect to the transmission system, based on the results of the System Impact Study. NERC agrees with the requirement that a wind generator plant be able to operate at a power factor range between 0.95 lagging and 0.95 leading, measured at the high side of the step-up transformer. This requirement is consistent with NERC guidelines for synchronous generators and the requirements the Commission has already adopted in Order No. 2003 for large generators. The wind generator plant should also maintain the voltage schedule

[4] NERC considers the FERC-defined Transmission Provider as the combination of the transmission operator, transmission owner, and the transmission service provider, or tariff administrator.

requirements of the transmission system operator. The wind generation plant should have adequate dynamic reactive capability to respond dynamically to transient voltages on the transmission system.

The transmission provider's decision to waive dynamic support requirements can be viewed as a commercial decision between the transmission provider and the wind generator owner, and NERC has no comment on this issue. However, that transmission provider, in conjunction with the transmission owner, continues to be responsible for ensuring that the dynamic reactive support requirements of the transmission system are provided to meet NERC and regional council reliability standards.

4. Other Generating Technologies

The NOPR asks if there are other generation technologies that should comply with the provisions of the proposed Appendix G. NERC believes that the proposed Appendix G, with the recommendations NERC has provided in this document, could be appropriate for any generation device other than a synchronous generator. However, NERC will reserve judgment on this question, preferring to review the other generation technologies as they develop before providing a definitive answer.

Conclusion

NERC is dedicated to improving the reliability and security of the bulk power system and looks forward to working with FERC and electric industry stakeholders in the development of appropriate interconnection requirements for groupings of wind generators.

Respectfully submitted,

NORTH AMERICAN
ELECTRIC RELIABILITY COUNCIL
By:

David N. Cook
Vice President & General Counsel
116-390 Village Blvd.
Princeton, NJ 08540-5731
(609) 452-8060
david.cook@nerc.net

NERC Recommended Changes to the FERC/AWEA LVRT Standard

A. Technical Standards Applicable to a Wind Generating Plant

i. Low Voltage Ride-Through (LVRT) Capability

A wind generating plant shall be able to remain online during voltage disturbances up to the time periods and associated voltage levels set forth in the standard in Figure 1, below, ~~if the Transmission Provider's System Impact Study shows that low voltage ride-through capability is required to ensure safety or reliability.~~ unless clearing the fault effectively disconnects the wind generating plant from the system.

The standard applies to voltage measured at the high side of the wind generating plant step-up transformer(s) ~~Point of Interconnection as defined in this LGIA~~. The figure shows the ratio of actual to nominal voltage (on the vertical axis) over time (on the horizontal axis). Before time 0.0, the voltage at the high side of the wind generating plant step-up transformer(s) is the nominal voltage. At time 0.0, the voltage may drop~~s~~ to zero (0). The wind plant must stay connected to the system if the voltage drops to zero (0) during the system fault normal clearing period (not to exceed 9.0 cycles: 0.15 seconds). ~~If the voltage remains at a level greater than 15 percent of the nominal voltage for a period that does not exceed 0.625 seconds, the plant must stay online.~~ Further, ~~if the voltage returns to 90 percent of the nominal voltage within 3.0 seconds of the beginning of the voltage drop (with the voltage at any given time never falling below the minimum voltage indicated by the solid line in Figure 1), the plant must stay online.~~ if the voltage at any given time remains at or above the curve proposed by NERC in Figure 1, the wind generating plant must stay online. After 3 seconds, the wind plant must not trip if the voltage remains at or above 90%. The Interconnection Customer may not disable low voltage ride-through equipment while the wind plant is in operation. Two key features of this regulation that are applicable to voltages measured at the high side of the wind generating plant step-up transformers are:

1. A wind generating plant must have low voltage ride-through capability down to ~~15 percent~~ zero (0) volts of the rated line voltage ~~for 0.625 seconds~~ during the system fault normal clearing period (not to exceed 9 cycles: 0.15 seconds);

2. ~~A wind generating plant must be able to operate continuously at 90 percent of the rated line voltage, measured at the high voltage side of the wind plant substation transformer(s).~~ If the voltage at any given time remains at or above the curve proposed by NERC in Figure 1, the wind generating plant must stay online.

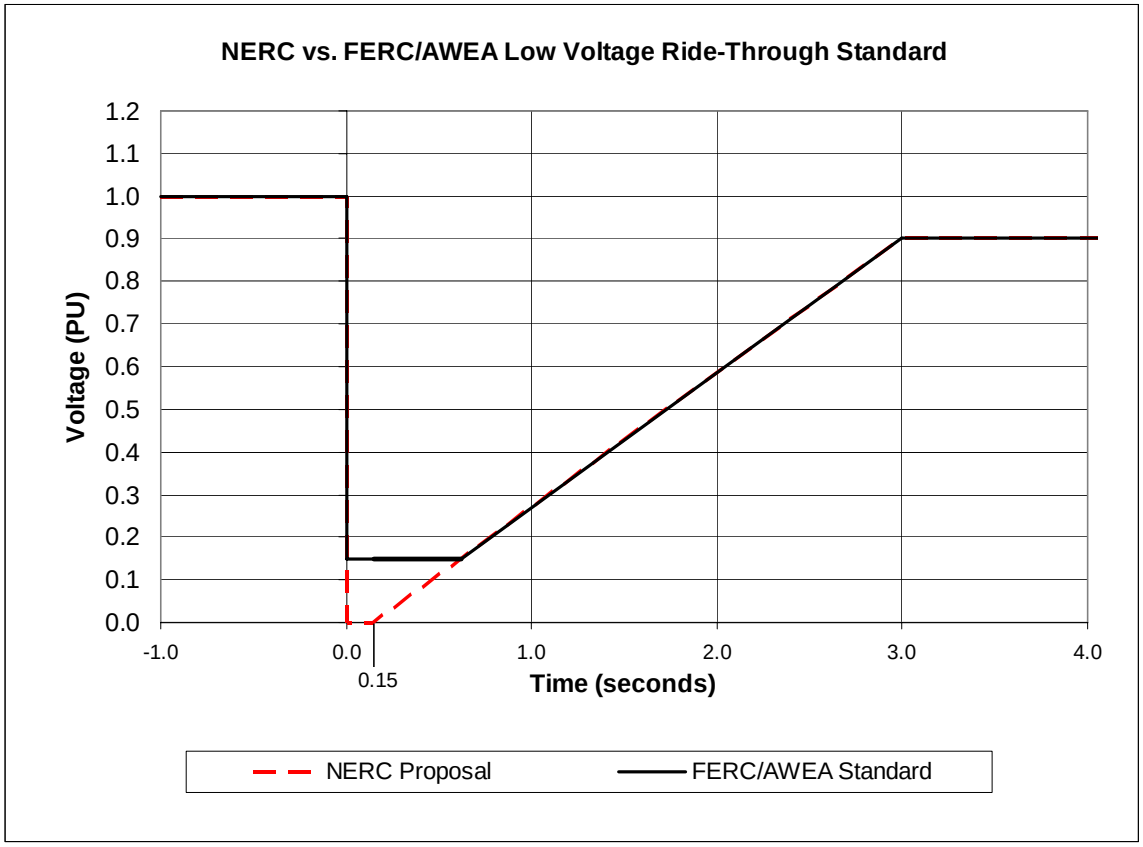


Figure 1: Proposed low voltage ride-through standard (NERC Modifications)

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

111 FERC ¶ 61,353
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 35

(Docket No. RM05-4-000 – Order No. 661)

Interconnection for Wind Energy

(Issued June 2, 2005)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final Rule

SUMMARY: The Federal Energy Regulatory Commission (Commission) is amending its regulations to require public utilities to append to their standard large generator interconnection procedures and large generator interconnection agreements in their open access transmission tariffs (OATTs) standard procedures and technical requirements for the interconnection of large wind generation.

EFFECTIVE DATE: This final rule will become effective [**INSERT DATE 60 DAYS FROM THE DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

FOR FURTHER INFORMATION CONTACT:

Bruce A. Poole (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8468

G. Patrick Rooney (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-6205

P. Kumar Agarwal (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8923

LaChelle Brooks (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6522

Jeffery S. Dennis (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-6027

SUPPLEMENTARY INFORMATION

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Interconnection for Wind Energy Docket No. RM05-4-000

ORDER NO. 661

FINAL RULE

(Issued June 2, 2005)

Table of Contents Page No.

I. Introduction 2
II. Background 4
III. Discussion 8
A. Low Voltage Ride-Through Capability 11
1. Comments 13
2. Commission Conclusion 18
B. Power Factor Design Criteria (Reactive Power) 24
1. Comments – Power Factor Range and General Application of Requirement 27
2. Commission Conclusion - Power Factor Range and General Application of Requirement 30
3. Comments – Point of Interconnection 34
4. Commission Conclusion – Point of Interconnection 34
5. Comments – Dynamic Reactive Power Capability 35
6. Commission Conclusion – Dynamic Reactive Power Capability 38
C. Supervisory Control and Data Acquisition Capability 40
1. Comments 41
2. Commission Conclusion 44

Table of Contents Page No.

D. Wind Plant Interconnection Modeling 46
1. Comments 47
2. Commission Conclusion 47
E. Self-Study of Interconnection Feasibility 47
1. Comments 48
2. Commission Conclusion 51
F. Applicability to Other Generating Technologies 55
1. Comments 55
2. Commission Conclusion 56
G. Variations from the Final Rule 58
1. Comments 58
2. Commission Conclusion 59
H. Transition Period 59
1. Comments 59
2. Commission Conclusion 61
I. Miscellaneous Comments 62
1. Commission Conclusion 63
J. Compliance Issues 64
IV. Information Collection Statement 65
V. Environmental Analysis 67
VI. Regulatory Flexibility Act Certification 68
VII. Document Availability 69
VIII. Effective Date and Congressional Notification 70

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

111 FERC ¶ 61,353
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Pat Wood, III, Chairman;
Nora Mead Brownell, Joseph T. Kelliher,
and Suedeen G. Kelly.

Interconnection for Wind Energy Docket No. RM05-4-000

ORDER NO. 661

FINAL RULE

(Issued June 2, 2005)

1. In this Final Rule, to meet our responsibility under sections 205 and 206 of the Federal Power Act (FPA)[1] to remedy undue discrimination, the Commission adopts standard procedures and technical requirements for the interconnection of large wind plants. The Commission requires all public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to append to the Large Generator Interconnection Procedures (LGIPs) and Large Generator Interconnection Agreements (LGIAs) in their Open Access Transmission Tariffs (OATTs) the Final Rule Appendix G adopted here. These standard technical requirements provide just and reasonable terms for the interconnection of wind plants.[2] The rule recognizes the technical differences of

[1] 16 U.S.C. §§ 824d-e (2000).

[2] As discussed in greater detail below, the Final Rule Appendix G applies only to wind plants, due to the unique characteristics of wind generating technology.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

wind generating technology, and benefits customers by removing unnecessary obstacles to further development of wind generating resources while ensuring that reliability is protected.

I. Introduction

2. In Order No. 2003,[3] the Commission adopted standard procedures and a standard agreement for the interconnection of large generation facilities. The Commission required public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to file revised OATTs containing these standard provisions, and use them to provide interconnection service to generating facilities having a capacity of more than 20 megawatts.

3. In Order No. 2003-A, on rehearing, the Commission noted that the standard interconnection procedures and agreement were based on the needs of traditional synchronous generation facilities and that a different approach might be more appropriate for generators relying on non-synchronous technologies,[4] such as wind plants.[5]

---

[3] Standardization of Generator Interconnection Agreements and Procedures, Order No. 2003, 68 Fed. Reg. 49,845 (Aug. 19, 2003), FERC Stats. & Regs., Regulations Preambles ¶ 31,146 (2003) (Order No. 2003), order on reh'g, 69 Fed. Reg. 15,932 (Mar. 24, 2004), FERC Stats & Regs., Regulations Preambles ¶ 31,160 (2004) (Order No. 2003-A), order on reh'g, 70 Fed. Reg. 265 (January 4, 2005), FERC Stats & Regs., Regulations Preambles ¶ 31,171 (2004) (Order No. 2003-B), reh'g pending; see also Notice Clarifying Compliance Procedures, 106 FERC ¶ 61,009 (2004).

[4] A wind generator is considered non-synchronous because it does not run at the same speed as a traditional generator. A non-synchronous generator possesses significantly different characteristics and responds differently to network disturbances.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Accordingly, the Commission granted certain clarifications, and also added a blank Appendix G (Requirements of Generators Relying on Non-Synchronous Technologies) to the standard LGIA for future adoption of requirements specific to non-synchronous technologies.[6]

4. Therefore, in a Notice of Proposed Rulemaking (NOPR), the Commission proposed technical standards applicable to the interconnection of large wind generating plants[7] to be included in Appendix G of the LGIA.[8] We proposed the standards in light of our findings in Order No. 2003-A noted above and in response to a petition submitted by the American Wind Energy Association (AWEA) on May 20, 2004.[9] The Commission proposed to adopt certain technical requirements that Transmission Providers would be required to apply to interconnection service for wind generation plants, which are different from those required of traditional synchronous generating plants. These standard technical requirements are now needed because of the increased

---

[5] Order No. 2003-A at P 407, n.85.

[6] Id.

[7] Large wind generating plants are those with an output rated over 20 MW at the point of interconnection.

[8] See Interconnection for Wind Energy and Other Alternative Technologies, Notice of Proposed Rulemaking, 110 FERC ¶ 61,036 (2004) (NOPR).

[9] See Petition for Rulemaking or, in the Alternative, Request for Clarification of Order No. 2003-A, and Request for Technical Conference of the American Wind Energy Association (May 20, 2004), filed in Docket Nos. RM02-1-005 and PL04-15-000.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

presence of larger aggregated wind plants on many Transmission Providers' systems. The NOPR stated that, except for those articles of the LGIA for which wind plants have been exempted,[10] these requirements would supplement the standard interconnection procedures and requirements adopted by the Commission in Order No. 2003. Additionally, the NOPR sought comments on certain specific issues, including whether there are other non-synchronous technologies, or other technologies in addition to wind, that should also be covered by the proposed Appendix G.

II. Background

5. In Order No. 2003, to meet our responsibility under sections 205 and 206 of the FPA to remedy undue discrimination, the Commission required all public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to append to their OATTs the LGIP and LGIA. To achieve greater standardization of interconnection terms and conditions, Order No. 2003 required such public utilities to file revised OATTs containing the LGIP and LGIA included in Order No. 2003.

6. As explained above, because some of the technical requirements in the LGIA were inappropriate for non-synchronous technologies (such as wind generators), the Commission clarified in Order No. 2003-A that LGIA article 5.4 (Power System Stabilizers), LGIA article 5.10.3 (Interconnection Customer's Interconnection Facilities

[10] LGIA article 5.4 (Power System Stabilizers), LGIA article 5.10.3 (Interconnection Customer's Interconnection Facilities Construction), and LGIA article 9.6.1 (Power Factor Design Criteria).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Construction) and LGIA article 9.6.l (Power Factor Design Criteria) would not be applied to wind generators.[11] Additionally, the Commission noted that "there may be other areas of the LGIP and LGIA that may call for a slightly different approach for a generator relying on newer technology because it may have unique electrical characteristics."[12]

7. On May 20, 2004, in Docket No. RM02-1-005, AWEA submitted a petition for rulemaking or, in the alternative, request for clarification of Order No. 2003-A, and a request for a technical conference. AWEA asked the Commission to adopt in Appendix G certain standards for the interconnection of wind generation plants. Specifically, AWEA submitted a proposed Appendix G that it argues addresses the concerns of both Transmission Providers and the wind generation industry. AWEA's proposed Appendix G included a low voltage ride-through capability standard that would allow the Transmission Provider to require as a condition of interconnection that wind generation facilities have the ability to continue operating or "ride through" certain low voltage conditions on the transmission systems to which they are interconnected. AWEA's proposed Appendix G also included that as a condition of interconnection, wind plants would install equipment enabling remote supervisory control and data acquisition (SCADA) that would limit the maximum plant output during system emergency and

[11] Id. at P 407, n. 85.

[12] Id.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

system contingency events and telemetry communication between the system operator and the wind plant for automatic forecasting and scheduling. Additionally, AWEA proposed that the power factor design criteria of up to 0.95 leading/lagging (required in Order No. 2003) be applied to wind generation plants, with flexibility regarding whether the reactive support equipment would be located at the common point of interconnection of all the generators in the plant rather than at the high side of the wind plant substation transformers. Further, AWEA proposed that the Commission require Transmission Providers and wind generator manufacturers to participate in a formal process to develop, update, and improve the engineering models and specifications used in modeling wind plant interconnections. Finally, AWEA proposed to include language in Appendix G allowing the wind Interconnection Customer to "self-study" interconnection feasibility by entering the interconnection queue without providing certain power and load flow data required of other large generators, receiving certain information from the Transmission Provider, and conducting its own Feasibility Study.

8. On September 24, 2004, the Commission held a Technical Conference to discuss the issues raised by AWEA's petition, including the technical requirements for the interconnection of wind plants and other such alternative technologies and the need for specific requirements for their interconnection. Additionally, the Technical Conference considered how wind and other alternative generator technologies may respond differently to transmission grid disturbances and have different effects on the

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

transmission grid. The Commission also solicited and received post-Technical Conference comments from interested persons.

9. As noted above, the Commission's NOPR proposed to adopt in Appendix G to the LGIA a somewhat modified version of the low voltage ride-through, SCADA and power factor design standards proposed by AWEA in its May 20, 2004 petition. Specifically, the NOPR proposed to establish uniform standards in Appendix G that would require large wind plants seeking to interconnect to the grid to (1) demonstrate low voltage ride-through capability; in other words, show that the plant can remain on line during voltage disturbances up to specified time periods and associated voltage levels; (2) possess SCADA capability to transmit data and receive instructions from the Transmission Provider; and (3) maintain a power factor within the range of 0.95 leading to 0.95 lagging, measured at the high voltage side of the substation transformers. In the case of the low voltage ride-through requirement, the Commission proposed to permit the Transmission Provider to waive the requirement on a comparable and not unduly discriminatory basis for all wind plants. In the case of the power factor requirement, the Commission proposed to permit the Transmission Provider to waive or defer compliance with the requirement where it is not necessary. The Commission declined, however, to adopt AWEA's proposal to allow a wind generator to "enter the interconnection queue and conduct its own Feasibility Study, having obtained the information necessary to do so

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

upon paying the initial deposit and submitting its interconnection application."[13] We asked for comments on how to balance the need of wind generators to obtain certain data from the Transmission Provider before completing their Interconnection Requests with the need to protect critical energy infrastructure information and commercially sensitive data against unwarranted disclosure.

III. Discussion

10. Based on AWEA's petition, the comments received during and after the Technical Conference, and the comments filed in response to the NOPR, the Commission is adopting certain standard procedures and technical requirements for the interconnection of wind generating plants, as discussed in greater detail below. These procedures and technical requirements will be appended, as Appendix G, to both the LGIP and the LGIA.[14]

[13] See AWEA Petition at 13.

[14] In the NOPR, the Commission proposed to include Appendix G as an attachment to the LGIA only. Upon further consideration, the Commission directs that the Final Rule Appendix G provisions related to completion of the Interconnection Request by a wind plant interconnection customer be appended to the LGIP, since they are procedural in nature, and that the remaining technical requirements be appended to the LGIA, to ensure that the provisions adopted here are applied throughout the interconnection process.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

11. These technical requirements for the interconnection of wind plants recognize the unique design and operating characteristics of wind plants,[15] their increasing size and increasing level of penetration on some transmission systems (in terms of the wind generating capacity's percentage contribution to total system generating capacity), and the effects they have on the transmission system. In Order No. 2003, the Commission noted that in the past, requests for interconnection frequently resulted in complex and time-consuming disputes over technical matters such as feasibility, cost, and cost responsibility.[16] That is true for wind interconnection as well as interconnection of more conventional generation. The special standard procedures we are adopting for the interconnection of large wind plants will minimize opportunities for undue discrimination by Transmission Providers and remove unnecessary obstacles to the development of wind generation, while protecting system reliability.[17] Like the LGIP and LGIA in Order No. 2003, the Final Rule Appendix G is to be added to the OATT of each public utility that

[15] As noted above, wind plants over 20 MW in total size are subject to the standard technical requirements in the Final Rule Appendix G. These wind plants are generally made up of several small induction wind generating turbines, laid out over a large area, and connected through a medium-voltage collector system. This collector system is connected to the low voltage side of the step-up transformer, which is then connected to the transmission system at a single Point of Interconnection.

[16] Order No. 2003 at P 11.

[17] See id. at P 11-12.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

owns, controls, or operates facilities for transmitting electric energy in interstate commerce.

12. The Final Rule Appendix G we adopt here applies only to the interconnection of wind plants. As discussed further below, the Commission does not believe at this time that the standard procedures and technical requirements in this Final Rule are appropriate for other alternative generating technologies that may supply over 20 MW at one Point of Interconnection. The standard procedures and technical requirements adopted here recognize the unique characteristics of wind plants, including the fact that they use induction generators, consist of several or numerous small generators connected to a collector system, and do not respond to grid disturbances in the same manner as large conventional generators.

13. The Appendix G procedures and technical requirements for the interconnection of wind generation plants are not the sole interconnection requirements for wind plants; large wind plants are subject to the other standard interconnection procedures and requirements adopted by the Commission in Order No. 2003, unless wind plants are exempted from such procedures and requirements by Order No. 2003 and its rehearing orders, and this order.

14. Additionally, as discussed further below, the Commission adopts a reasonable transition period for the technical requirements adopted in the Final Rule. Specifically, the standard technical requirements, if applicable, for low voltage ride-through capability, SCADA capability, and power factor design criteria apply only to LGIAs signed, filed

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

with the Commission in unexecuted form, or filed as a non-conforming agreement, on or after January 1, 2006, or the date six months after publication of the Final Rule in the Federal Register, whichever is later. The procedural requirements related to the completion of the Interconnection Request by a wind plant Interconnection Customer, however, apply when the Final Rule takes effect, which is 60 days after the date of publication in the Federal Register.[18]

A. Low Voltage Ride-Through Capability

15. As the Commission stated in the NOPR, early wind generator technology would shut down the wind generating unit if there was a sudden change in voltage on the transmission system. With the increasing number and size of wind plants in the United States, there is a concern that wind plants tripping off-line during a low voltage situation could raise significant reliability concerns. As a result, Transmission Providers state that they need large wind plants to remain on-line during low voltage occurrences to maintain reliability. Further, in the past, Transmission Providers would often shut down wind units during a system disturbance. Wind generators would prefer to stay on-line, but they are concerned that having each Transmission Provider design its own low voltage ride-

[18] As discussed in greater detail below, in this Final Rule the Commission is adopting procedures that permit a wind plant Interconnection Customer to provide in the Interconnection Request a set of electrical design specifications that depict the wind plant as a single generator. These procedures recognize that the unique characteristics of wind plants do not permit them to submit a detailed electrical design in the initial Interconnection Request stage, and allow wind plants to enter the queue and receive the base case data necessary to provide a detailed design to the Transmission Provider.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

through requirement would greatly affect wind turbine manufacturing costs. As a result, both wind generators and most Transmission Providers support having a low voltage ride-through standard for large wind plants.

16. The NOPR proposed to require that large wind plants seeking to interconnect to the transmission system demonstrate low voltage ride-through capability, unless waived by the Transmission Provider on a comparable and not unduly discriminatory basis for all wind plants. Specifically, the NOPR Appendix G would require that wind generating plants demonstrate the ability to remain on-line during voltage disturbances up to the time periods and associated voltage levels set forth in Figure 1 of the NOPR. We proposed to measure voltage levels at the high voltage side of the wind plant substation transformer. The NOPR noted that while low voltage ride-through capability is needed for wind plants, it is less of a concern for large synchronous generating facilities because most of these facilities are equipped with automatic voltage control devices to increase output during low voltage events.

17. The NOPR sought comments on the proposed low voltage ride-through standard. In particular, the Commission was interested in comments addressing whether it should adopt a low voltage ride-through standard at all, whether the proposed standard or another standard is appropriate, and whether the proposed standard is specific enough. Specifically, the Commission sought comments on whether the required time periods and associated voltage levels proposed in Figure 1 of the NOPR Appendix G were appropriate or should be modified.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

1. Comments

18. Several commenters, including AWEA,[19] Western, FirstEnergy, and the Midwest ISO, state that they support the low voltage ride-through standard in Figure 1 of the NOPR. Midwest Reliability Organization suggests, however, that the standard could be in article 9.6 of the LGIA. CenterPoint contends that the reliability concerns presented by the failure of a large wind plant to ride through a low voltage event also exist if other generators also fail to ride through such events, and thus would apply a low voltage ride-through requirement to all generators. Western supports the standard as proposed, with the understanding that it may need to be modified later if it causes unforeseen problems on the transmission system.

19. Numerous other entities support the proposed low voltage ride-through requirement with modifications. For instance, numerous commenters, including AWEA, PacifiCorp-PPM Energy, FPL Energy, Southern California Edison, AEP, Xcel, PJM, National Grid and Southern, believe that the required voltage should be measured at the point of interconnection, as opposed to the high side of the wind plant substation transformer.

20. Additionally, several entities dispute the specific time periods and associated voltage levels set forth in Figure 1 of the proposed Appendix G. American

[19] See AWEA Reply Comments (April 1, 2005) at 10. Specifically, AWEA asks that the proposed low voltage ride-through standard be adopted, specifically the proposed standard of Figure 1.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Superconductor states generally that the proposed low voltage ride-through curve in Figure 1 of the NOPR is unrealistic and does not resemble voltage situations that wind plants are likely to encounter. It also argues that the low voltage requirement proposed in the NOPR is not comparable to what is required of conventional generators. Midwest ISO TOs, CenterPoint and Xcel assert that requiring the low voltage ride-through capability to go only to 15 percent of the rated line voltage (as set out in Figure 1 of the NOPR) may be too high and may present reliability problems. They recommend that the Figure 1 low voltage ride-through profile require the wind turbine to ride through low voltage at zero percent of the rated line voltage for 150 milliseconds. NUSCo recommends that the Commission require wind generators to ride through a fault with zero percent of the rated line voltage at the point of interconnection for 250 milliseconds (15 cycles). American Transmission argues that the low voltage ride-through curve of Figure 1 should show the voltage to be at 0.90 per unit prior to time zero. ISO New England states that to the extent the Commission adopts a low voltage ride-through requirement, it should require wind plants to remain connected to the transmission system for a zero voltage level for the time period associated the typical time it takes to clear a normal design contingency fault.[20]

[20] NERC similarly states that to meet its general reliability standards for system performance, wind plants should remain online "through a normally cleared fault." NERC Comments at 3. Also, PJM states that wind plants should be required to operate during a zero voltage level at the Point of Interconnecton until the fault is cleared by primary protective devices on the Transmission System.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

21. Several of the commenters, including AWEA, Gamesa, and GE suggest that the low voltage ride-through standard should be clarified to apply only to three-phase faults. AWEA also asks that the requirement be clarified to state that a wind plant would not be expected to continue to operate in low voltage situations where the wind farm is tripped off-line following a fault if (a) this action is performed intentionally under a special protection scheme, or (b) if the fault is on the Transmission Provider's side of the Point of Interconnection and clearing the fault would effectively disconnect the wind plant from the system. Midwest ISO TOs and Montana-Dakota Utilities also seek clarification regarding application of the proposed standard to unbalanced phase voltages.

22. Many commenters, while supportive of requiring wind plants to possess low voltage ride-through capability, argue that the specific standard should be permitted to vary based on reliability needs. For example, the New York PSC, while agreeing that large wind plants should possess low voltage ride-through capability, argues that the specific voltage-time standard should be developed on a case-by-case basis to reflect system needs. Midwest ISO TOs similarly contend that Transmission Providers should be able to establish different low voltage ride-through standards on a case-by-case basis. NYISO asserts that the low voltage ride-through standard proposed by the Commission should be a minimum performance requirement, and that Transmission Providers should have the flexibility to require a higher low voltage ride-through standard if the particular site location or wind plant design requires a higher standard to protect system reliability. Similarly, LIPA suggests that the Commission adopt a two-part low voltage ride-through

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

standard; the first part would be the standard proposed in the NOPR, while the second part would apply a more stringent low voltage ride-through standard where the studies indicate that the NOPR requirements are inadequate, such as in locations with special reliability concerns. ISO New England recommends that the Commission not adopt a specific standard for low voltage ride-through capability, or alternatively, that the standard serve only as a guideline for wind turbine manufacturers. BPA and NERC contend that the development of low voltage ride-through standards should be left to the Western Electricity Coordinating Council, NERC, regional reliability councils, the Institute of Electrical and Electronics Engineers (IEEE), and the American National Standards Institute.[21] American Superconductor, Nevada Power, and NUSCo, among others, assert that the low voltage ride-through standard should be based on established regional reliability standards. Likewise, NorthWestern Energy asks that the standard be modified to allow the Transmission Provider to use the reliability council standard in effect when the LGIA is signed.

23. FPL Energy asks that the proposed low voltage ride-through requirement be modified so that the determination of whether a wind plant must have low voltage ride-through capability is made on a case-by case basis. According to FPL Energy, the NOPR would have the "unintended consequence" of mandating costly low voltage ride-through

[21] Similarly, EEI suggests that the Commission adopt standards on an interim basis, until NERC, the regional reliability councils, or IEEE establish formal standards.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

technology for all wind plants because Transmission Providers will not be able to determine that the capability will never be needed.[22] FPL Energy argues that the Commission's Final Rule should require the Transmission Provider to determine through the System Impact Study, on a case-by-case basis, whether the wind plant is required to possess low voltage ride-through capability. It notes that currently, Transmission Providers may not require an Interconnection Customer to be responsible for Network Upgrades that are not identified in the studies as necessary, and that a similar process should apply to the low voltage ride-through requirement. Finally, FPL Energy expresses concern that the use of the term "demonstrate" in the proposed requirement could be interpreted to require the wind plant to physically demonstrate the capability, risking harm to its electrical equipment.

24. With regard to the Commission's proposal to permit the Transmission Provider to waive the low voltage ride-through requirement, NUSCo and Tucson Electric both argue that no waiver of the low voltage ride-through requirement should be permitted. NUSCo asserts that the reliability of one Transmission Provider's system may be affected by the grant of a waiver by a neighboring Transmission Provider.

[22] FPL Energy estimates that for a 100 MW wind farm, the cost of low voltage ride-through exceeds $1.5 million.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

25. Xcel and LIPA believe there should also be a high voltage ride-through standard for wind plants, comparable to the high voltage ride-through standards for conventional generators.

2. Commission Conclusion

26. As discussed further below, we adopt the low voltage ride-through standard proposed in the NOPR, but will not require that it be met unless the System Impact Study shows that it is needed. Specifically, under the requirement we adopt in this Final Rule, a wind plant is required to satisfy the low voltage ride-through standard if the Transmission Provider shows, through the System Impact Study, that such capability is required to ensure safety or reliability. This differs from the NOPR, which proposed to require low voltage ride-through capability in all cases, except when the Transmission Provider waived the requirement on a comparable and not unduly discriminatory basis for all wind plants. Additionally, the Final Rule adopts the Point of Interconnection as the point of measurement for the low voltage ride-through standard, instead of the proposed high side of the wind plant substation transformers, and replaces the term "demonstrate" with "possess." We also grant certain clarifications, as discussed further below.

27. The Commission believes that establishing the achievable low voltage ride-through standard in this Final Rule if the Transmission Provider shows that it is necessary to maintain safety or reliability provides certainty to wind plant developers that their interconnection to the grid will not be frustrated, and limits opportunities for undue discrimination. A requirement based on a uniform standard ensures that wind developers

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

are not faced with widely varying interconnection standards in different areas of the country, which would increase manufacturing costs needlessly. We believe that in the long run this is in the best interests of the wind industry and customers, as it helps provide a secure and reliable power supply, and will facilitate increased use of wind as a generation resource while ensuring that reliability is protected.

28. As noted above, the Commission requires low voltage ride-though capability only if the Transmission Provider shows that it is needed on a case-by-case basis, as FPL Energy requests. Specifically, low voltage ride-through capability is required only if the Transmission Provider shows, through the System Impact Study, that it is required to ensure the safety or reliability of the Transmission Provider's transmission system. Given that Transmission Providers have responsibility for ensuring the reliable operation of their systems (pursuant to NERC and regional reliability council standards), the Commission believes that they are in the best position to establish whether low voltage ride-through capability is needed in individual circumstances. The System Impact Study is the best vehicle for assessing the need for such capability, and this study should determine if there is a need for a wind plant to remain on-line during low voltage events to ensure the safety or reliability of the system. Requiring low voltage ride-through capability only if the System Impact Study shows it to be necessary ensures that the increased reliance on wind plants does not degrade system safety or reliability. It also ensures that the Transmission Provider does not require a wind plant to install costly equipment that is not needed for grid safety or reliability. This limits the opportunities

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

for undue discrimination; a wind plant Interconnection Customer will not have its interconnection frustrated by unnecessary requirements to install costly equipment that is not needed for safety or reliability. Should the wind plant Interconnection Customer disagree with the Transmission Provider that the System Impact Study shows that low voltage ride-through capability is needed, it may challenge the Transmission Provider's conclusion through dispute resolution or appeal to the Commission.

29. Given our decision to apply the low voltage ride-through capability standard only on a case-by-case basis if the Transmission Provider shows, through the System Impact Study, that it is needed to ensure safety or reliability, there is no need for the waiver provision in the NOPR. As a result, issues raised by commenters regarding the waiver provision are moot.

30. As noted above, many entities representing a broad mix of market participants request that the low voltage ride-through requirement be modified to require that the voltage be measured at the Point of Interconnection, as opposed to the high voltage side of the wind plant substation transformer. Given the need to protect grid safety and reliability by having wind plants ride through low voltage events where necessary, and continue to provide output at the point where the plant and its associated interconnection facilities join the grid, we will do so. Use of this measurement point recognizes that the Point of Interconnection is the point at which the Interconnection Customer's responsibility ends and the Transmission Provider's responsibility begins. Additionally, this change to the NOPR is broadly supported, and simplifies the interconnection process

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

by maintaining the same Point of Interconnection definition adopted in Order No. 2003.

31. We also find convincing FPL Energy's argument that using the term "demonstrate the ability" could be interpreted to require the wind plant to physically demonstrate that it has low voltage ride-through capability and thus could lead to unnecessary tests that could harm the wind plant electrical equipment. Accordingly, we replace the term "demonstrate the ability" with "be able."

32. We also clarify certain portions of the low voltage ride-through standard. First, we clarify that the low voltage ride-through requirement, and the time periods and associated voltage levels set forth in Appendix G, Figure 1, apply to three-phase faults.[23] This is because three-phase faults are the most severe, whereas two-phase or single-phase faults drop the voltage to a level not as low as that specified in Figure 1. Further, in response to AWEA, we clarify that a wind plant is not required to satisfy the standard in Appendix G, Figure 1 if the wind plant is intentionally tripped off line following a fault under a "special protection scheme"[24] agreed to by the Transmission Provider. These

[23] A three-phase fault is an unintentional short circuit condition involving all three phases in an electric system. It is the most severe in its impact, but occurs least frequently. For complete reliability, it is virtually universal to design an electric system for three-phase faults. Other types of faults are: single line-to-ground fault, line-to-line fault, and double line-to-ground fault.

[24] A special protection scheme is an automatic protection scheme designed to detect abnormal or predetermined system conditions and take corrective actions to

(continued)

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

situations may include a fault on the Transmission Provider's side of the Point of Interconnection, as well as a fault other than a three-phase fault covered by the low voltage ride-through standard.

33. We reject the requests that the standards be only guidelines. The Commission sets forth in this Final Rule a low voltage ride-through standard that it believes, after consideration of the comments from all interested entities, including the wind industry, is achievable and will maintain grid safety and reliability while facilitating the increased use of wind resources. As noted above, the Commission is setting a standard for low voltage ride-through to provide certainty and diminish the opportunities for undue discrimination. Permitting Transmission Providers to set their own specific low voltage ride-through standards would create too great a risk that this opportunity would be used to frustrate wind plant interconnections or to favor a Transmission Provider's wind generating affiliate.

34. In response to comments suggesting that we should allow NERC and the regional reliability councils to establish low voltage ride-through standards, we are aware of the work being done by these organizations to address wind plant interconnection standards. However, no such standards are available today, and Transmission Providers and wind Interconnection Customers are looking for interconnection standards to apply now. If

---

maintain system reliability. Such actions may include changes in demand, generation, or system configuration to maintain acceptable voltage or power flows.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

other entities develop an alternate standard, a Transmission Provider may seek to justify adopting them as variations from Appendix G, as discussed below. Additionally, the Commission would consider a future industry petition to revise Appendix G to conform to NERC developed standards.

35. With respect to Midwest ISO TOs' concern that Appendix G, Figure 1 does not contain information on how the standard would apply to unbalanced voltages in close proximity to the point of interconnection,[25] we note that it is impossible to identify all possible conditions and circumstances that may arise on the transmission system. The low voltage ride-through standard is a general one that will be adequate under most circumstances. We recognize that special circumstances may occur. These may be identified by the System Impact Study, which should identify any additional protection requirements in addition to this standard. We also note that, as discussed below, the Commission permits variations from the Final Rule Appendix G that are "consistent with or superior to" the standard provisions, that are based on regional reliability council requirements, or that are offered by independent entities such as Regional Transmission Organizations (RTOs) or Independent System Operators (ISOs).

36. Similarly, we are not persuaded to alter the specific time periods and associated voltage levels in Figure 1 of the NOPR Appendix G. The low voltage ride-through

[25] Additionally, a number of commenters suggest low voltage ride-through levels and timing or cycling standards different from those reflected in the NOPR Appendix G, Figure 1.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

standard proposed in that figure and adopted here is close to the standard used in other countries and was presented to the Commission by representatives of the wind industry as an achievable requirement. Several commenters, including Transmission Providers, support the standard as one that would safeguard reliability. The Western Electricity Coordinating Council (WECC), a regional reliability council, has approved a similar low voltage ride-through standard. The standard we adopt in this Final Rule is an international standard that has been accepted for use by the Alberta Electric System Operator and Germany, and was developed following detailed study. We do not believe it would be appropriate to deviate from such a widely-accepted and achievable standard in this rulemaking.

37. We are not convinced of a need for a separate high voltage ride-through standard for wind generators. The record developed here does not indicate that this is a general concern across the country. Parties that believe a high voltage ride-through standard is required should ask NERC or the regional reliability councils to address this need. A Transmission Provider may seek to justify variations from Appendix G to establish these requirements under the variation provisions of Order No. 2003 and its rehearing order, as briefly summarized below in section III.G, "Variations from the Final Rule."

B. Power Factor Design Criteria (Reactive Power)

38. The Commission stated in the NOPR that until recently, Transmission Providers did not require wind generators to have the capability to provide reactive power because the generators were generally small and had little effect on the transmission grid.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

However, because of the larger size of many of the wind plants being built and the increased presence of wind energy on various transmission systems, the Commission proposed to require wind plants to operate within a specified power factor range to help balance the reactive power needs of the transmission system.

39. Specifically, the NOPR proposed to require that large wind plants maintain a power factor within the range of 0.95 leading to 0.95 lagging (as required by Order No. 2003), to be measured at the high voltage side of the wind plant substation transformer.[26] In Appendix G of the NOPR, we further proposed to allow wind plants flexibility in how they meet the power factor requirement; for example, using either power electronics designed to supply this level of reactive capability, fixed and switched capacitors if agreed to by the Transmission Provider, or a combination of the two.[27] Additionally, the NOPR proposed to allow the Transmission Provider to waive the power factor requirement for wind plants where it is not needed at that location or for a generating facility of that size, provided that such waiver is not unduly discriminatory (that is, is offered on a comparable basis to similarly situated wind plants). The NOPR stated, however, that if the Transmission Provider waived the power factor requirement, the

[26] This proposed measurement point is different from Order No. 2003, which measures the power factor at the Point of Interconnection.

[27] Conventional generators inherently provide reactive power, whereas most induction-type generators used by wind plants currently can only provide reactive power through the addition of external devices.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

interconnection agreement would be considered a non-conforming agreement under section 11.3 of the LGIP and thus would have to be filed with the Commission. The NOPR also proposed to require that wind plants have the capability to provide sufficient dynamic (as opposed to static) voltage support to interconnect to the transmission system, if the System Impact Study shows that dynamic capability is necessary for system reliability.[28]

40. The NOPR sought comments about whether the proposed power factor range should be increased or decreased for wind generating plants. It also sought comments as to whether any dynamic (i.e., controllable) reactive capability should be required of wind plants, and if so, how much. Finally, the NOPR sought comments on the proposed waiver provision.

41. The comments received fall into several categories, including the general application of a power factor requirement to wind plants and the waiver provisions, the power factor range and operation within that range, measurement of the power factor requirement at the point of interconnection, and whether dynamic reactive power capability should be a requirement. These subcategories are separately addressed below.

[28] NOPR at P 18.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

1. Comments – Power Factor Range and General Application of the Requirement

42. Western, NERC, BPA and Great River support the proposed power factor range of 0.95 leading to 0.95 lagging (hereinafter stated as +/- 0.95). Southern California Edison agrees that the proposed power factor range is appropriate unless it is waived by the Transmission Provider.

43. Numerous other commenters state that they support the standard, but that the Transmission Provider should be allowed to impose a wider power factor range on a wind generating plant to maintain the reliability of the transmission system. American Superconductor, for instance, believes that the +/- 0.95 power factor range should be adopted as a standard except in cases where the Transmission Provider's System Impact Study indicates that additional reactive support is needed. Similarly, EEI asserts that the wind plant should operate within the +/- 0.95 power factor range unless the Transmission Provider has established a different standard that applies to all generators in its control area. New York PSC agrees with the NOPR power factor range, but argues that the Transmission Provider should be able to require a power factor of 0.90 lagging if the System Impact Study indicates it is needed for system reliability. FirstEnergy and American Transmission believe that to ensure a greater level of reliability, the Commission should adopt a power factor range of 0.90 lagging to 0.95 leading. NRECA-APPA maintains that while most Transmission Providers impose the +/- 0.95 power factor requirement on conventional generators, some impose a larger range, such

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

as 0.90 lagging to 0.95 leading, to meet reliability criteria. In that situation, they contend that the Transmission Provider should be allowed to impose that same wider power factor range on wind generating plants. In similar comments, NYISO urges the Commission to (1) consider the power factor standard a minimum requirement, as opposed to a maximum, and (2) find that the large wind farms should not be able to depend on the transmission system interconnection for the plants' excitation power.

44. NRECA-APPA and Xcel also state that the standard is unclear about whether the wind generator can operate anywhere in the +/- 0.95 range. Xcel asks that the Commission clarify whether the wind generator is expected to operate over the entire +/- 0.95 power factor range or at a specified point within that range.

45. Several commenters assert that the adherence to the Transmission Provider's voltage schedule is more important than merely maintaining a power factor within the specified range. NRECA-APPA asks that the wind plant be required to comply with the Transmission Provider’s voltage schedule directives. PacifiCorp/PPM Energy asks the Commission to revise the proposed power factor standard to require the Transmission provider to specify a power factor or voltage control set point within the 0.95 leading to 0.95 lagging range. PacifCorp/PPM Energy also contends that the parenthetical in the proposed Appendix G (stating “taking into account any limitations due to voltage level, real power output, etc.”) is ambiguous and should be eliminated.

46. AWEA argues that we should specify the minimum real power output of the wind facility at which the +/- 0.95 power factor range would apply. It states that to be clear

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

about the limits of this standard, the reactive power output criteria should use a minimum real power output set at greater than 10 percent of the rated output of the generator. FPL Energy states that General Electric wind turbines cannot meet the proposed power factor standard over the full range of real power output, and that dynamic VAR control (DVAR) banks or static capacitors would have to be installed at an additional expense to meet the proposed power factor over the entire range. FPL Energy asserts that such costs would provide limited reliability benefits.

47. Zilkha, FirstEnergy, NorthWestern Energy, and BPA indicate that the Transmission Provider should be allowed to waive the power factor requirement where it is not required. NUSCo, ISO New England and Midwest ISO TOs oppose allowing such a waiver. Midwest ISO TOs argue that if the Commission allows waiver, it should require that, where the Transmission Provider granting the waiver is not also the owner, the Transmission Owner approve the waiver. AWEA asserts that the proposed requirement that an interconnection agreement be filed with the Commission as a non-conforming agreement if the Transmission Provider has waived the reactive power requirement is inappropriate and inconsistent with Order No. 2003-A.

48. AWEA and FPL Energy ask that the +/- 0.95 power factor standard not be required of a wind plant unless the Transmission Provider shows that it is needed for system safety or reliability. FPL Energy states that the Transmission Provider should have the burden of demonstrating that the reactive power standard is needed. It suggests that the Commission use the same test it used in the NOPR for dynamic voltage support,

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

which requires that the Transmission Provider, before requiring such capability, must show that it is necessary for system reliability. The CPUC recommends a "least cost, best fit" approach to dealing with the reactive power requirement needs of wind farms.

49. Southern California Edison states that because reactive power at wind generating plants may be produced from devices external to the generator, a time delay may be necessary to allow for switching of reactive resources to enable the wind generator to operate at the appropriate power factor within the +/- 0.95 power factor range. It states, however, that exempting the wind generating plant altogether from the power factor requirement is inappropriate.

2. Commission Conclusion - Power Factor Range and General Application of the Requirement

50. We adopt the power factor range of +/- 0.95 for large wind generating plants. We modify other parts of the proposed requirements. First, this Final Rule requires the wind plant to maintain the required power factor range only if the Transmission Provider shows, through the System Impact Study, that such capability is required of that plant to ensure safety or reliability. This differs from the NOPR, which required the wind plant to maintain the required power factor in all cases, except if the Transmission Provider waived or deferred compliance with the reactive power standard. Establishing an achievable reactive power standard if it is needed for safety or reliability provides assurance to wind plant developers that their interconnection to the grid will not be frustrated or face uncertainty due to a lack of standards, and thus will limit opportunities

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

for undue discrimination. This uniform standard ensures that wind developers, when they seek to interconnect, are not faced with widely varying standards in different areas, or for different wind technologies, manufacturers, or plant owners. This should remove unnecessary obstacles to the increased growth of wind generation. Furthermore, ensuring that a large wind plant provides reactive support to the transmission grid if needed will ensure that safety and reliability is protected.

51. Specifically, the Commission revises the proposed power factor standard to require that the wind plant maintain the required power factor only on a case-by-case basis if the Transmission Provider, in the System Impact Study, shows that it is necessary to ensure safety or reliability. The reactive power standard adopted here properly requires the Transmission Provider to show that reactive power capability is needed for each wind plant Interconnection Customer. As we noted with regard to low voltage ride-through capability, because the Transmission Provider is responsible for the safe and reliable operation of its transmission system (pursuant to NERC and regional reliability council standards), it is in the best position to establish if reactive power is needed in individual circumstances. The System Impact Study is the appropriate study for assessing the need for reactive power capability, and this study should determine if there is a need for a wind plant to have reactive power capability to ensure that the safety or reliability of the system is maintained. Also, as we reasoned above with regard to low voltage ride-through, requiring wind plants to maintain the required power factor only if the System Impact Study shows it to be necessary ensures that the increased reliance on

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

wind plants does not degrade system safety or reliability. It also ensures that the Transmission Provider does not require a wind plant to install costly equipment that is not needed for grid safety or reliability. Furthermore, requiring that the System Impact Study find a need for reactive power will limit the opportunities for undue discrimination; a wind plant Interconnection Customer will not have its interconnection frustrated by unnecessary requirements that are not necessary to maintain safety or reliability. Should a wind plant Interconnection Customer disagree with the Transmission Provider that the System Impact Study shows that the power factor requirement is needed, it may challenge the Transmission Provider's conclusion through dispute resolution or appeal to the Commission.

52. Given our decision to require that a wind plant maintain the power factor standard only on a case-by-case basis where the Transmission Provider shows, through the System Impact Study, that reactive power is needed to ensure reliability, there is no need to retain the waiver provisions proposed in the NOPR. As a result, issues raised by commenters regarding the waiver provisions are moot.

53. We clarify that the wind generating plant, if required to provide reactive power capability as described above, should be able to operate anywhere in the +/- 0.95 power factor range.

54. We reject proposals to change the power factor range standard in Appendix G to 0.90 lagging to 0.95 leading. Adopting such a standard would make the power factor requirement more onerous for wind plants than for conventional generators. Concerning

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

NYISO's request that the Commission consider the standard as a minimum requirement as opposed to a maximum, as we declined to do so in Order No. 2003, we decline to do so here for the same reasons.

55. In response to those who assert that adherence to the voltage schedule is more important than merely maintaining a power factor within the specified range, we note that article 9.6.2 of the LGIA already requires that the "Interconnection Customer . . . . operate the Large Generating Facility to maintain the specified output voltage or power factor at the Point of Interconnection." This language applies to wind plants and addresses this concern.

56. We disagree with PacifiCorp/PPM Energy that the parenthetical statement in the NOPR, "taking into account any limitations due to voltage level, real power output …," is ambiguous and unnecessary. AWEA explains that the stated power factor range cannot be accomplished by all equipment vendors at all levels of output, and asks that the wind plant be held to the +/- 0.95 power factor range only when it is generating above 10 percent of its rated output. The parenthetical statement is necessary due to the technical differences of wind plants, which cannot meet the power factor standard below certain levels of output, and addresses the concern raised by the wind industry.

57. We disagree with the CPUC's recommendation of a "least cost, best fit" approach. Such a "standard" is not a standard at all. Adopting such a least cost approach would result in widely varying "standards" for wind turbines and related equipment. This would not only open the door further for the undue discrimination that this rule is designed to

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

eliminate, but also would lead to high cost individualized generator designs by equipment manufacturers that would not serve the long-term needs of the wind industry.

3. Comments - Point of Interconnection

58. In the NOPR, the Commission proposed to measure the required power factor at the high side of the wind plant substation transformers, as opposed to the Point of Interconnection measurement point used in Order No. 2003. Numerous commenters, including NUSCo, Southern, National Grid, PacifiCorp/PPM Energy, and Southern California Edison request that the power factor be measured at the Point of Interconnection, as opposed to at the high voltage side of the wind plant substation transformer. FPL Energy notes that while meeting the power factor requirement at the Point of Interconnection may be more costly for wind plants that have long generation tie lines, reliability requirements will not be met by measuring the power factor at a different point. AWEA states that the appropriate point of measurement is either at the Point of Interconnection or at the high side of the wind plant's transformer, depending upon the particular electrical circumstances. It adds that the point of measurement should be determined based on the Transmission Provider's System Impact Study.

4. Commission Conclusion - Point of Interconnection

59. We adopt the Point of Interconnection as the appropriate measurement point for the power factor standard. We agree that adopting the Point of Interconnection as the measurement point will better protect system reliability because it is closer to the bulk electrical power system, and will be consistent with Order No. 2003. In addition,

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

numerous Transmission Providers and wind energy developers including PPM Energy and FPL Energy endorse establishing the point of measurement at the Point of Interconnection, instead of the high side of the substation transformers, as proposed in the NOPR. Moreover, FPL Energy supports this measurement point, even though it may be more costly for plants with long generation tie lines, because it is necessary for system safety and reliability.

5. Comments - Dynamic Reactive Power Capability

60. The Commission proposed in the NOPR to require wind plants to be able to provide sufficient dynamic voltage support if the System Impact Study shows that it is needed to maintain system reliability. Several commenters assert that wind generators should have dynamic reactive capability for the entire power factor range, and that dynamic reactive capability must be required in every instance. Midwest ISO TOs assert that the System Impact Study may show that no such capability is needed at the time of the study, but the need may arise later. They contend that at a minimum, a wind plant should not degrade the transient under-voltage performance of the transmission system at the Point of Interconnection.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

61. Midwest ISO points to language from NERC standards[29] and argues that the need for dynamic reactive power capability cannot be determined by the System Impact Study because it is almost impossible to conceive of every possible disturbance scenario ahead of time. AEP argues that dynamic reactive capability must be required and that the specific level of dynamic capability should be determined on a need basis. ISO New England states that the wind plant's rate of response for dynamic voltage control should be comparable to that provided by a conventional synchronous generator using an automatic voltage regulator.

62. FirstEnergy and FPL Energy ask the Commission to clarify what it meant by the term "sufficient dynamic voltage support." It claims that the term "sufficient" is vague and requires clarification. Similarly, FPL Energy contends that the term "sufficient" is ambiguous, and should be clarified or removed from the Final Rule.

63. Further, FPL Energy notes that only one wind turbine manufacturer currently holds the patent for the variable speed wind turbine electronics that allow the turbine to produce dynamic reactive power. According to FPL Energy, the Commission, as a

[29] Specifically, Midwest ISO cites the following language: "Dynamic reactive power support and voltage control are essential during power system disturbances. Synchronous generators, synchronous condensers, and static var compensators (SVCs and STATCOMs) can provide dynamic support." See Comments of Midwest ISO at 5-6, citing NERC Planning Standard I. D., System Adequacy and Security – Voltage Support and Reactive Power, approved by the NERC Board of Trustees on September 16, 1997.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

matter of public policy, should consider whether it is appropriate to set a power factor standard that will give one turbine manufacturer a significant competitive advantage.

64. American Superconductor argues that based on its experience of integrating wind generating plants into transmission systems, it is not always necessary to install dynamic capability for all of the reactive compensation required at a wind generating plant. It reports that all eight of the reactive compensation systems it has provided to wind generating plants used a combination of dynamic and static reactive capability. These hybrid systems consist of a small STATCOM device (with full dynamic capability)[30] that controls a number of switched shunt capacitors or reactors. They have proven to be very sound technically, as well as good economic choices, according to American Superconductor. It asks the Commission to recognize that the benefits of dynamic reactive capability can be achieved, often at substantially lower cost, by such systems.

65. NorthWestern Energy argues that dynamic reactive capability should not be required if the wind developer demonstrates that the wind generating plant will not cause voltage fluctuations greater than the "Border Line of Irritation," as identified in Section 10.5.1 of the IEEE's Standard 519, measured at the Point of Interconnection. The wind developer should also demonstrate that its addition will not diminish the rating of an

[30] A Static Compensator (STATCOM) provides voltage support to the electric system in a manner similar to a synchronous condenser and therefore is superior to Static VAR compensators or switched capacitor banks. Hybrid systems consist of a small STATCOM device and a number of switched capacitors or reactors.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

existing transmission line by reducing reactive voltage support, according to NorthWestern Energy. It agrees that wind generators should be allowed to use a combination of fixed and/or switched capacitors and reactors in combination with dynamic capability to control the voltage. It states that dynamic capability would allow for the smooth switching of these devices, as well as the energizing and de-energizing of the wind turbines, without affecting the quality of power delivered to customers.

6. Commission Conclusion – Dynamic Reactive Power Capability

66. The Commission adopts the language in the NOPR regarding dynamic reactive power capability. The Final Rule Appendix G, as explained above, requires that a wind plant have reactive power capability if the Transmission Provider shows, in the System Impact Study, that it is needed for safety or reliability. The Final Rule does not require that the reactive power capability installed by the wind plant be dynamic unless the System Impact Study also shows that this type of capability is needed for system reliability. We are not convinced that dynamic reactive capability is needed in every case, and we permit the Transmission Provider to make that determination on a case-by-case basis through the System Impact Study. We believe that the Transmission Provider is best situated to determine in the first instance whether dynamic reactive capability is needed, and what level of dynamic capability is necessary. We emphasize, however, that Transmission Providers must assess the need for dynamic reactive power capability on a comparable and not unduly discriminatory basis.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

67. We reject requests that the Final Rule require that the reactive capability possessed by the wind plant be dynamic in every case. We conclude that the Transmission Provider's System Impact Study should show that dynamic reactive capability is needed in a particular case. If the wind plant Interconnection Customer disagrees with the Transmission Provider that the System Impact Study shows that dynamic reactive power capability is needed, it may challenge the Transmission Provider's conclusion through dispute resolution or appeal to the Commission. We disagree with Midwest ISO TOs that a System Impact Study can account only for the need of the dynamic reactive capability on the day of the study; the study should be able to make reasonable assumptions about future days.

68. We disagree with FirstEnergy and FPL Energy that the term "sufficient" requires clarification. The Final Rule allows the Transmission Provider to determine the sufficient level of dynamic reactive capability on a case-by-case basis through the System Impact Study. As noted above, if the wind plant Interconnection Customer disagrees with the Transmission Provider's determination, it may challenge the Transmission Provider's conclusion through dispute resolution or appeal to the Commission.

69. We acknowledge that dynamic reactive capability can be achieved, often at substantially lower cost, by systems with a combination of true dynamic capability plus switched shunt capacitors and reactors. The Final Rule Appendix G gives wind plants the flexibility to use a variety of combinations to provide the reactive capability necessary.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

70. In response to FPL Energy's concern regarding wind turbine supply competition, we note that the wind turbine industry is highly competitive and that manufacturers are continually improving their designs. Although one manufacturer may have a competitive advantage right now, other manufacturers have indicated that they can rapidly improve their designs as required. Also, no manufacturer took exception to the Commission's proposed requirements. Furthermore, as described in detail below, there will be a transition period before the Appendix G standards will apply.

C. Supervisory Control and Data Acquisition Capability

71. We noted in the NOPR that in the past, Transmission Providers generally did not require wind generators to have remote supervisory control and data acquisition (SCADA) capability because of their small size and minimal effects on the transmission system. Many Transmission Providers now argue that with the increasing number of large wind plants connecting to transmission systems, SCADA capability is needed to acquire wind facility operating data and ensure the safety and reliability of the transmission system during normal, system emergency, and system contingency conditions.

72. The NOPR proposed to require that a large wind plant seeking to interconnect to the transmission grid possess SCADA capability to transmit data and receive instructions from the Transmission Provider. Additionally, Appendix G would have required that the Transmission Provider and the wind plant owner determine the type of SCADA information and equipment that is essential for the proposed wind plant, taking into

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

account the size of the plant, its characteristics, its location, and its importance in maintaining generation resource adequacy and transmission system reliability.[31]

73. The NOPR sought comments regarding the proposed SCADA capability requirements, specifically on whether there is any essential SCADA information that large wind plants should be required to provide, such as information needed to determine how the plant's maximum megawatt output and megawatt ramp rate vary over time with changes in the wind speed or information needed to forecast the megawatt output of the plant.

1. Comments

74. Great River, Midwest ISO, First Energy and Southern California Edison support the SCADA requirement in the NOPR. Ohio Consumer's Council, while also supportive, suggests that the Commission clarify the SCADA requirement so that future disputes regarding interpretation of it are minimized.

75. Numerous other commenters support the requirement with certain modifications. For example, EEI states that the requirement should require the parties to adhere to good utility practice, as that term is refined over time. It also asserts that the Commission

[31] Unlike synchronous generating plants, which generally have SCADA capability, can respond to automatic generation control signals from the control center and are often staffed, wind generating plants consist of numerous induction generators connected through a medium-voltage collector system, and are often remote, unmanned, and characterized by an unpredictable rate of change of output, thus making it difficult for the Transmission Provider to limit the output of the wind plant when necessary for system reliability.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

should recognize that NERC and other regional reliability councils are the appropriate entities to determine how to support real-time operations associated with data acquisition and data exchange. Western and Gamesa, among others, believe that SCADA capability, at a minimum, should include real-time and hourly real power output and reactive power output information and interconnection facility status information. Gamesa and NorthWestern Energy also argue that third parties who have experience with wind energy forecasting, not the Transmission Provider or the control area operator, should develop wind forecasting models and paradigms. NorthWestern Energy further asserts that the wind plant should be manned at all times. Similarly, Xcel supports a requirement that wind plants provide a leased voice line from the Transmission Control Center to a manned wind plant control center for voltage support.

76. Xcel, New York PSC, AEP, NERC and LIPA, among others, support a SCADA requirement, but generally contend that the type of SCADA capability required should be determined between the individual Transmission Provider and the wind plant, based on local system requirements. LIPA, New York PSC and Southern assert that the right to determine what SCADA capability is required should not be delegated in whole or part to the wind plant developer. Southern is also concerned that limiting SCADA information requirements to only what is “essential” for the wind plant may be interpreted to jeopardize reliability. It suggests eliminating the term “essential” and replacing it with “required” to ensure that reliability is not jeopardized.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

77. NRECA-APPA generally support the Commission's proposed SCADA requirement, but they question the Commission's statement in footnote 13 of the NOPR that it is difficult for the Transmission Provider to limit the output of a wind plant when necessary for reliability. They state that according to General Electric, wind farms in Europe are installing communications and control equipment (including turbine blades that can be adjusted to reduce the output of the wind generator at various wind speeds) to allow this to be done. They note that while not all wind plants need this capability, it may be needed at some plants, depending on the size of the plant or the number of wind plants on a transmission system, or other system characteristics.

78. AWEA and FPL Energy both express concern that the requirement in the NOPR that wind plants have the capability to "receive instructions" through SCADA could be interpreted to require control of the wind plant by the Transmission Provider, for example, to curtail the wind plant remotely at any time. FPL Energy asks the Commission to revise the requirement that the wind plant be able to "receive instructions" through SCADA to apply only during Emergency Conditions, as defined in the LGIA. AWEA asks that the Commission clarify that the proposed SCADA requirement does not establish a presumption that output controls are part of the standard, and that it state clearly that the terms and conditions for use of SCADA capability is a separate transmission service issue, not an interconnection issue, and must be resolved by contract or Commission-approved transmission tariff. Conversely, BPA asserts that direct SCADA control by the Transmission Provider is preferable and that the final

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

SCADA requirement should permit a Transmission Provider to exercise supervisory control over a wind plant.

79. Southern, Nevada Power and American Transmission maintain that the SCADA requirement for wind generators should be the same as that for synchronous generators.

2. Commission Conclusion

80. We adopt the SCADA requirement proposed in the NOPR. In response to AWEA and FPL Energy, however, we clarify that Appendix G requires the wind plant to have only the capability to receive instructions. Nothing in this Final Rule authorizes a Transmission Provider to control a wind plant. Any such authorization would be subject to separate negotiation and agreement between the Interconnection Customer and the Transmission Provider.

81. Under the SCADA requirement adopted here, the wind Interconnection Customer will provide SCADA capability, with the specific SCADA information and control capability required to be agreed to by the wind plant Interconnection Customer and the Transmission Provider. This flexible requirement ensures that wind plants have SCADA capability, which we believe is necessary to ensure that system reliability is protected, and permits the wind plant Interconnection Customer and the Transmission Provider to negotiate the specific SCADA capability that meets the needs of the transmission system at the specific location of the wind plant. We expect Transmission Providers to be reasonable in these negotiations and not to use their control over the Transmission System to unnecessarily burden wind plants. Should the wind plant Interconnection

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Customer disagree with the Transmission Provider about the level of SCADA capability required, it may challenge the Transmission Provider's conclusion through dispute resolution or appeal to the Commission.

82. In response to EEI's request, the SCADA requirement does not need to be revised explicitly to require adherence to good utility practice. We note that Appendix G is a component of the LGIA, and the LGIA itself already requires the parties to adhere to good utility practice.

83. With respect to comments concerning the type of SCADA information needed for wind plants, the SCADA requirement in the NOPR allows the Parties to decide what information should be provided and the equipment to be installed at the site. We adopt this policy in this Final Rule. We are not deciding such issues as whether third parties should be used to develop wind forecasting models and paradigms. We simply require that some SCADA capability be installed for operation and reliability purposes. The flexible nature of the requirement we adopt here recognizes, as NERC states, that other entities are more appropriate to determine how best to support real-time operation with data acquisition and exchange. We agree with AWEA and others that this Final Rule only requires that SCADA capability be provided by the wind plant, and that the type of SCADA information supplied and control exercised can be negotiated and set forth in a separate agreement between the wind plant Interconnection Customer and the Transmission Provider.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

84. Similarly, we deny requests that the Transmission Provider have the sole authority to determine the type of SCADA equipment to be installed at the wind plant. To ensure that unnecessary SCADA equipment is not required of the wind plant, the parties must determine together the SCADA capability and equipment needed, taking into account the size, location and characteristics of the wind plant and the safety and reliability of the transmission system. Southern has not shown that replacing the term "essential" with "required" would add any clarity to the requirement.

85. We are not convinced by arguments that the SCADA requirements for wind plants should be the same as for conventional generators. Since wind is different from conventional generators (as discussed above), information exchanged between the Transmission Provider and the wind plant may be of a different nature. As a result, it is appropriate to have different, more flexible SCADA requirements for wind plants.

D. Wind Plant Interconnection Modeling

86. In its May 20, 2004 petition, AWEA proposed that Transmission Providers be required to "participate in a formal process for updating, improving, and validating the engineering models used for modeling the interconnection impacts of wind turbines."[32] The Commission did not propose such a requirement in the NOPR, because such a process should take place outside the Commission, through industry technical groups or the regional reliability councils. The Commission recognized, however, that

[32] See Petition of AWEA at 5.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

improvements in the way that wind interconnections are modeled would be beneficial, and encouraged the industry to address this issue.

1. Comments

87. Those submitting comments regarding wind plant interconnection modeling generally support the Commission's conclusion that the issue is best addressed through industry technical groups, NERC, and regional reliability councils.

2. Commission Conclusion

88. As we stated in the NOPR, we recommend that wind developers, wind turbine manufacturers, Transmission Providers and affected parties form technical groups and participate in a formal process to address, update, improve and validate wind turbine engineering models. We remain convinced, however, that the Commission is not the appropriate forum for such a process.

E. Self-Study of Interconnection Feasibility

89. In the NOPR, the Commission rejected a proposal by AWEA that would permit a wind plant Interconnection Customer to enter the interconnection queue and receive the base case data to "self-study" the feasibility of its proposed interconnection without having first submitted an Interconnection Request that includes power and load flow data and fully completed plant electric design specifications, as required under Order No. 2003.[33] The Commission noted that Order No. 2003 requires that a valid and complete

[33] See id. at 13-14.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Interconnection Request be on file with the Transmission Provider before the Interconnection Customer may receive Base Case data.[34] We further noted, however, that Section 2.3 of the LGIP did not address situations where the Interconnection Customer might need access to the Base Case data before it could complete its Interconnection Request. The Commission therefore sought comments on how to balance the need of wind generators to receive the base case data and "self-study" before filing a completed Interconnection Request with the need to protect this critical energy infrastructure information and commercially sensitive data against unwarranted disclosure.

1. Comments

90. Several entities, including Tucson Electric, Midwest Reliability Organization, Montana-Dakota Utilities, New York PSC, Nevada Power, Great River, LIPA, BPA, American Transmission, NUSCo, Xcel, and Midwest ISO TOs oppose AWEA's proposal to allow wind generators to be placed in the queue, receive the base case data and "self-study" before filing completed electric design specifications and other related technical data. They generally argue that wind plants should be treated no differently from other generating plants. Montana-Dakota Utilities suggests that wind plant developers use generic power flow network models before filing Interconnection Requests, since these models would not likely reveal commercially sensitive data or critical energy

[34] See NOPR at P 22, citing LGIP, section 2.3; see also Order No. 2003 at P 77-84.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

infrastructure information. BPA does state, however, that while it supports the Commission's decision not to alter the LGIA timelines, the requirement that wind plants provide detailed project specifications could be relaxed at the Feasibility Study stage, and that it is willing to work with wind developers to ensure that they have the information necessary to develop their Interconnection Requests. It asserts that the Commission should allow Transmission Providers the flexibility to determine when wind developers should submit turbine specifications and detailed electrical design data. LIPA argues that all generators should have comparable access to base case data, subject to their willingness to sign a confidentiality agreement, and that discussion of how to accommodate alternative plant designs (such as wind plants) in the interconnection process should be left to the Transmission Provider and the generator.

91. NRECA-APPA state that while they are willing to accept AWEA's proposal, they do not object to the NOPR proposal. Numerous other commenters, including Western, PacifiCorp/PPM Energy, FPL Energy, and the Ohio Consumer's Council indicate that they generally support the AWEA "self-study" proposal, or offer suggestions to balance the need of wind plants to obtain base case data with the need to protect such data from unwarranted release. Western has no objection to allowing wind generators to self-study if the Transmission Provider is given final approval before the Interconnection Request is completed. It asserts that wind plants should request base case data directly from the regional reliability council, execute a confidentiality agreement and pay a fee. PJM similarly contends that allowing wind plants to obtain base case data from the regional

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

reliability councils will allow sufficient self-study by the developer while also limiting the need for multiple restudies by the Transmission Provider. Western contends that self-study and base case information should be available to all prospective Interconnection Customers.

92. Ohio Consumer's Council asks that the Commission seriously consider AWEA's proposal that wind projects not be required to provide some detailed design data as a condition of obtaining a place in the interconnection queue. It states that large wind projects are based on complex and variable site work compared to the more traditional generating plants that are studied for selected locations based on transportation needs and access to water for cooling purposes. It stresses that the Commission's requirements regarding the submission of design data for entry in the interconnection queue should reflect these differences in technologies.

93. AWEA and PacifiCorp/PPM Energy ask the Commission to reconsider its proposal not to adopt AWEA's self-study proposal. PacifiCorp/PPM Energy state that wind turbine performance varies significantly by manufacturer and that wind plant developers necessarily typically negotiate turbine selection and evaluate the configuration of the facility throughout the interconnection study period. AWEA similarly notes the complexities involved in laying out the medium voltage collector systems used by wind plants, and states the layout cannot be finalized until the Point of Interconnection is firmly established. It states that consequently, the detailed design and data for the collector system, which many Transmission Providers assert is required by the

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Interconnection Request, cannot be available when the Interconnection Request is submitted. AWEA suggests that, rather than requiring that the generating plant design be "substantially completed" at the time the Interconnection Request is submitted, the Commission should allow a wind plant to file an Interconnection Request with the generating plant design data and other related data depicting the wind plant as "a single generating unit connected through step-up transformation, with the equivalent power output characteristics (MW output and MVAR range) as the total net MW output of the wind generating facility in question."[35] Under this proposal, the wind plant developer would be required to provide a "substantially completed" generating plant design before the System Impact Study, along with either the power system load flow data sheets or the newly developed machine models with substantially complete input data to those models. AWEA states that many, but not all, Transmission Providers now accept such data as satisfying the requirements of the Interconnection Request.

2. Commission Conclusion

94. In this Final Rule, we allow a wind plant Interconnection Customer to satisfy the requirements of the Interconnection Request by providing a set of preliminary electric design specifications depicting the wind plant as a single equivalent generator, as explained below. Once completing the Interconnection Request in this manner, the wind plant may enter the queue and receive the base case data as provided for in Order No.

[35] Comments of AWEA at 10-11.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

2003. The Commission directs that these provisions be attached as Appendix G to the LGIP in the OATTs of all public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce.[36]

95. In the NOPR, we noted that Section 2.3 of the LGIP did not address situations in which the Interconnection Customer needs the Base Case data before it can complete its Interconnection Request. We sought comments on how to balance the need of wind generators to have this information before filing a completed Interconnection Request with the need to protect this critical energy infrastructure information and commercially sensitive data against unwarranted disclosure. In addition, we sought to ensure that one class of customers was not being given undue preferential treatment.

96. We note that many Transmission Providers, non-wind generators, and a state regulatory commission oppose allowing wind generators to file Interconnection Requests, and hence be given a place in the queue, before submitting their final plant designs and related technical data. However, some trade organizations, wind developers, and Transmission Providers with substantial experience interconnecting wind plants, including AWEA, FPL Energy, PacifiCorp/PPM Energy, Western and Ohio Consumer's

[36] The Commission requires that these procedural provisions be separately appended as Appendix G to the LGIP, because they are procedural in nature, and to ensure that they are in force during the initial stages of the interconnection process. We are retaining the Appendix G moniker to ensure that these procedural provisions are recognized as applicable only to the interconnection of large wind plants, the subject of this Final Rule. The remaining technical requirements adopted in this Final Rule must be appended as Appendix G to the LGIA.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Council, support the AWEA proposal or some accommodation of wind's special needs.

97. We are persuaded that wind projects are not the same as conventional generators with regard to Interconnection Requests. Large conventional generators are generally standard in design, and their design specifications and configurations do not necessarily change as a result of where they are located on the Transmission Provider's transmission system. Large wind plants, on the other hand, are located on sites made up of several acres of land. Their physical layout often consists of hundreds of wind turbines in the more remote areas of a Transmission Provider's system, and that layout can extend for several miles. The physical placement of the turbines, transformers and voltage support devices that affect the electrical characteristics created by the medium voltage collector system depend on the size and location of the wind plant and the location of other generators on the Transmission Provider's system. For these reasons, wind plant developers are unable to submit completed design specifications for individual wind turbines until much later in the interconnection process, in comparison with other developers.

98. However, a wind plant developer can provide at the time the Interconnection Request is submitted design specifications for the wind generating plant based on its aggregate output, though perhaps not for the individual wind turbines. As we stated in Order No. 2003-A and in the NOPR, the Appendix G we adopt in this rule is designed to account for these unique technical characteristics of wind plants. Recognizing these

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

unique characteristics is not favoring one form of generation over others; it simply removes barriers to wind plant development that are not necessary to protect safety or reliability.

99. In short, we are persuaded that the technical characteristics of wind plants prevent them from providing certain detailed design specifications and other information at the time of the Interconnection Request. Therefore, the Commission adopts provisions in the Final Rule Appendix G permitting the wind developer to satisfy the requirements of the Interconnection Request by providing a set of preliminary electrical design specifications depicting the wind plant as a single equivalent generator.[37] Upon satisfying these and other applicable Interconnection Request requirements in Order No. 2003, the wind plant may enter the queue and receive the base case data as provided for all large generators in Order No. 2003. However, no more than six months later, the wind plant must submit completed detailed design specifications and other data (including collector system layout data) needed to allow the Transmission Provider to complete its System Impact Study. This information must be provided before the System Impact Study can begin. This deadline provides a date certain regarding when the final design specifications must be submitted to the Transmission Provider to avoid having uncertain projects in the queue.

[37] "Single equivalent generator" information is design data that represents the aggregate electrical characteristics of the individual wind generators as a single generator.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

100. Permitting wind plants to provide single-generator-equivalent specifications at the Interconnection Request stage appropriately balances the need of a Transmission Provider to have adequate data in the Interconnection Request and the difficulty that a wind plant developer has in completing its detailed design before entering the queue and receiving access to the base case data. This provision also protects critical energy infrastructure information by making none of it available to anyone who has not made a satisfactory Interconnection Request. Wind plants will follow all other requirements of the queue and study processes set forth in Order No. 2003, including the timelines and confidentiality provisions.

F. Applicability to Other Generating Technologies

101. In the NOPR, the Commission sought comments as to whether there are other alternative technologies that should be covered by Appendix G.

1. Comments

102. Numerous entities state that other alternative technologies should be made subject to Appendix G.[38] Southern California Edison asserts that all non-synchronous generators should be subject to Appendix G. Tucson Electric submits that solar generators without fueled backup should be included in Appendix G. Other commenters, including Midwest Reliability Organization, National Grid, Xcel, the CPUC and Great River generally state

[38] These entities include PJM, BPA, ISO New England, NYISO, Southern California Edison, CenterPoint, the NARUC, LIPA, New York PSC, Nevada Power, NUSCo and Tucson Electric.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

that they do not necessarily support including other alternative technologies within the coverage of Appendix G. The CPUC, for example, does not believe that Appendix G should be expanded to apply to "renewable" technologies other than those that are intermittent or geographically constrained. National Grid states that these proceedings have focused exclusively on wind generation and thus does not support applying Appendix G more broadly. Xcel states that other non-synchronous technologies have not matured sufficiently to operate on a scale greater than 20 MW, and therefore should not be able to use Appendix G.

103. American Transmission asserts that the Commission should adopt the Alberta Electric System Operator definition of asynchronous generation, which is "a type of generator that produces alternating electric current that matches the frequency of an interconnected power system and the mechanical rotor of the generator does not rotate in synchronism with the system frequency." It argues that the Alberta Electric System Operator definition is superior because it is used in the electric power technical community to refer to the type of generator to which the NOPR is directed and because it compares the speed of an asynchronous generator to that of a traditional generator.

2. Commission Conclusion

104. The Commission concludes that the Final Rule Appendix G exceptions to the LGIP and LGIA apply only to large wind plants. As discussed above, the Appendix G was designed around the special needs and design characteristics of wind generators. The NOPR asked whether there were other generators that have similar characters and require

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

similar technical requirements to those contained in Appendix G. Although numerous commenters suggested that other generators may have special needs and suggested that they should be made subject to Appendix G, none other than Tucson (who suggested solar generators without fueled backup) offered a specific induction generator technology with similar characteristics to wind as an Appendix G candidate. The Appendix G provisions adopted here focuses on the special characteristics of large wind plants, particularly the fact that they utilize many induction generators connected to the transmission system at a single point through a medium-voltage collector system. The Commission has not found at this time that any other technologies, including the solar generators without fueled backup offered by Tucson, have similar characteristics.

105. The Commission does not adopt American Transmission's proposed definition of "asynchronous generation" in the Final Rule. The Commission is not relying on the concept of asynchronous generation in this Final Rule, and we do not believe that this characteristic appropriately identifies the interconnection needs of large wind plants addressed by the Final Rule Appendix G. Accordingly, we do not make any definitional changes.

106. While we are not applying the Final Rule Appendix G to non-wind technologies, we may do this in the future, or take other generic or case-specific actions, if another technology emerges for which a different set of interconnection requirements is necessary.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

G. Variations from the Final Rule

107. The NOPR proposed to permit Transmission Providers to justify variations from the Final Rule Appendix G using the same three variation standards in Order No. 2003. First, public utilities may seek variations from the Final Rule Appendix G based on regional reliability council requirements.[39] Second, we proposed that public utilities may argue that proposed variations are "consistent with or superior to" the Final Rule Appendix G.[40] Third, we proposed to permit independent public utility Transmission Providers, such as Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs), greater flexibility in adopting Appendix G(the "independent entity variation").[41]

1. Comments

108. Numerous entities request that they be permitted to justify variations from the Appendix G requirements. Several ask the Commission to clarify that the Appendix G performance standards are minimum requirements, as noted elsewhere.[42] Some commenters encourage the Commission to use NERC or regional reliability councils to

[39] See NOPR at P 25, citing Order No. 2003 at P 823-24.

[40] See NOPR at P 25, citing Order No. 2003 at P 816.

[41] See NOPR at P 25, citing Order No. 2003 at P 822-27 and Order No. 2003-A at P 48.

[42] These entities include Midwest ISO TOs, FirstEnergy, NYISO, LADWP, NorthWestern Energy, CPUC and Southern, among others.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

develop necessary technical standards and requirements applicable to wind generation and its effect on reliability, including the incorporation of NERC's American National Standards Institute-approved standards, field tests and other requirements.

2. Commission Conclusion

109. As we proposed in the NOPR, we apply here all three of the variation standards in Order No. 2003. If a Transmission Provider seeks to justify variations from Appendix G, it may do so in its compliance filing. A Transmission Provider may propose to include standards developed by NERC or a regional reliability council in its own Appendix G. The Commission is mindful of the work being done by these organizations in developing standards for the interconnection of wind plants, and we strongly encourage all interested parties, including Transmission Providers, wind plant developers and wind turbine manufacturers, to continue to participate in developing these standards. The Commission will consider them in any request for a variation from the Final Rule Appendix G by an individual Transmission Provider, or a request by many to revise Appendix G.

H. Transition Period

110. In the NOPR, the Commission did not propose a transition period before the technical requirements in Appendix G would take effect.

1. Comments

111. AWEA, FPL Energy, and PacifiCorp/PPM Energy ask that there be a transition period so Appendix G would apply only to LGIAs signed or unexecuted LGIAs filed with the Commission after January 1, 2006, or six months after the issuance of this Final

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Rule, whichever is later. FPL Energy asserts that a transition period is needed to prevent added costs and delays to protect previously executed wind equipment purchase agreements and power purchase arrangements. PacifiCorp/PPM Energy add that wind turbines are already in the process of being manufactured that would require substantial changes to their electronics to meet the proposed requirements. AWEA asserts that the Commission has historically provided a transition period in similar circumstances, including in Order No. 2003.

112. AWEA also asks that all wind plants that are interconnected to the transmission system when Appendix G is adopted, or that have executed an LGIA or filed an unexecuted LGIA with the Commission before January 1, 2006 or six months after the issuance of this Final Rule, whichever is later, be exempted from the Appendix G requirements for the remaining life of the existing wind generator equipment. Likewise, Ohio Consumer's Council, LIPA and Xcel support a transition period and state that existing wind projects or those in advanced planning should be exempt from the Appendix G requirements.

113. BPA and American Transmission are opposed to any transition period. American Transmission states that once Appendix G is adopted, no deviations should be permitted unless otherwise agreed to by the Transmission Provider. BPA states that installing outdated or inferior wind equipment that is incapable of complying with reliability criteria is contrary to the intent of this proceeding. American Transmission also maintains that existing interconnection agreements with wind plants must be amended to

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

conform to the requirements adopted in this proceeding. It argues that technical requirements for similar generating facilities should not be based merely on the timing of the interconnection.

2. Commission Conclusion

114. For the low voltage ride-through, SCADA, and power factor design criteria requirements adopted in the Final Rule Appendix G, which are substantive technical requirements, the Commission adopts the transition period requested by AWEA and others. Accordingly, these technical requirements in the Final Rule Appendix G, if applicable, apply only to LGIAs signed, filed with the Commission in unexecuted form, or filed as non-conforming agreements, on or after January 1, 2006, or the date six months after publication of the Final Rule in the Federal Register, whichever is later. The procedures permitting the wind plant Interconnection Customer to complete the Interconnection Request with single-generator equivalent design specifications apply immediately when the Final Rule becomes effective, 60 days after its publication in the Federal Register. This effective date also applies for purposes of public utilities making compliance filings to meet this Final Rule, as discussed further below.

115. It would be unfair and unreasonable to apply the low voltage ride-through, SCADA and power factor requirements in the Final Rule immediately or retroactively. The reasonable transition period we establish in this Final Rule allows wind equipment currently in the process of being manufactured to be completed without delay or added expense. This ensures that the Final Rule does not interrupt the supply of wind turbines.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

Further, we disagree with BPA that the transition period will undermine the reliability of a Transmission Provider's system. We note that during the transition period, our large generator interconnection rule applies to wind plants. Even though article 9.6.1 (Power Factor Design Criteria) of the LGIA does not apply to wind plants, the other provisions of that rule are adequate to prevent an interconnection that would undermine reliability of a Transmission Provider's system

116. Consistent with our action grandfathering existing interconnection agreements in Order No. 2003,[43] the Commission is not requiring modifications to existing interconnection agreements, and is not requiring that interconnection agreements signed, filed with the Commission in unexecuted form, or filed as a non-conforming agreement before January 1, 2006, or the date six months after publication of the Final Rule in the Federal Register, whichever is later, comply with the low voltage ride-through, SCADA and power factor requirements of the Final Rule Appendix G, if applicable.

I. Miscellaneous Comments

117. The Fertilizer Institute notes that wind generators and generators that use waste heat have several things in common; for example, both produce electricity without any fuel consumption or air emissions. It states that through no fault of their own, neither wind generators nor fertilizer-fired generators can meet the rigorous balancing and scheduling requirements imposed by Transmission Provider's. It urges the Commission

[43] See Order No. 2003 at P 911.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

to exempt both from any requirement to balance their power deliveries and power receipts during any time period shorter than the peak and non-peak periods of a given day.

118. Also, American Transmission contends that Transmission Owners who are part of an RTO/ISO should be allowed to pursue ADR before an LGIA is filed with the Commission on an unexecuted basis.

1. Commission Conclusion

119. In response to the comments of the Fertilizer Institute, we note that the Commission recently issued a NOPR in Docket No. RM05-10-000 to address generator imbalance penalties assessed to intermittent generating resources.[44] We will consider the Fertilizer Institute's comments in that proceeding.

120. Further, in response to American Transmission's request that ADR be permitted before an unexecuted LGIA is filed, we note that the LGIP already provides dispute resolution procedures that apply to wind plant interconnections.[45]

---

[44] Imbalance Provisions for Intermittent Resources Assessing the State of Wind Energy in Wholesale Electricity Markets, Notice of Proposed Rulemaking, 70 Fed. Reg. 21,349 (Apr. 26, 2005), 111 FERC ¶ 61,026 (2005).

[45] See LGIP § 13.5.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

J. Compliance Issues

121. As in Order No. 2003,[46] the Commission is requiring all public utilities that own, control, or operate transmission facilities in interstate commerce to adopt the Final Rule Appendix G as amendments (as discussed above) to the LGIP and LGIA in their OATTs 60 days after publication of the Final Rule in the Federal Register. Public utilities subject to this Final Rule are directed to adopt the low voltage ride-through, SCADA, and power factor design criteria requirements of the Final Rule Appendix G as amendments to their LGIAs, and to adopt the procedural provisions in the Final Rule Appendix G concerning completion of the Interconnection Request by the wind plant Interconnection Customer as amendments to their LGIPs. Further, consistent with our approach in Order No. 2003 and as discussed above,[47] we are not requiring retroactive changes to wind plant interconnection agreements that are already in effect. Also, as noted above, the low voltage ride-through, SCADA and power factor requirements adopted in the Final Rule Appendix G, if applicable, do not apply to LGIAs signed, filed with the Commission in unexecuted form, or filed as a non-conforming agreement, on or before January 1, 2006 or six months after the publication of this Final Rule in the Federal Register, whichever is later. As we state above, however, the procedures adopted in the Final Rule Appendix G

[46] See Order No. 2003 at P 910.

[47] Id. at P 911.

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

regarding completion of the Interconnection Request by a wind plant Interconnection Customer apply beginning on the effective date of this Final Rule.

IV. Information Collection Statement

122. Office of Management and Budget (OMB) regulations require OMB to approve certain information collection requirements imposed by agency rule.[48] The Commission solicited comments on the Commission's need for this information, whether the information would have practical use, the accuracy of provided burden estimates, ways to enhance the quality, utility and clarity of the information to be collected, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques. With the exception of BPA, which supported the objectives of the Paperwork Reduction Act, the Commission did not receive any comments concerning its burden or cost estimates. Therefore, the Commission retains the estimates proposed in the NOPR.

123. Public Reporting Burden:

Data Collection	No. of Respondents	No. of Responses	Hours Per Response	Total Annual Hours
FERC-516	238	1	18	4,284

Title: FERC-516, Electric Rate Schedule Filings

Action: Proposed Information Collection.

[48] 5 CFR § 1320.11 (2004).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

OMB Control No.: 1902-0096

The applicant shall not be penalized for failure to respond to this collection of information unless the collection of information displays a valid OMB control number.

Respondents: Business or other for profit.

Frequency of Responses: On occasion.

Necessity of Information: The regulations revise the requirements contained in 18 CFR Part 35. The Commission is revising its standardized interconnection procedures and agreements to adopt standard technical requirements and procedures specifically applicable to wind generating plants. In particular, the Commission requires that public utilities add to their standard interconnection procedures and agreements standard technical requirements and procedures for the interconnection of wind generation plants. The Final Rule requires that each public utility that owns, operates, or controls transmission facilities make filings incorporating these technical requirements into its open access transmission tariff.

Internal Review: The Commission has assured itself, by means of internal review, that there is specific, objective support for the burden estimates associated with the information collection requirements. The Commission's Office of Market, Tariffs and Rates uses the data included in filings under section 203 and 205 of the Federal Power to evaluate efforts for interconnection and coordination of the U.S. electric transmission system as well as for general industry oversight. These information requirements conform to the Commission's plan for efficient information collection, communication,

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

and management within the electric power industry. Interested persons may obtain information on the reporting requirements by contacting the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, D.C. 20426, Attention: Michael Miller, Office of the Executive Director, phone: (202) 502-8415, fax: (202) 273-0873, e-mail: michael.miller@ferc.gov. Comments on the requirements of the subject rule may also be sent to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503, Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4650.

V. Environmental Analysis

124. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect on the human environment.[49] As we stated in the NOPR, the Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in this categorical exclusion are rules that are clarifying, corrective, or procedural, or that do not substantially change the effect of the regulations being amended.[50] The categorical exclusion also includes information

[49] Order No. 486, Regulations Implementing the National Environmental Policy Act, 52 Fed. Reg. 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (Dec. 10, 1987).

[50] 18 CFR § 380.4(a)(2)(ii) (2004).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

gathering, analysis, and dissemination.[51] This Final Rule updates and clarifies the application of the Commission's standard interconnection requirements to wind generating plants. Further, this Final Rule involves information gathering, analysis, and dissemination regarding the interconnection of wind generators. Therefore, the rule falls within the categorical exemptions provided in the Commission's Regulations, and as a result neither an environmental impact statement nor an environmental assessment is required. Additionally, we note that this rule removes unnecessary obstacles to the development and interconnection of wind plants, eliminating the airborne and other emissions that would otherwise result from the construction of fossil fuel generating plants.

VI. Regulatory Flexibility Act Certification

125. The Regulatory Flexibility Act of 1980 (RFA)[52] generally requires a description and analysis of final rules that have significant economic impact on a substantial number

[51] 18 CFR § 380.4(a)(5) (2004).

[52] 5 U.S.C. § 601-612 (2000).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

of small entities.[53] The Commission is not required to make such analyses if a rule would not have such an effect.

126. The Commission does not believe that this Final Rule will have such an impact on small entities. Most filing companies subject to the Commission's jurisdiction do not fall within the RFA's definition of a small entity. Further, the filing requirements contain standard generator interconnection procedures and agreement for interconnecting wind plants larger than 20 MW, which exceeds the threshold of the Small Business Size Standard of NAICS. Therefore, the Commission certifies that this rule will not have a significant economic impact on a substantial number of small entities.

VII. Document Availability

127. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through FERC's Home Page (http://www.ferc.gov) and in FERC's Public Reference Room during normal business

[53] The RFA definition of "small entity" refers to the definition provided in the Small Business Act, which defines a "small business concern" as a business that is independently owned and operated and that is not dominant in its field of operation. 15 U.S.C. § 632 (2000). The Small Business Size Standards component of the North American Industry Classification System defines a small electric utility as one that, including its affiliates, is primarily engaged in the generation, transmission, and/or distribution of electric energy for sale and whose total electric output for the preceding fiscal years did not exceed 4 million MWh. 13 CFR § 121.201 (Section 22, Utilities, North American Industry Classification System, NAICS) (2004)).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, N.E., Room 2A, Washington, D.C. 20426.

128. From the Commission's Home Page on the Internet, this information is available in the Commission's document management system, eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

129. User assistance is available for eLibrary and the FERC's website during normal business hours. For assistance, please contact FERC Online Support at 1-866-208-3676 (toll free) or 202-502-6652 (e-mail at FERCOnlineSupport@FERC.gov), or the Public Reference Room at 202-502-8371, TTY 202-502-8659 (e-mail at public.referenceroom@ferc.gov).

VIII. Effective Date and Congressional Notification

130. This Final Rule will take effect [insert date that is 60 days after date of publication in the **FEDERAL REGISTER].** However, as noted above (under "Transition Period"), the technical requirements in the Final Rule LGIA Appendix G will apply only to LGIAs signed, or agreements filed with the Commission in unexecuted form, on or after January 1, 2006, or the date six months from the date of publication of this Final Rule in the Federal Register, whichever is later. The Commission has determined with the concurrence of the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, that this rule is not a major rule within the meaning

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

of section 251 of the Small Business Regulatory Enforcement Fairness Act of 1996.[54] The Commission will submit the Final Rule to both houses of Congress and the General Accountability Office.[55]

List of Subjects in 18 C.F.R. Part 35

Electric power rates; Electric utilities.

By the Commission.

Linda Mitry,
Deputy Secretary.

[54] See 5 U.S.C. 804(2) (2000).

[55] See 5 U.S.C. 801(a) (1) (A) (2000).

In consideration of the foregoing, the Commission revises part 35, Chapter I, Title 18 of the Code of Federal Regulations, as follows.

PART 35 – FILING OF RATE SCHEDULES

1. The authority citation for part 35 continues to read as follows:

Authority: 16 U.S.C. §§ 791a-825r, §§ 2601-2645; 31 U.S.C. § 9701; 42 U.S.C. §§ 7101-7352.

2. In § 35.28, the first sentences of currently existing paragraphs (f)(1) and (f)(1)(iii) are revised, a new paragraph (f)(1)(iii) is added, and currently existing paragraph (f)(1)(iii) is renumbered to account for new paragraph (f)(1)(iii) all to read as follows:

§ 35.28 Non-discriminatory open access transmission tariff.

* * * * *

(f) Standard generator interconnection procedures and agreements.

(1) Every public utility that is required to have on file a non-discriminatory open access transmission tariff under this section must amend such tariff by adding the standard interconnection procedures and agreement contained in Order No. 2003, FERC Stats. & Regs. ¶ 31,146 (Final Rule on Generator Interconnection), as amended by the Commission in Order No. 661, FERC Stats. & Regs. ¶ _____ (Final Rule on Interconnection for Wind Energy), and the standard small generator interconnection procedures and agreement contained in Order No. 2006, FERC Stats. & Regs. ¶ _____

(Final Rule on Small Generator Interconnection), or such other interconnection procedures and agreements as may be approved by the Commission consistent with Order No. 2003, FERC Stats. & Regs. ¶ 31,146 (Final Rule on Generator Interconnection) and Order No. 2006, FERC Stats. & Regs. ¶ _____ (Final Rule on Small Generator Interconnection).

(i) The amendment to implement the Final Rule on Generator Interconnection required by the preceding subsection must be filed no later than January 20, 2004.

(ii) The amendment to implement the Final Rule on Small Generator Interconnection required by the preceding subsection must be filed no later than [insert date 60 days after publication in the FEDERAL REGISTER].

(iii) The amendment to implement the Final Rule on Interconnection for Wind Energy required by the preceding subsection must be filed no later than [insert date 60 days after publication in the FEDERAL Register].

(iv) Any public utility that seeks a deviation from the standard interconnection procedures and agreement contained in Order No. 2003, FERC Stats. & Regs. ¶ 31,146 (Final Rule on Generator Interconnection), as amended by the Commission in Order No. 661, FERC Stats. & Regs. ¶ _____ (Final Rule on Interconnection for Wind Energy), or the standard small generator interconnection procedures and agreement contained in Order No. 2006, FERC Stats. & Regs. ¶ _____ (Final Rule on Small Generator

Interconnection), must demonstrate that the deviation is consistent with the principles of either Order No. 2003, FERC Stats. & Regs. ¶ 31,146 (Final Rule on Generator Interconnection) or Order No. 2006, FERC Stats. & Regs. ¶ _____ (Final Rule on Small Generator Interconnection).

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

[NOTE: THE ATTACHMENTS WILL NOT BE PUBLISHED IN THE CODE OF FEDERAL REGULATIONS]

20050602-3073 Issued by FERC OSEC 06/02/2005 in Docket#: RM05-4-000

APPENDIX A

List of Commenter Acronyms
RM05-4-000

AEP - American Electric Power System
American Superconductor - American Superconductor Corporation
American Transmission - American Transmission Company, LLC
AWEA - American Wind Energy Association
BPA - Bonneville Power Administration
CenterPoint – CenterPoint Energy Houston Electric, LLC
CPUC - California Public Utilities Commission
EEI - Edison Electric Institute
Exelon - Exelon Corporation
FirstEnergy – FirstEnergy Companies
Fertilizer Institute – The Fertilizer Institute
FPL Energy – FPL Energy, LLC
Gamesa – Gamesa Energy USA, Inc
GE – General Electric
Great River - Great River Energy
Innovation – Innovation Investments, LLC
ISO New England – ISO New England Inc
LADWP - Los Angeles Department of Water and Power
LIPA - Long Island Power Authority and LIPA
Midwest ISO - Midwest Independent Transmission System Operator, Inc.
Midwest ISO TOs - Midwest ISO Transmission Owners
Midwest Reliability Organization – Midwest Reliability Organization
Montana-Dakota Utilities – Montana-Dakota Utilities
NARUC - National Association of Regulatory Utility Commissioners
National Grid– National Grid USA
NERC - North America Electric Reliability Council
Nevada Power - Nevada Power Company/Sierra Pacific Power Company
New York PSC - New York State Public Service Commission
NRECA/APPA - National Rural Electric Cooperative Association and the American Public Power Association
NYISO - New York Independent Transmission System Operator, Inc.
NUSCo - Northeast Utilities Service Company
NorthWestern Energy – NorthWestern Energy
Ohio Consumers' Council- The Office of the Ohio Consumers' Council
PacifiCorp/PPM Energy – PacifiCorp and PPM Energy, Inc
PJM - PJM Interconnection, LLC
SoCal Edison - Southern California Edison Company
Southern – Southern Company Services, Inc.

Tucson Electric - Tucson Electric Power
Western - Western Area Power Administration
Xcel - Xcel Energy Services, Inc.
Zilkha - Zilkha Renewable Energy, LLC

Appendix B

[NOTE: THESE PROVISIONS TO BE ADOPTED AS APPENDIX G TO THE LGIA]

APPENDIX G

INTERCONNECTION REQUIREMENTS FOR A WIND GENERATING PLANT

Appendix G sets forth requirements and provisions specific to a wind generating plant. All other requirements of this LGIA continue to apply to wind generating plant interconnections.

A. Technical Standards Applicable to a Wind Generating Plant

i. Low Voltage Ride-Through (LVRT) Capability

A wind generating plant shall be able to remain online during voltage disturbances up to the time periods and associated voltage levels set forth in the standard in Figure 1, below, if the Transmission Provider's System Impact Study shows that low voltage ride-through capability is required to ensure safety or reliability.

The standard applies to voltage measured at the Point of Interconnection as defined in this LGIA. The figure shows the ratio of actual to nominal voltage (on the vertical axis) over time (on the horizontal axis). Before time 0.0, the voltage at the transformer is the nominal voltage. At time 0.0, the voltage drops. If the voltage remains at a level greater than 15 percent of the nominal voltage for a period that does not exceed 0.625 seconds, the plant must stay online. Further, if the voltage returns to 90 percent of the nominal voltage within 3 seconds of the beginning of the voltage drop (with the

voltage at any given time never falling below the minimum voltage indicated by the solid line in Figure 1), the plant must stay online. The Interconnection Customer may not disable low voltage ride-through equipment while the wind plant is in operation. Two key features of this regulation are:

1. A wind generating plant must have low voltage ride-through capability down to 15 percent of the rated line voltage for 0.625 seconds;
2. A wind generating plant must be able to operate continuously at 90 percent of the rated line voltage, measured at the high voltage side of the wind plant substation transformer(s).

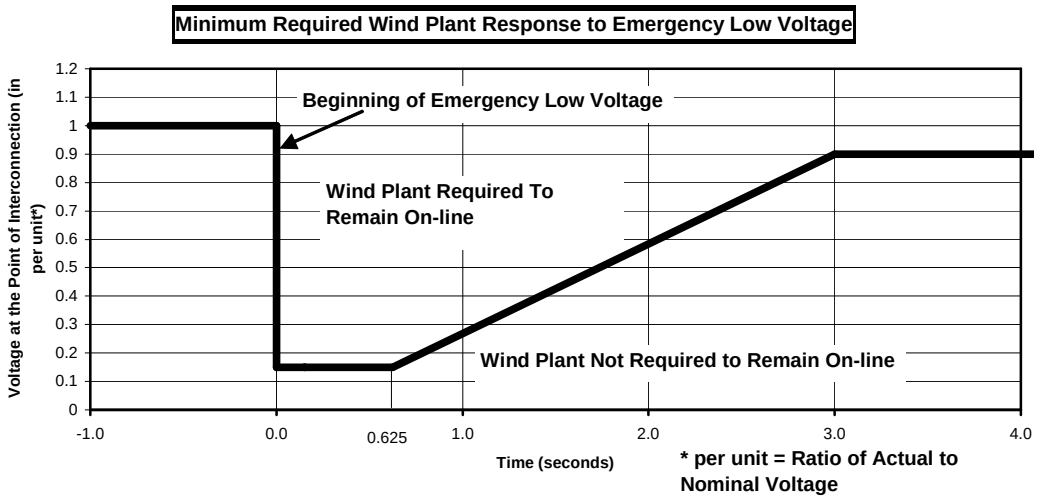


Figure 1 Proposed low voltage ride-through standard

ii. Power Factor Design Criteria (Reactive Power)

A wind generating plant shall maintain a power factor within the range of 0.95 leading to 0.95 lagging, measured at the Point of Interconnection as defined in this LGIA,

if the Transmission Provider's System Impact Study shows that such a requirement is necessary to ensure safety or reliability. The power factor range standard can be met by using, for example, power electronics designed to supply this level of reactive capability (taking into account any limitations due to voltage level, real power output, etc.) or fixed and switched capacitors if agreed to by the Transmission Provider, or a combination of the two. The Interconnection Customer shall not disable power factor equipment while the wind plant is in operation. Wind plants shall also be able to provide sufficient dynamic voltage support in lieu of the power system stabilizer and automatic voltage regulation at the generator excitation system if the System Impact Study shows this to be required for system safety or reliability.

iii. Supervisory Control and Data Acquisition (SCADA) Capability

The wind plant shall provide SCADA capability to transmit data and receive instructions from the Transmission Provider to protect system reliability. The Transmission Provider and the wind plant Interconnection Customer shall determine what SCADA information is essential for the proposed wind plant, taking into account the size of the plant and its characteristics, location, and importance in maintaining generation resource adequacy and transmission system reliability in its area.

Appendix C

[NOTE: THESE PROVISIONS TO BE ADOPTED AS APPENDIX G TO THE LGIP]

APPENDIX G

INTERCONNECTION PROCEDURES FOR A WIND GENERATING PLANT

Appendix G sets forth procedures specific to a wind generating plant. All other requirements of this LGIP continue to apply to wind generating plant interconnections.

A. Special Procedures Applicable to Wind Generators

The wind plant Interconnection Customer, in completing the Interconnection Request required by section 3.3 of this LGIP, may provide to the Transmission Provider a set of preliminary electrical design specifications depicting the wind plant as a single equivalent generator. Upon satisfying these and other applicable Interconnection Request conditions, the wind plant may enter the queue and receive the base case data as provided for in this LGIP.

No later than six months after submitting an Interconnection Request completed in this manner, the wind plant Interconnection Customer must submit completed detailed electrical design specifications and other data (including collector system layout data) needed to allow the Transmission Provider to complete the System Impact Study.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 35

(Docket No. RM05-4-001; Order No. 661-A)

Interconnection for Wind Energy

(Issued December 12, 2005)

AGENCY: Federal Energy Regulatory Commission

ACTION: Order on Rehearing and Clarification

SUMMARY: The Federal Energy Regulatory Commission is granting in part and denying in part the requests for rehearing and clarification of its Final Rule on Interconnection for Wind Energy, Order No. 661. Order No. 661 requires public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to append to their standard large generator interconnection procedures and large generator interconnection agreements in their open access transmission tariffs standard procedures and technical requirements for the interconnection of large wind generation.

EFFECTIVE DATE: Changes made to Order No. 661 in this order on rehearing and clarification will become effective on [insert date 30 days after publication in the Federal Register].

FOR FURTHER INFORMATION CONTACT:

Bruce A. Poole (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8468

G. Patrick Rooney (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-6205

P. Kumar Agarwal (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-8923

LaChelle Brooks (Technical Information)
Office of Markets, Tariffs and Rates
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6522

Jeffery S. Dennis (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426
(202) 502-6027

SUPPLEMENTARY INFORMATION:

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Joseph T. Kelliher, Chairman;
Nora Mead Brownell, and Suedeen G. Kelly.

Interconnection for Wind Energy Docket No. RM05-4-001

ORDER NO. 661-A

ORDER ON REHEARING AND CLARIFICATION

(Issued December 12, 2005)

1. On June 2, 2005, the Commission issued Order No. 661, the Final Rule on Interconnection for Wind Energy (Final Rule).[1] Several entities have filed timely requests for rehearing and clarification of the Final Rule.[2] In this order, the Commission grants in part and denies in part the requests for rehearing and clarification.

I. Background

2. In Order No. 2003,[3] the Commission adopted standard procedures and a standard

[1] Interconnection for Wind Energy, Order No. 661, 70 FR 34993 (June 16, 2005), FERC Stats. & Regs. ¶ 31,186 (2005) (Final Rule); see also Order Granting Extension of Effective Date and Extending Compliance Date, 70 FR 47093 (Aug. 12, 2005), 112 FERC ¶ 61,173 (2005).

[2] Those entities requesting rehearing and/or clarification, and the acronyms used to refer to them in this order, are listed in Appendix A to this order.

[3] Standardization of Generator Interconnection Agreements and Procedures, Order No. 2003, 68 FR 49845 (Aug. 19, 2003), FERC Stats. & Regs., Regulations Preambles ¶ 31,146 (2003) (Order No. 2003), order on reh'g, 69 Fed. Reg. 15,932 (Mar. 24, 2004), FERC Stats & Regs., Regulations Preambles ¶ 31,160 (2004) (Order No. 2003-A), (continued)

agreement for the interconnection of large generation facilities. The Commission required public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to file revised Open Access Transmission Tariffs (OATTs) containing these standard provisions, and use them to provide interconnection service to generating facilities having a capacity of more than 20 megawatts.

3. In Order No. 2003-A, on rehearing, the Commission noted that the standard interconnection procedures and agreement were based on the needs of traditional generation facilities and that a different approach might be more appropriate for generators relying on other technologies, such as wind plants.[4] Accordingly, the Commission granted certain clarifications, and also added a blank Appendix G to the standard Large Generation Interconnection Agreement (LGIA) for future adoption of requirements specific to other technologies.[5]

4. The Commission issued a Notice of Proposed Rulemaking (NOPR) that proposed technical standards applicable to the interconnection of large wind generating plants[6] to

---

order on reh'g, 70 Fed. Reg. 265 (January 4, 2005), FERC Stats & Regs., Regulations Preambles ¶ 31,171 (2004) (Order No. 2003-B), order on reh'g, 70 FR 37661 (June 30, 2005), FERC Stats. & Regs. ¶ 31,190 (2005) (Order No. 2003-C); see also Notice Clarifying Compliance Procedures, 106 FERC ¶ 61,009 (2004).

[4] Order No. 2003-A at P 407, n.85.

[5] Id.

[6] Large wind generating plants are those with an output rated at more than 20 MW at the point of interconnection. The interconnection requirements for small generators rated at 20 MW or less are set forth in Standardization of Small Generator

(continued)

be included in Appendix G of the LGIA.[7] We proposed the standards in light of our findings in Order No. 2003-A noted above and in response to a petition submitted by the American Wind Energy Association (AWEA).[8] Specifically, the Commission proposed to establish uniform standards in Appendix G that would require large wind plants seeking to interconnect to the grid to: (1) demonstrate low voltage ride-through capability; in other words, show that the plant can remain on line during voltage disturbances up to specified time periods and associated voltage levels; (2) have supervisory control and data acquisition (SCADA) capability to transmit data and receive instructions from the Transmission Provider; and (3) maintain a power factor within the range of 0.95 leading to 0.95 lagging, measured at the high voltage side of the substation transformers. The Commission proposed to permit the Transmission Provider to waive the low voltage ride-through requirement on a comparable and not unduly discriminatory basis. We proposed to permit the Transmission Provider to waive or defer compliance with the power factor requirement where it is not necessary. The Commission did not

---

Interconnection Agreements and Procedures, Order No. 2006, 70 FR 34190 (June 13, 2005), FERC Stats. & Regs. ¶ 31,180 (2005), reh'g pending.

[7] See Interconnection for Wind Energy and Other Alternative Technologies, Notice of Proposed Rulemaking, 70 FR 4791 (Jan. 31, 2005), 110 FERC ¶ 61,036 (2005) (NOPR).

[8] See Petition for Rulemaking or, in the Alternative, Request for Clarification of Order No. 2003-A, and Request for Technical Conference of the American Wind Energy Association (May 20, 2004), filed in Docket Nos. RM02-1-005 and PL04-15-000 (AWEA Petition).

propose to adopt a proposal by AWEA to allow a wind generator to "enter the interconnection queue and conduct its own Feasibility Study, having obtained the information necessary to do so upon paying the initial deposit and submitting its interconnection application" (referred to as "self-study" provisions).[9] The Commission did, however, ask for comments on how to balance the need of wind generators to obtain certain data from the Transmission Provider before completing their Interconnection Requests with the need to protect critical energy infrastructure information and commercially sensitive data against unwarranted disclosure.

5. In the Final Rule, the Commission adopted final standard procedures and technical requirements for the interconnection of large wind plants in Appendix G, and required all public utilities that own, control, or operate facilities for transmitting electric energy in interstate commerce to append Appendix G to the Large Generator Interconnection Procedures (LGIPs) and LGIAs in their OATTs. As described in more detail below, the Commission adopted provisions establishing standards for low voltage ride-through and power factor design criteria, and requiring that wind plants meet those standards if the Transmission Provider shows, in the System Impact Study, that they are needed to ensure the safety or reliability of the transmission system. Additionally, the Appendix G adopted by the Commission included a SCADA requirement applicable to all wind

[9] See AWEA Petition at 13.

plants. Finally, as described in more detail below, the Commission adopted in Appendix G to the LGIP limited special interconnection procedures applicable to wind plants.

II. Requests for Rehearing and Clarification and Commission Conclusions

A. Low Voltage Ride-Through Provisions

6. In the Final Rule, the Commission adopted a low voltage ride-through standard, but provided that a wind plant is required to meet the standard only if the Transmission Provider shows, in the System Impact Study, that low voltage ride-through capability is needed to ensure safety or reliability. The standard (adopted in Figure 1 of Appendix G to the LGIA), if applicable, requires the wind plant to stay online for specified time periods and at associated voltage levels where there is a disturbance on the transmission system. The Final Rule requires that the required voltage levels be measured at the Point of Interconnection.

7. Several entities requested rehearing of various aspects of the low voltage ride-through requirement and standard included in the Final Rule, including: (1) provisions that require low voltage ride-though only when the System Impact Study shows that such capability is necessary for safety or reliability; (2) the specific low voltage ride-through standard adopted in the Final Rule; (3) the point of measurement for the standard; and (4) arguments that Transmission Providers should be permitted to adopt other provisions of the German low voltage ride-through standard (which the Commission referenced in the Final Rule).

8. However, as described in more detail below, NERC and AWEA jointly requested

that the Commission delay the effective date of the Final Rule to give them time to resolve concerns expressed by NERC regarding the low voltage ride-through provisions. The Commission granted this extension, and on September 19, 2005, NERC and AWEA submitted a joint report with recommended revisions.

1. Case-by-Case Application/Burden of Proof for Applying the Low Voltage Ride-Through Standard

9. Prior to the NERC/AWEA joint report, several entities objected on rehearing to the Final Rule's adoption of a low voltage ride-through requirement on a case-by-case basis, placing the burden of proof on the Transmission Provider to show that low voltage ride-through capability is needed. ATC, EEI, NERC, NRECA/APPA, and SCE, among others, urged the Commission to return to the approach in the NOPR, which would have required low voltage ride-through for all wind plants unless waived by the Transmission Provider on a not unduly discriminatory basis. ATC noted that interconnection studies only consider a snapshot of the transmission system, and do not take into account changes in the future that may cause a need for low voltage ride-through capability to ensure reliability. ATC, as well as EEI and SCE, argued that under the case-by-case approach adopted in the Final Rule, Transmission Providers will need to perform additional analyses to determine if a reliability need will exist over the life of the wind plant. SCE, for example, noted that while a particular System Impact Study may not conclusively demonstrate that low voltage ride-through is needed at that time, if other generation projects are built, the first wind plant may come to need low voltage ride-

through. According to various entities, the additional analyses needed to take these scenarios into account will increase the time, cost and complexity of wind plant interconnections and could be a barrier to their development.[10]

10. Furthermore, ATC asserted that the case-by-case approach imposes the responsibility for resolving reliability concerns that arise in the future on the Transmission Provider because wind generating plants cannot be retrofitted with low voltage ride-through capability. Similarly, NRECA/APPA argued that this approach unduly discriminates in favor of wind plants in that low voltage ride-through capability may not be "necessary" (and therefore required) for a specific plant because other generators or Transmission Providers can "make up the difference."[11] ATC also contended that the case-by-case approach may require the Transmission Provider to incur capital costs that should have been incurred by the wind plant.

11. EEI and NU argued that the case-by-case approach adopted by the Commission in the Final Rule "lowers the bar for reliability."[12] NERC similarly asserted that requiring Transmission Providers to justify common elements of good utility practice on a case-by-

[10] New York ISO asserts that the case-by-case approach could lead to acute problems in New York, where it has received interconnection applications from wind plants totaling over 5000 MW of generation. According to New York ISO, conducting case-by-case reviews for each of these projects could greatly complicate the study process and result in substantial delays.

[11] Request for Rehearing of NRECA/APPA at 6.

[12] Request for Rehearing of EEI at 8.

case basis is unwise and may deter Transmission Providers from implementing and following good utility practice.[13] Southern Company states that the Transmission Provider, as the entity responsible for maintaining reliability, should not bear the burden of proof to establish what is required to maintain system reliability. Southern Company states that it supports the Commission's statement that Transmission Providers should not be permitted to require wind plants to install costly equipment that is not needed for reliability, but argues that the burden of proof should be shifted, and the System Impact Study should establish that such equipment is not required. Also, NRECA/APPA argued that the case-by-case approach imposes unreasonable reliability risks, and effectively voids the requirement that wind plants have low voltage ride-through capability "in a broad range of circumstances."[14]

12. Those requesting rehearing raised several other arguments regarding the case-by-case approach and burden of proof for applying the low voltage ride-through standard. NERC believed that the case-by-case approach could unintentionally create a "patchwork" of varying requirements. EEI and NU also suggested that requiring a showing of need may introduce prolonged uncertainties into the interconnection process if parties disagree as to the study assumptions. SCE asserted that rather than limiting opportunities for undue discrimination, the requirement of a showing of need could result

[13] New York ISO states that it adopts NERC's position on this issue.

[14] Request for Rehearing of NRECA/APPA at 6.

in discriminatory treatment in areas with large amounts of wind generation because projects lower in the queue may be responsible for additional costs since the need for low voltage ride-through could not be demonstrated for earlier projects. EEI contended that Order No. 2003 already contains provisions allowing the parties to an interconnection to exercise their discretion in complying with system reliability obligations, and that there is no evidence of problems with these procedures that justifies such a significant departure from them in the Final Rule. Further, EEI argued that the Final Rule was a significant departure from the NOPR and that the Commission should not adopt it without providing an opportunity for comments on it. Finally, NRECA/APPA argued that the Commission has not explained how this approach is consistent with NERC and WECC standards.

2. Specific Low Voltage Ride-Through Standard

13. Certain requests for rehearing and clarification also addressed the specific low voltage ride-through standard adopted by the Commission in the Final Rule. In its request for rehearing, NERC asserted that the standard in Figure 1 of the Final Rule is not appropriate. More specifically, NERC contended that Figure 1, by allowing a wind plant to disconnect from the transmission system when the voltage drops below 15 percent of the nominal voltage, could result in violation of NERC Reliability Standard TPL-002-0. This standard requires transmission planners to ensure that the system will remain stable and within applicable thermal and voltage ratings, with no loss of demand or curtailment of firm transfers, where there is a normally cleared fault on a single element, which is typically four to eight cycles or 0.067 to 0.133 seconds (67 to 133 milliseconds).

According to NERC, a fault occurring on a transmission line near a wind plant could cause the voltage at that point to drop to zero for this clearing time. NERC stated that because Figure 1 would allow the wind plant to disconnect when the voltage drops below 15 percent of the nominal voltage, the loss of the single grid element (the transmission line) would be compounded by the loss of the real power (and any reactive power) produced by the wind plant. This "double contingency event" (loss of both the transmission line and wind plant) violates Reliability Standard TPL-002-0, NERC asserted.

14. To remedy this problem, NERC requested that the Commission simply require wind plants to meet NERC and regional reliability council requirements.[15] Alternatively, NERC argued that the rule should be modified to require wind plants to remain connected through a normally cleared single line to ground or three phase fault. Specifically, NERC asserted that Figure 1 should be altered to require a wind plant to remain online for 0.167 seconds (167 milliseconds), or ten cycles, if voltage at the high side of the wind plant step-up transformer is reduced to zero. After 0.167 seconds (167 milliseconds), but before 0.625 seconds (625 milliseconds), NERC argued that Figure 1 should require the wind plant to stay connected as long at the voltage is at or above 15 percent of the

[15] ISO-NE argued that the Commission should have required wind plants to be subject to the same system performance standards that are applied to other generating technologies.

nominal voltage. NERC contended that these modifications would reduce the risk to the reliability of the electric system to an acceptable level.[16]

15. Similarly, NU asserted that wind plants should be required to "remain on-line for all faults cleared by normal operation of all protective equipment unless clearing the fault . . . isolates the plant from the rest of the grid."[17] According to NU, this change would require generators to have low voltage ride-through capability down to zero percent of the nominal voltage at the Point of Interconnection. CenterPoint also contend that wind plants should be required to maintain low voltage ride-through capability down to zero percent of the rated line voltage 150 milliseconds (.150 seconds) (the time generally needed for the transmission system protective equipment to clear the fault). NU and CenterPoint argued that this change would reduce the likelihood that a low voltage event would escalate to a cascading outage or voltage collapse. NU also asserted that this requirement is similar to those applicable to other generators, and could be achieved by wind turbines that are currently available. NU stated that the standard adopted in the Final Rule would threaten reliability by allowing a wind plant to reduce output, or trip offline, simply due to a typical system fault.

---

[16] ISO-NE also suggested that, if the Commission adopted a low voltage ride-through standard, it be modified to require the wind plant to be connected at zero voltage for "a time period associated with the typical clearing time of a normal design contingency fault." Request for Rehearing of ISO-NE at 4.

[17] Request for Rehearing of NU at 5.

16. NRECA/APPA also objected to the low voltage ride-through standard adopted in the Final Rule. Specifically, they contended that the Final Rule should not have established the low voltage ride-through curve as an absolute standard, and instead should have permitted Transmission Providers to adopt an alternative curve (subject to review by the Commission if there is a dispute) when the System Impact Study shows that it is necessary. ISO-NE, going further, requested that if the Commission adopted a low voltage ride-through standard, it should be only a guideline for wind turbine manufacturers. NRECA/APPA asserted that the Final Rule did not conclude that the low voltage ride-through standard will protect reliability or address the technical concerns raised by comments, and, by stating that the Commission might consider an alternative low voltage ride-through standard, recognizes that it may not be adequate to preserve reliability in all circumstances. Alternatively, NRECA/APPA asked that the Commission clarify that Transmission Providers may support variations from the low voltage ride-through curve in the Final Rule, based on local and subregional reliability conditions, under the three variation standards adopted in the Final Rule.

17. EEI asserted that the technical challenges presented by wind generation are being considered by the industry worldwide, and that many international standards differ from the Commission's Final Rule. Both EEI and SCE objected to the specific low voltage ride-through standard through comparison to the German interconnection guidelines. Particularly, EEI noted that the German grid code requires wind plants to remain connected to the grid following a fault that results in the voltage at the Point of

Interconnection dropping to 15 percent of the nominal voltage for as long as 0.15 seconds. According to EEI, revisions to the German grid code are nearing completion that will require wind plants to remain connected to the transmission system following a fault that drops the voltage at the Point of Interconnection to zero percent of the nominal voltage for as long at 0.15 seconds. Further, EEI reported that the Hydro-Québec requirements for wind farm interconnection are stricter than the Commission's Final Rule; they require wind plants to ride through a fault resulting in a voltage drop to zero percent of nominal voltage for as long as 0.15 seconds. Finally, EEI noted that Ireland requires wind plants to stay online after a fault that drops the voltage to 15 percent of nominal voltage for as long as 0.15 seconds. SCE additionally asserted that the requirement that low voltage ride-through be shown to be necessary in the System Impact Study conflicts with the German wind interconnection guidelines because those guidelines assume that all generation will meet the low voltage ride-through standard. SCE stated that the Final Rule should adopt low voltage ride-through capability as a governing standard, with exceptions approved by the governing technical body (NERC or the Western Electricity Coordinating Council (WECC), a regional reliability council), as in the German standard.

18. In the Final Rule, the Commission stated that "the low voltage ride-through requirement, and the time periods and associated voltage levels set forth in Appendix G, Figure 1, apply to three-phase faults." ATC sought clarification as to whether the low voltage ride-through requirement applied only to three-phase faults. Assuming that is the

case, ATC asked whether there was a requirement for single-phase and double-phase faults.

3. Point of Measurement for the Low Voltage Ride-Through Standard

19. NERC argued on rehearing that because the Point of Interconnection may be some distance from a wind plant, the plant might actually disconnect at voltages higher than 15 percent of the nominal voltage at the high side of the wind plant step-up transformer. According to NERC, this could create a further risk of a double contingency event.[18] To avoid this risk, NERC contended that low voltage ride-through capability should be measured at the high voltage terminal of the wind plant step-up transformer. Southern Company stated that a revision to section A.i.2 of the LGIA Appendix G was necessary to reflect the Commission's decision in the Final Rule to adopt the Point of Interconnection as the measurement point.

4. Adoption of Other Provisions from the German Standards

20. SCE noted that while the Final Rule adopted a low voltage ride-through standard based on the German wind interconnection guidelines, the Commission did not adopt the related requirements in the German guidelines. It noted several provisions of the German guidelines that it stated go hand-in-hand with the low voltage ride-through standard.[19]

---

[18] See supra, P 13.

[19] See Request for Rehearing and Clarification of SCE at 9-10.

SCE asked the Commission to clarify that Transmission Providers may implement these other guidelines in the German standard.

5. NERC/AWEA Recommended Revisions to Low Voltage Ride-Through Provisions

21. As noted above, NERC filed a request for rehearing of the Final Rule contending, in part, that the specific low voltage ride-through standard adopted by the Commission would permit violations of a NERC system performance standard.[20] On August 4, 2005, NERC and AWEA filed a request to extend the effective date of the Final Rule to allow for discussions to resolve the reliability concerns expressed by NERC. They committed to submitting to the Commission a joint final report on their discussions. On August 5, 2005, the Commission issued an order granting this request.[21]

22. On September 19, 2005, NERC and AWEA submitted their joint final report, which recommended revisions to the low voltage ride-through provisions of the Final Rule. They state that the recommended revisions are supported by the NERC Planning Committee and AWEA members. NERC states that the concerns expressed in its request for rehearing will be resolved if the Commission adopts the recommended revisions.

23. Specifically, NERC and AWEA recommend a different low voltage ride-through

---

[20] See supra, P 13.

[21] Interconnection for Wind Energy, 70 FR 47093 (Aug. 12, 2005), 112 FERC ¶ 61,173 (2005).

section to be inserted in Appendix G. The recommended provisions include a transition period standard, which would apply to wind plants that either: (a) have interconnection agreements signed and filed with the Commission, filed with the Commission in unexecuted form, or filed with the Commission as non-conforming agreements between January 1, 2006 and December 31, 2006, with a scheduled in-service date no later than December 31, 2007; or (b) involve wind turbines subject to a procurement contract executed before December 31, 2005 for delivery through 2007. During this transition period, wind plants would be required to ride through low voltage events down to 0.15 per unit for normal clearing times up to a maximum of nine cycles.

24. Following this transition period, the NERC/AWEA proposal would require wind plants to ride through low voltage events down to a zero voltage level for "location-specific" clearing times up to a maximum of nine cycles. If the fault on the transmission system remained after this clearing time, the joint recommendation would permit the wind plant to disconnect from the system.

25. Under the joint recommendation of NERC and AWEA, during both the transition period and after, low voltage ride-through capability would be required for all new wind plant interconnections, instead of only when the System Impact Study shows that such capability is needed for safety or reliability, as in the Final Rule. Additionally, in both cases the point of measurement for the requirement would be at the high side of the wind plant step-up transformer, instead of at the Point of Interconnection, as in the Final Rule. NERC and AWEA also recommend eliminating Figure 1 during both the transition

period and after the transition period because the low voltage ride-through standard described in their Joint Report replaces the voltage trace represented by Figure 1.

26. Finally, NERC and AWEA recommend limiting the variations to the low voltage ride-through provisions that were permitted by the Final Rule. The Final Rule permits Transmission Providers to justify variations between their pro forma tariff and the Final Rule Appendix G based on the regional reliability, the "consistent with or superior to," or the independent entity variation standards in Order No. 2003.[22] NERC and AWEA recommend that variations to their proposed low voltage ride-through provisions be permitted on an interconnection-wide basis only, reasoning that such a limitation is appropriate because the provisions are intended to satisfy a NERC reliability standard, and because wind generators could incur significant additional costs if they had to meet many different standards. NERC and AWEA note that limiting variations would not restrict the ability to request a deviation in a specific non-conforming agreement filed with the Commission (as opposed to a variation built into a pro forma tariff).

27. The Commission issued notice of the NERC/AWEA joint report on September 21, 2005, and provided interested parties with the opportunity to submit comments on or before October 3, 2005. FPL Energy, National Grid, New York ISO and PJM all filed comments supporting the technical recommendations in the joint report.

28. National Grid also asks that the Commission make two clarifications. First, it asks

[22] Final Rule at P 107, 109.

the Commission to clarify that while the point of measurement for compliance with the low voltage ride-through standard would be at the high side of the step-up transformer, the point of measurement for reactive power would remain at the Point of Interconnection. Second, National Grid requests that the nine cycle maximum clearing time in the low voltage ride-through provision applies only to three-phase faults. It says that single line-to-ground faults are typically much longer than nine cycles, so a general, non-specified standard is more appropriate for such faults.

29. New York ISO, while strongly supporting the technical aspects of the NERC/AWEA joint recommendations, urges the Commission to reject the proposal that variations to the low voltage ride-through provision be permitted only on an interconnection-wide basis or through individually-filed interconnection agreements. It argues that this could hamper efforts to preserve reliability in individual regions, and asserts that satisfying NERC planning standards is not sufficient to preserve reliability because New York State, as well as other regions, sometimes need more stringent reliability requirements than those of NERC. New York ISO says that the Commission has viewed NERC's criteria as being minimum reliability requirements, which individual regions may exceed if necessary. Therefore, New York ISO argues that at a minimum, the Commission should permit independent entities to seek variations from the low voltage ride-through standards recommended by NERC and AWEA.

30. Finally, New York ISO asks the Commission to clarify that, assuming the NERC/AWEA recommendations are adopted, the "filing date" for purposes of the

proposed transition period includes the date that conforming interconnection agreements are fully and finally executed. New York ISO notes that executed conforming agreements need not be filed with the Commission. Therefore, it contends that the transition period should apply to agreements executed within its timeframe but not filed with the Commission.

Commission Conclusion on Low Voltage Ride-Through Provisions

31. The Commission grants rehearing with regard to the low voltage ride-through provisions, and adopts the joint recommendation of NERC and AWEA without modification. This provides a standard that will ensure that wind plants are interconnected to the grid in a manner that will not degrade system reliability. Furthermore, this standard satisfies the reliability concerns expressed by NERC, and either satisfies or renders moot many of the rehearing requests described above, including those related to the case-by-case application of the low voltage ride-through standard and point of measurement for the low voltage ride-through standard. Additionally, the joint recommendation also responds to the arguments on rehearing of EEI and SCE regarding comparison to the German interconnection guidelines.

32. We are eliminating Figure 1 from Appendix G because the standard we are adopting in Appendix G replaces that figure. Accordingly, all references to Figure 1 in the preamble to the Final Rule should be read to apply to the standard now described in Appendix G.

33. We also adopt the NERC/AWEA proposal to permit variations to the low voltage ride-through provisions of Appendix G only on an interconnection-wide basis. The low voltage ride-through provisions we adopt in this order on rehearing were crafted specifically, after negotiation among the wind industry and NERC, to ensure that NERC Reliability Standard TPL-002-0 is met in all regions. While other interconnection standards may be more susceptible to variation among Transmission Providers or independent entities, the close connection of this standard to an industry-wide reliability standard persuades us that limiting variations to those made on an interconnection-wide basis will best ensure that reliability is protected. Accordingly, we reject SCE's request that we clarify that Transmission Providers may implement other guidelines from the German interconnection standard. Adoption of other guidelines from the German standard on a Transmission Provider-specific basis could result in varying requirements that may not meet established reliability standards. For the same reasons, we also reject New York ISO's assertion that the Commission should continue to permit variations to the low voltage ride-through provisions under the three variation standards in the Final Rule, and particularly the independent entity variation. We note, however, that under section 1211 of the Energy Policy Act of 2005, the State of New York "may establish rules that result in greater reliability within that State, as long as such action does not result in lesser reliability outside the State than that provided by the reliability

standards."[23] Therefore, the Commission will consider proposed variations from the State of New York under this statutory provision.

34. In response to the arguments of NRECA/APPA that the Final Rule should have permitted Transmission Providers to adopt alternative low voltage ride-through standards, and ISO-NE's contention that the standard in the Final Rule should be only a guideline, we find that the definitive standard we adopt here will provide certainty to wind developers and manufacturers and ensure that reliability is maintained and NERC planning standards are met. If another standard is necessary for a specific wind plant interconnection to maintain reliability, a non-conforming agreement may be filed with the Commission.

35. In response to ATC and National Grid, we clarify that the low voltage ride-through provisions we are adopting apply to all types of faults, not just to three-phase faults. The standard refers to three-phase faults with normal clearing as well as single line to ground faults with delayed clearing. In response to National Grid's specific concern, we clarify that the nine cycle maximum clearing time expressed in the low voltage ride-through provisions applies only to three-phase faults. Single line to ground faults have typically much longer clearing times, as National Grid notes, and the low voltage ride-through provisions adopted here recognize this difference by specifically

[23] Energy Policy Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 594, 945 (2005).

referring to "single line to ground faults with delayed clearing." This non-specified standard is appropriate for those types of faults.

B. Power Factor (Reactive Power) Provisions

36. In the Final Rule, the Commission adopted in Appendix G to the LGIA a power factor standard applicable to wind plants. The Final Rule provides that wind plants are required to meet this standard only if the Transmission Provider shows, in the System Impact Study, that reactive power capability is necessary to ensure the safety or reliability of the transmission system. The specific power factor standard in Appendix G to the LGIA, if applicable, requires a wind plant to maintain a power factor within the range of 0.95 leading to 0.95 lagging (hereinafter +/- 0.95), to be measured at the Point of Interconnection.

37. Requests for rehearing and/or clarification of these provisions concern whether wind plants should have to maintain a required power factor only where the System Impact Study shows that it is required for reliability or safety, and whether the power factor standard and point of measurement adopted by the Commission in the Final Rule are appropriate.

1. Case-by-Case Application/Burden of Proof for Applying the Power Factor Standard

38. Several entities object to the provisions in the Final Rule that require wind plants to maintain the required power factor only when the Transmission Provider, in the System Impact Study, shows that it is necessary to ensure safety or reliability. NERC

objects to this approach because it may deter Transmission Providers from implementing and following good utility practice and could create a "patchwork" of varying requirements. NU argues that this approach "lowers the bar for reliability," and will add complexity, cost and delay to the generator interconnection process because Transmission Providers will be required to perform more studies to determine whether reactive power capability is necessary for reliability or safety. Southern Company states that the Transmission Provider, as the entity responsible for maintaining reliability, should not bear the burden of proof to establish what is required to maintain system reliability. It supports the Commission's statement that Transmission Providers should not be permitted to require wind plants to install costly equipment that is not needed for reliability, but argues that the burden of proof should be shifted to the generator.

39. NRECA/APPA notes that traditional generators are required to meet the power factor standard not because reactive power is needed in every case to preserve reliability, but instead because the transmission system is dynamic and requires flexibility over time to maintain reliability. They state that the need for reactive power in the future under a variety of operating conditions cannot be determined with perfect certainty in the System Impact Study. The case-by-case approach, they contend, grants an undue preference to wind plants, imposes risks to system reliability, and shifts costs to consumers and other generating plants. The risk to system reliability is that the Final Rule may only require a wind plant to provide reactive power after other wind plants have been installed without such capability, and that at that point the resources from that single plant may not be

enough to protect the transmission system. NRECA/APPA also asserts that the case-by-case approach increases uncertainty, contrary to the Commission's conclusion in the Final Rule, because each wind plant will face different requirements based on the outcome of the System Impact Study. Additionally, it contends that this approach creates more opportunities for discrimination because it would permit wind plants to be treated differently.

40. ATC contends that the Commission has offered no guidance as to what power factor range would be acceptable if a reliability need is not identified (and thus reactive power is not required), and whether wind plants in this instance must operate within any particular reactive power operating band. Similarly, NU expresses concern that wind plants could operate at any power factor in the absence of a showing of need in the System Impact Study, and thus avoid a physical requirement for delivering power onto the transmission system. According to ATC, the rule could be interpreted to permit wind plants to operate at any power factor they choose. It claims that reactive power is needed for each generator, and that each generator should be obligated to operate within a range of power factors, regardless of whether the transmission system as a whole needs additional reactive power capability. ATC recommends that at a minimum, the Commission require all wind plants to meet a power factor range of 0.95 leading to 1.0 (unity), and allow the Transmission Provider to require a range of 1.0 (unity) to 0.95 lagging if the System Impact Study shows that there is a reliability need.

Commission Conclusion

41. The Commission will not modify the Final Rule to require wind plants to meet the power factor standard without a showing by the Transmission Provider, through the System Impact Study, that it is needed for safety or reliability. The case-by-case approach to a reliability needs assessment adopted in the Final Rule will not threaten reliability, as several of those seeking rehearing argue. As we noted in the Final Rule, if reactive power is necessary to maintain the safety or reliability of the transmission system, the System Impact Study performed by the Transmission Provider will establish that need.[24] We stated in the Final Rule, and reiterate here, that the System Impact Study is the appropriate study for determining whether reactive power capability is needed.[25] Furthermore, we reasoned in the Final Rule that requiring wind plants to maintain the power factor standard only if the System Impact Study shows it to be necessary will not only ensure that increased reliance on wind power will not degrade system safety or reliability, but also will limit opportunities for undue discrimination by ensuring that Transmission Providers do not require costly equipment that is not necessary for reliability.[26]

---

[24] Final Rule at P 51.

[25] Id.

[26] Id.

42. NERC states that the decision in Order No. 661 to use a case-by-case approach may deter Transmission Providers from following Good Utility Practice, and may have the unintended consequence of spawning a patchwork of varying requirements. We agree with NERC that Transmission Providers must follow Good Utility Practice when interconnecting all generating plants, including wind plants, and that not following Good Utility Practice when performing System Impact Studies could lead to problems. However, the Commission points out that every Transmission Provider is required under Order No. 2003 to follow Good Utility Practice. Transmission Providers are required to complete a detailed System Impact Study, and are required to ensure that NERC reliability standards are met in all instances. This includes performing studies to determine what is necessary to ensure that the interconnection of a wind generating facility does not degrade grid reliability. The Commission recognizes that the industry (and particularly NERC) is continuing to address technical issues involved in the interconnection of wind plants. If NERC through its stakeholders and Board approval process develops a new standard, the Commission will entertain such a standard. Finally, we disagree with NRECA/APPA's suggestion that the Final Rule threatens the reliability of the transmission system because it may require only wind plants later in the queue to provide reactive power, which may not be sufficient to protect the grid. The System Impact Study will take into account the system's need for reactive power, both as it exists today and under reasonable anticipated assumptions. NRECA/APPA has not explained how assessing the need for reactive power through the System Impact Study process will

result in too little reactive power being available in the future. Whenever a new generator is added to its system, the Transmission Provider must complete a new System Impact Study to ensure that reliability requirements are met; this may require a new wind generator later in the queue to meet the reactive power requirement.

43. We also reject arguments that the case-by-case approach is inappropriate because of the dynamic nature of the transmission system. The fact that the transmission system is constantly changing is not new or unique to the study of wind plant interconnections. The studies that are part of the interconnection process should take into account likely circumstances that could occur on the Transmission Provider's system, whether the studies are conducted in connection with a proposed wind plant or another type of generating facility.

44. Furthermore, we are not persuaded that the approach adopted in the Final Rule will result in additional studies, increased costs and delays, and cost shifts. First, as noted previously, the System Impact Study, as well as the other interconnection studies, should take into account a variety of assumptions concerning anticipated transmission system conditions. If additional or expanded studies are needed to determine whether the power factor standard is necessary, the Commission does not believe that the additional burden will outweigh the cost considerations underlying the case-by-case approach. Finally, although the case-by-case approach may result in some delay, we remind the parties to a wind plant interconnection, like other interconnections, that they are still required to meet the milestones set forth in the LGIP. Any increased costs from completing expanded or

additional studies within the timeframe required by this rule will be borne by the wind plant Interconnection Customer, as provided in Order No. 2003, which will leave other generators and the Transmission Provider unharmed.

45. The Commission also rejects arguments that the case-by-case approach provides more opportunities for discrimination. As we noted in the Final Rule Appendix G was adopted to take into account the technical differences between wind plants and traditional generating plants. One of these differences is that for wind plants, reactive power capability is a significant added cost, while it is not a significant additional cost for traditional generators. Given these technical differences, treating wind plants differently with regard to reactive power requirements is not unduly discriminatory or preferential. Additionally, we note that the outcome of the System Impact Study, which determines whether reactive power will be required, can be challenged, which will serve to minimize the opportunities for discrimination by the Transmission Provider. Also, the wind plant Interconnection Customer will have recourse to the Commission if it believes the Transmission Provider has acted in a discriminatory manner.

46. The Commission declines to adopt ATC's request that all wind plants, at a minimum, operate within a power factor range of 0.95 leading to 1.0 (unity). This requirement would essentially require reactive power in every case, which we have already rejected. If reactive power capability is needed, including a power factor range of 0.95 leading to 1.0 (unity), the System Impact Study will demonstrate this need.

2. Specific Power Factor Standard

47. NRECA/APPA argues that the Commission should clarify that wind generators must meet the same reactive power requirements as other generators, provided the requirements are imposed in a nondiscriminatory manner. It notes that some Transmission Providers impose a power factor range wider that +/- 0.95 on all new generation, and argues that in such cases, the same range should be applied to wind plants. It argues that not imposing the same range threatens reliability and shifts the costs of preserving reliability to customers or competing generators.

48. EEI and NU assert that wind plants should regulate voltage to a set point established by the Transmission Provider, as do synchronous generators. EEI contends that the language it offered in its initial comments would provide this necessary clarity, while also maintaining the flexibility provided in Order No. 2003 so that individual, site-specific conditions may be addressed.[27] NU states that wind turbines have this capability, either inherently (doubly fed induction generators) or through external equipment.

49. NRECA/APPA also expresses concern that the phrase "taking into account any limitations due to voltage level, real power output, etc." in the power factor requirements

[27] EEI's March 2, 2005 comments in this proceeding suggest that we require the wind plant to maintain a power factor within the range specified by the Transmission Provider "from time to time," but would not require that it operate outside of the 0.95 leading to 0.95 lagging range. See Comments of EEI (March 2, 2005) at 5-6.

section of Appendix G could create operational problems for Transmission Providers with wind plants on their systems. Specifically, it is concerned that this language could exempt wind plants from their reactive power requirements during startup and low output periods, which could degrade reliability during a system contingency.

Commission Conclusion

50. With regard to NRECA/APPA's request for clarification that wind generators must meet a wider power factor range because some Transmission Providers impose a power factor range wider that +/- 0.95 on all new generation, we note that if we were to allow the Transmission Provider to impose a wider power factor range as a matter of routine, that would defeat the purpose of adopting a reactive power standard for wind generators. However, we note that if the System Impact Study shows the need for a power factor range wider than +/- 0.95 for safety or reliability, the Transmission Provider must file a non-conforming agreement, as Order No. 2003 permits. The Commission will consider these non-conforming agreements on a case by case basis. If a Transmission Provider has a different power factor range in its LGIA and wishes to apply that same range in Appendix G, it may seek a variation from the Commission under the variation standards approved in the Final Rule.[28] We remind Transmission Providers, however, that the Commission has adopted a specific power factor standard for wind plants because of their technical differences. Any proposed variations will be viewed in light of

[28] Final Rule at P 109.

these technical differences.

51. In response to the assertion of EEI and NU that wind plants should regulate voltage to a set point established by the Transmission Provider, we note that in the Final Rule we concluded that article 9.6.2 of the LGIA (which applies to all plants, including wind plants) already requires that the "Interconnection Customer . . . operate the Large Generating Facility to maintain the specified output voltage or power factor at the Point of Interconnection."[29]

52. Finally, the Commission addressed in the Final Rule the concerns raised by NRECA/APPA regarding the phrase "taking into account any limitations due to voltage level, real power output, etc." We stated that this language was necessary due to the technical limitations of wind generating technology.[30] We noted that all wind generating equipment vendors cannot meet the required power factor range at all levels of output. We reiterate that these technical differences make the disputed language necessary. Furthermore, without this language, a Transmission Provider could discriminate against a wind plant by requiring that it operate at the stated power factor at voltages where it is technically infeasible to do so.

3. Point of Measurement of Power Factor

53. National Grid asks that if the Commission adopts the recommended revisions to

[29] Id. at P 55.

[30] Id. at P 56.

the low voltage ride-through provisions filed jointly by AWEA and NERC, it clarify that while the point of measurement for compliance with the low voltage ride-through standard would be at the high-side of the step-up transformer, the point of measurement for reactive power is at the Point of Interconnection.

Commission Conclusion

54. We clarify that the point of measurement for the reactive power standard is at the Point of Interconnection.

C. Self-Study of Interconnection Feasibility

55. In the Final Rule, the Commission adopted special interconnection procedures that allow the wind plant Interconnection Customer, when completing the Interconnection Request form required by section 3.3 of the LGIP, to provide the Transmission Provider with a simplified set of preliminary data depicting the wind plant as a single equivalent generator.[31] Once the wind generator has provided this data and satisfied all other applicable Interconnection Request conditions, the special procedures permit the wind plant to enter the queue and receive the base case data as provided for in the LGIP. Finally, the special procedures adopted in the Final Rule require the wind plant Interconnection Customer to submit, within six months of submitting the Interconnection Request, completed detailed electrical design specifications and other data (including

[31] "Single equivalent generator" information is design data that represents the aggregate electrical characteristics of the individual wind generators as a single generator.

collector system layout data) needed by the Transmission Provider to complete the System Impact Study.

56. Southern Company argues on rehearing that these provisions give wind developers a special preference that unfairly disfavors other generating technologies.

57. EEI, NU and Southern Company contend that the "self-study" provisions of the Final Rule will add further complexity and uncertainty to the queue process and make queue management and assignment of cost responsibilities more difficult for Transmission Providers with large wind-powered generation projects in their queue. Southern Company adds that the self-study provisions could increase costs to market participants because the Transmission Provider will have to run multiple studies. EEI argues that until the industry can fully address the issues raised by these provisions in a technical forum, the Commission should remove the provisions from Appendix G. EEI and NU assert that the provisions do not protect against a wind plant Interconnection Customer making significant revisions to its project proposal. If the Commission does not remove the provisions entirely, EEI and NU suggest that the Commission allow the Transmission Provider to determine whether the detailed electrical design specifications later submitted by the wind plant Interconnection Customer are a material modification to the initial proposal, which would result in the initial Interconnection Application being withdrawn.

58. Midwest ISO agrees with the Commission that a wind plant should be able to enter

the queue and receive base case data based on preliminary design specifications. However, it seeks rehearing of the provision that permits a wind plant to wait up to six months before submitting final design specifications. It argues that this procedure promotes inefficiency because the Transmission Provider may be able to evaluate the proposed interconnection, but cannot do so because it lacks necessary data. Midwest ISO requests that the Commission revise the Appendix G self-study provisions to permit the Transmission Provider to notify the wind plant Interconnection Customer of its intent to start the System Impact Study. Once this notice is given, the wind plant developer would have five business days to "submit either actual design specifications or generic specifications based on typical equipment used in the industry."[32] Further, Midwest ISO proposes that if the wind plant Interconnection Customer submits generic specifications, it should have to accept cost uncertainty, because additional facilities may be required when the actual design specifications are taken into account. Midwest ISO asserts that this would limit delays in the study process and would allow the Transmission Provider to identify potential problems or eliminate tenuous or technically deficient projects earlier and to better use its resources to study proposed interconnections.

Commission Conclusion

59. The Commission will deny these requests for rehearing. We will make one minor revision to label these special interconnection procedures for wind plants as "Appendix

[32] Request for Rehearing of Midwest ISO at 4.

7" to the LGIP, as discussed in more detail below.

60. In response to arguments that the self-study procedures for wind plants give these plants a preference, we reiterate that these procedures were developed to recognize the technical differences of wind plants. Unlike conventional generators, wind plant design specifications and configurations can change significantly based on their placement on the transmission system.[33] For example, the placement of wind turbines, voltage support devices, transformers, and other equipment (including the layout of the medium voltage collector system) depend on the location of the wind plant, the location of other generators on the transmission system, and other information included in the base case data.[34] To accommodate these differences, the Final Rule permits wind plants to enter the interconnection queue with a set of preliminary electrical design specifications depicting the wind plant as a single generator, instead of providing detailed design specifications as required by Order No. 2003. Treating wind plants differently in this regard is not unduly discriminatory or preferential, but as noted elsewhere, simply recognizes that wind plants have different technical characteristics than the more traditional forms of generation that the LGIP and LGIA were designed to accommodate. We continue to believe that without this reasonable accommodation, Transmission Providers could frustrate the interconnection of wind plants by requiring them to submit

[33] Final Rule at P 97.

[34] Id.

detailed design data, which they cannot do until later in the interconnection process.

61. We are not persuaded that the reasonable self-study provision we adopted will make the interconnection queue process significantly more difficult or complex. Wind plant Interconnection Customers who provide the preliminary single generator equivalent data are required to provide final detailed electrical design specifications no later than six months after submitting the initial Interconnection Request. This six-month time period takes into account the procedures needed before the start of the System Impact Study, including the Feasibility Study and negotiation of study agreements. Therefore, the Transmission Provider will receive from the wind plant the detailed design information needed to conduct the System Impact Study. For this reason, we also deny Midwest ISO's request to modify the six-month deadline. If we adopted Midwest ISO's proposed modifications, the Transmission Provider could request that the wind plant provide detailed design specifications at any time it believes it is ready to begin the System Impact Study, even a day after the initial Interconnection Request is submitted. As a result, this modification would defeat the purpose of permitting wind plants to submit preliminary design specifications, and could allow Transmission Providers to frustrate the interconnection of wind plants.

62. With respect to the alternative suggestion by EEI and NU that the Transmission Provider be permitted to determine that a detailed design specification later submitted by the wind plant Interconnection Customer is a material modification of the Interconnection Request, we note that section 4.4 of the LGIP already addresses modifications and will

apply to wind plants as well as other generating technologies. When applying this section to wind plant Interconnection Requests that first submit preliminary design specifications, Transmission Providers are not to consider the detailed design data provided later by the wind plant Interconnection Customer to be a material modification unless it significantly departs from the preliminary specifications provided. In other words, the detailed design provided later should be substantially the same as the initial single-generator equivalent design in terms of its costs and effect on the transmission system.

63. Finally, to avoid confusion, the Commission will rename the Appendix G to the LGIP it adopted in the Final Rule as "Appendix 7, Interconnection Procedures for a Wind Generating Plant." Accordingly, when complying with the Final Rule and this order on rehearing, public utilities must adopt the special interconnection procedures applicable to wind plants as Appendix 7 to their LGIPs. The low voltage ride-through, power factor design criteria and SCADA provisions should continue to be labeled "Appendix G" to the LGIA.

D. Adoption of Appendix G on an Interim Basis Only

64. EEI and NU each generally argue that the Commission should apply Appendix G only on an interim basis, and should defer to NERC and Institute of Electrical and Electronics Engineers (IEEE) processes to develop formal technical standards. Southern Company argues that the Commission should defer to NERC, regional reliability councils, and other technical organizations to develop technical requirements for wind

plants, and should suspend application of the Final Rule and formally request that these entities develop technical standards. Southern Company argues that this would avoid the problems that result from having the Commission review each variation to Appendix G as the technical standards are developed and revised. It also asserts that the Commission should not be the arbiter of technical disputes, such as the outcome of the System Impact Study or specific SCADA requirements, as the Final Rule provides.

65. As noted above, NERC similarly argues that the Commission should only require wind plants to meet NERC and regional reliability council requirements, noting that Figure 1 is likely to remain static over time, which could hamper the development of wind generator technology. EEI notes that NERC has established a Wind Generator Task Force that is examining existing standards and will make proposals later this year. It states that the industry worldwide is addressing technical challenges presented by wind generation. Significant modifications are being developed for the German grid code, and Hydro-Québec is considering several reliability issues regarding wind generator interconnection. NERC further notes that Hydro-Québec requires the same dynamic performance of wind plants that it requires of other generating facilities, and that major wind turbine manufacturers have shown that they can meet this requirement. EEI proposes that the industry conduct a technical forum to resolve issues related to wind plant interconnection, concluding with formal recommendations to the Commission that could be used in a new NOPR, or to develop formal proposals for NERC or IEEE standards.

Commission Conclusion

66. The Commission denies these requests for rehearing, and others noted earlier, that ask us to adopt Appendix G only on an interim basis. Standards are needed today because no nationwide standard is currently in place and it is uncertain when such a standard will be finalized. Without a firm standard in place, the current ad hoc practices for wind interconnection requirements may frustrate the interconnection of wind plants. As we noted in the Final Rule, Appendix G is necessary to recognize the technical differences between wind plants and traditional plants to ensure that the entry of wind generation into markets is not unnecessarily inhibited.

67. We recognize, however, that the industry continues to study and address issues raised by the interconnection and operation of wind plants. For that reason, the Commission stated in the Final Rule that if another entity develops an alternate standard, a Transmission Provider may seek to justify adopting it as a variation from Appendix G.[35] We also stated that we would consider a future industry petition to revise Appendix G to conform to a NERC-developed standard.[36] We reiterate both of those statements

[35] Id. at P 34. We note that in this order on rehearing, variations to the low voltage ride-through standard will only be permitted on an interconnection-wide basis. As we note above, however, non-conforming agreements may be submitted to the Commission. See P 33-34, supra.

[36] Id.

here, and also note that under the Energy Policy Act of 2005, the Commission will be addressing mandatory reliability standards.[37]

E. Transition Period

68. In the Final Rule, the Commission adopted a transition period that applies to the low voltage ride-through, power factor design criteria and SCADA requirements. These technical requirements in the Final Rule Appendix G, if applicable, apply only to LGIAs signed, filed with the Commission in unexecuted form, or filed as non-conforming agreements, on or after January 1, 2006, or the date six months after publication of the Final Rule in the Federal Register, whichever is later.[38] The Commission adopted this transition period to allow wind equipment currently in the process of being manufactured to be completed without delay or added expense, and to ensure that the Final Rule did not interrupt the supply of wind turbines.

69. NRECA/APPA argues that the transition period is arbitrary, capricious, and unduly discriminatory. NRECA/APPA asserts that the Commission adopted the

---

[37] See Energy Policy Act of 2005, Pub. L. No. 109-58, § 1211, 119 Stat. 594, 941 (2005).

[38] The Final Rule was published in the Federal Register on June 16, 2005. Thus, the low voltage ride-through, power factor design criteria and reactive power provisions in the Final Rule, as revised herein, will apply to LGIAs signed, filed with the Commission in unexecuted form, or filed as non-conforming agreements, on or after January 1, 2006.

transition period with no technical justification and no explanation of how the transition period will maintain the reliability of the transmission system. They contend that the transition period requires transmission customers and competing generators to bear the reliability effects of wind plants interconnected during the transition period. While NRECA/APPA state that there are "valid commercial considerations" that should be taken into account for the existing inventory of wind equipment, they contend that such determinations should be made on a case-by-case basis.

Commission Conclusion

70. The Commission declines to remove the transition period as NRECA/APPA request. We adopted this reasonable transition mechanism to allow wind turbines in the process of being manufactured to be completed without delay or additional expense.[39] The transition period ensures that the supply of wind turbines is not unfairly or unreasonably interrupted.[40] Furthermore, contrary to NRECA/APPA's contention, the Commission considered the possible reliability effects of the transition period, and concluded that the remaining provisions of Order No. 2003 will adequately protect reliability.[41] The remaining provisions of Order No. 2003 will also ensure that other generators or the Transmission Provider will not bear the reliability effects of a wind

[39] Final Rule at P 115.

[40] Id.

[41] Id.

plant because that rule, and the LGIA and LGIP contained in it, ensure that generating facilities are not interconnected in a manner that degrades reliability.

III. Document Availability

71. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through FERC's Home Page (http://www.ferc.gov) and in FERC's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, N.E., Room 2A, Washington, D.C. 20426.

72. From the Commission's Home Page on the Internet, this information is available in the Commission's document management system, eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

73. User assistance is available for eLibrary and the Commission's website during normal business hours. For assistance, please contact FERC Online Support at 1-866-208-3676 (toll free) or 202-502-6652 (e-mail at FERCOnlineSupport@FERC.gov), or the Public Reference Room at 202-502-8371, TTY 202-502-8659 (e-mail at public.referenceroom@ferc.gov).

IV. Effective Date

74. As noted above, on August 5, 2005, the Commission issued an order extending the

effective date of the Final Rule to October 14, 2005.[42] Those provisions of the Final Rule not revised in this order on rehearing and clarification are effective as of that date. Changes made to the Final Rule in this order on rehearing and compliance will become effective on [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

V. Compliance with the Final Rule and Order on Rehearing and Clarification

75. In the Commission's August 5, 2005 order extending the effective date of the Final Rule, the Commission also extended to November 14, 2005, the date by which all public utilities that own, control, or operate transmission facilities in interstate commerce are to adopt, in their OATTS, the Final Rule Appendix 7 (as described above)[43] as an amendment to the LGIP, and Final Rule Appendix G as an amendment to the LGIA. By further notice issued October 28, 2005, the Commission extended this date further, to December 30, 2005. Public utilities who have already filed a Final Rule Appendix G as amendments to the LGIPs and LGIAs in their OATTs must file, by December 30, 2005, the revisions to the Final Rule Appendix G to the LGIA made in this order on rehearing.

[42] Order Granting Extension of Effective Date and Extending Compliance Date, 70 FR 47093 (Aug. 12, 2005), 112 FERC ¶ 61,173 (2005).

[43] See supra, P 60.

List of Subjects in 18 C.F.R. Part 35

Electric power rates; Electric utilities.

By the Commission. Chairman Kelliher dissenting in part with a separate statement attached.

(S E A L)

Magalie R. Salas,
Secretary.

In consideration of the foregoing, the Commission revises part 35, Chapter I, Title 18 of the Code of Federal Regulations as follows.

PART 35 B FILING OF RATE SCHEDULES

1. The authority citation for part 35 continues to read as follows:

Authority: 16 U.S.C. §§ 791a-825r, §§ 2601-2645; 31 U.S.C. § 9701; 42 U.S.C. §§ 7101-7352.

2. In § 35.28, the first sentences of currently existing paragraphs (f)(1) and (f)(1)(iii) are revised, a new paragraph (f)(1)(iii) is added, and currently existing paragraph (f)(1)(iii) is renumbered to account for new paragraph (f)(1)(iii), all to read as follows:

§ 35.28 Non-discriminatory open access transmission tariff.

* * * * *

(f) Standard generator interconnection procedures and agreements.

(1) Every public utility that is required to have on file a non-discriminatory open access transmission tariff under this section must amend such tariff by adding the standard interconnection procedures and agreement contained in Order No. 2003, FERC Stats. & Regs. & 31,146 (Final Rule on Generator Interconnection), as amended by the Commission in Order No. 661, FERC Stats. & Regs. ¶ 31,186 (Final Rule on Interconnection for Wind Energy), and the standard small generator interconnection

procedures and agreement contained in Order No. 2006, FERC Stats. & Regs. ¶ 31,180 (Final Rule on Small Generator Interconnection), or such other interconnection procedures and agreements as may be approved by the Commission consistent with Order No. 2003, FERC Stats. & Regs. & 31,146 (Final Rule on Generator Interconnection) and Order No. 2006, FERC Stats. & Regs. ¶ 31,180 (Final Rule on Small Generator Interconnection).

(i) The amendment to implement the Final Rule on Generator Interconnection required by the preceding subsection must be filed no later than January 20, 2004.

(ii) The amendment to implement the Final Rule on Small Generator Interconnection required by the preceding subsection must be filed no later than August 12, 2005.

(iii) The amendment to implement the Final Rule on Interconnection for Wind Energy required by the preceding subsection must be filed no later than December 30, 2005.

(iv) Any public utility that seeks a deviation from the standard interconnection procedures and agreement contained in Order No. 2003, FERC Stats. & Regs. & 31,146 (Final Rule on Generator Interconnection), as amended by the Commission in Order No. 661, FERC Stats. & Regs. ¶ 31,186 (Final Rule on Interconnection for Wind Energy), or the standard small generator interconnection procedures and agreement contained in

Order No. 2006, FERC Stats. & Regs. ¶ 31,180 (Final Rule on Small Generator Interconnection), must demonstrate that the deviation is consistent with the principles of either Order No. 2003, FERC Stats. & Regs. & 31,146 (Final Rule on Generator Interconnection) or Order No. 2006, FERC Stats. & Regs. ¶ 31,180 (Final Rule on Small Generator Interconnection).

[NOTE: THE APPENDICES WILL NOT BE PUBLISHED IN THE CODE OF FEDERAL REGULATIONS]

Appendix A

List of Entities Requesting Rehearing and/or Clarification or Submitting Comments and Acronyms

ATC – American Transmission Company LLC
CenterPoint – CenterPoint Energy Houston Electric, LLC
EEI – Edison Electric Institute
FPL Energy – FPL Energy, LLC
ISO-NE – ISO New England, Inc.
Midwest ISO – Midwest Independent Transmission System Operator, Inc.
National Grid – National Grid USA
NERC – North American Electric Reliability Council
New York ISO – New York Independent System Operator, Inc.
NRECA/APPA – National Rural Electric Cooperative Association and American Public Power Association
NU – Northeast Utilities
PJM – PJM Interconnection, L.L.C.
SCE - Southern California Edison Company
Southern Company – Southern Company Services, Inc

Appendix B

[NOTE: THESE PROVISIONS TO BE ADOPTED AS APPENDIX G TO THE LGIA]

APPENDIX G

INTERCONNECTION REQUIREMENTS FOR A WIND GENERATING PLANT

Appendix G sets forth requirements and provisions specific to a wind generating plant. All other requirements of this LGIA continue to apply to wind generating plant interconnections.

A. Technical Standards Applicable to a Wind Generating Plant

i. Low Voltage Ride-Through (LVRT) Capability

A wind generating plant shall be able to remain online during voltage disturbances up to the time periods and associated voltage levels set forth in the standard below. The LVRT standard provides for a transition period standard and a post-transition period standard.

Transition Period LVRT Standard

The transition period standard applies to wind generating plants subject to FERC Order 661 that have either: (i) interconnection agreements signed and filed with the Commission, filed with the Commission in unexecuted form, or filed with the Commission as non-conforming agreements between January 1, 2006 and December 31, 2006, with a scheduled in-service date no later than December 31, 2007, or (ii) wind

generating turbines subject to a wind turbine procurement contract executed prior to December 31, 2005, for delivery through 2007.

1. Wind generating plants are required to remain in-service during three-phase faults with normal clearing (which is a time period of approximately 4 – 9 cycles) and single line to ground faults with delayed clearing, and subsequent post-fault voltage recovery to prefault voltage unless clearing the fault effectively disconnects the generator from the system. The clearing time requirement for a three-phase fault will be specific to the wind generating plant substation location, as determined by and documented by the transmission provider. The maximum clearing time the wind generating plant shall be required to withstand for a three-phase fault shall be 9 cycles at a voltage as low as 0.15 p.u., as measured at the high side of the wind generating plant step-up transformer (i.e. the transformer that steps the voltage up to the transmission interconnection voltage or "GSU"), after which, if the fault remains following the location-specific normal clearing time for three-phase faults, the wind generating plant may disconnect from the transmission system.
2. This requirement does not apply to faults that would occur between the wind generator terminals and the high side of the GSU or to faults that would result in a voltage lower than 0.15 per unit on the high side of the GSU serving the facility.
3. Wind generating plants may be tripped after the fault period if this action is intended as part of a special protection system.

4. Wind generating plants may meet the LVRT requirements of this standard by the performance of the generators or by installing additional equipment (e.g., Static VAr Compensator, etc.) within the wind generating plant or by a combination of generator performance and additional equipment.

5. Existing individual generator units that are, or have been, interconnected to the network at the same location at the effective date of the Appendix G LVRT Standard are exempt from meeting the Appendix G LVRT Standard for the remaining life of the existing generation equipment. Existing individual generator units that are replaced are required to meet the Appendix G LVRT Standard.

Post-transition Period LVRT Standard

All wind generating plants subject to FERC Order No. 661 and not covered by the transition period described above must meet the following requirements:

1. Wind generating plants are required to remain in-service during three-phase faults with normal clearing (which is a time period of approximately 4 – 9 cycles) and single line to ground faults with delayed clearing, and subsequent post-fault voltage recovery to prefault voltage unless clearing the fault effectively disconnects the generator from the system. The clearing time requirement for a three-phase fault will be specific to the wind generating plant substation location, as determined by and documented by the transmission provider. The maximum clearing time the wind generating plant shall be required to withstand for a three-phase fault shall be 9 cycles after which, if the fault remains following the

location-specific normal clearing time for three-phase faults, the wind generating plant may disconnect from the transmission system. A wind generating plant shall remain interconnected during such a fault on the transmission system for a voltage level as low as zero volts, as measured at the high voltage side of the wind GSU.

2. This requirement does not apply to faults that would occur between the wind generator terminals and the high side of the GSU.

3. Wind generating plants may be tripped after the fault period if this action is intended as part of a special protection system.

4. Wind generating plants may meet the LVRT requirements of this standard by the performance of the generators or by installing additional equipment (e.g., Static VAr Compensator) within the wind generating plant or by a combination of generator performance and additional equipment.

5. Existing individual generator units that are, or have been, interconnected to the network at the same location at the effective date of the Appendix G LVRT Standard are exempt from meeting the Appendix G LVRT Standard for the remaining life of the existing generation equipment. Existing individual generator units that are replaced are required to meet the Appendix G LVRT Standard.

ii. Power Factor Design Criteria (Reactive Power)

A wind generating plant shall maintain a power factor within the range of 0.95 leading to 0.95 lagging, measured at the Point of Interconnection as defined in this LGIA, if the Transmission Provider's System Impact Study shows that such a requirement is

necessary to ensure safety or reliability. The power factor range standard can be met by using, for example, power electronics designed to supply this level of reactive capability 606 (taking into account any limitations due to voltage level, real power output, etc.) or fixed and switched capacitors if agreed to by the Transmission Provider, or a combination of the two. The Interconnection Customer shall not disable power factor equipment while the wind plant is in operation. Wind plants shall also be able to provide sufficient dynamic voltage support in lieu of the power system stabilizer and automatic voltage regulation at the generator excitation system if the System Impact Study shows this to be required for system safety or reliability.

iii. Supervisory Control and Data Acquisition (SCADA) Capability

The wind plant shall provide SCADA capability to transmit data and receive instructions from the Transmission Provider to protect system reliability. The Transmission Provider and the wind plant Interconnection Customer shall determine what SCADA information is essential for the proposed wind plant, taking into account the size of the plant and its characteristics, location, and importance in maintaining generation resource adequacy and transmission system reliability in its area.

Appendix C

[NOTE: THESE PROVISIONS TO BE ADOPTED AS APPENDIX G TO THE LGIP]

APPENDIX 7

INTERCONNECTION PROCEDURES FOR A WIND GENERATING PLANT

Appendix G sets forth procedures specific to a wind generating plant. All other requirements of this LGIP continue to apply to wind generating plant interconnections.

A. Special Procedures Applicable to Wind Generators

The wind plant Interconnection Customer, in completing the Interconnection Request required by section 3.3 of this LGIP, may provide to the Transmission Provider a set of preliminary electrical design specifications depicting the wind plant as a single equivalent generator. Upon satisfying these and other applicable Interconnection Request conditions, the wind plant may enter the queue and receive the base case data as provided for in this LGIP.

No later than six months after submitting an Interconnection Request completed in this manner, the wind plant Interconnection Customer must submit completed detailed electrical design specifications and other data (including collector system layout data) needed to allow the Transmission Provider to complete the System Impact Study.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Interconnection for Wind Energy Docket No. RM05-4-001

(Issued December 12, 2005)

Joseph T. KELLIHER, Chairman, *dissenting in part*:

I vote for this order because it constitutes an improvement over the final rule. I agree with the Commission's decision to grant rehearing with respect to the low voltage ride-through (LVRT) provisions and to adopt the joint recommendation of NERC and AWEA. As the order points out, by adopting a definitive, uniform, LVRT standard, the Commission "provide[s] certainty" to the industry and "ensure[s] that reliability is maintained and NERC planning standards are met."[1]

Unfortunately, the Commission's decision on LVRT contrasts with its decision to exempt wind generators from compliance with the same power factor standard as all other generators. The Commission requires all non-wind generators to maintain a power factor within the range of 0.95 leading to 0.95 lagging, which NERC has determined to be "within a range required by Good Utility Practice."[2] Order No. 661, however, singles out wind generators for special treatment by exempting them from meeting the standard power factor requirement unless the Transmission Provider demonstrates in the System Impact Study that reactive power capability is necessary to ensure the safety or reliability of the transmission system. In my view, exempting only wind generators from the power factor standard does not provide certainty to the industry, results in an undue preference for wind generators and does not adequately ensure that reliability of the transmission system is maintained.

Section 205 of the Federal Power Act broadly precludes public utilities, in any transmission or sale subject to the Commission's jurisdiction, from "mak[ing] or grant[ing] any undue preference or advantage to any person or subject[ing] any person to any undue prejudice or disadvantage. . . ."[3] In my view, Order No. 661 gives preferential treatment to

[1] Order at P34.

[2] Order No. 2003 at P541.

[3] 16 U.S.C. § 824d(b).

wind generators, since it exempts wind generators from meeting the same power factor requirement as all other non-wind generators. The issue is whether the preferential treatment afforded to wind generators is undue.

I do not believe that either the record or the explanation offered in this order provides a basis for giving preferential treatment to wind generators when it comes to meeting the power factor requirement. The order's attempt to justify discriminating in favor of wind generators as an accommodation for "technical differences"[4] is not convincing. The only "technical" difference identified is the assertion that compliance with reactive power capability is more expensive for wind generators than for other generator resources.[5] While one can understand why wind generators would like to be relieved of the added cost of complying with the same power factor standard as all other non-wind generators, I fail to see how the desire to avoid incurring the costs of complying with the Commission's standardized power factor requirement constitutes a technological difference warranting discriminatory treatment.

Equally troubling, I disagree with the Commission's decision to brush aside the concerns raised by NERC and other protesters that the Commission has "lowered the bar" for reliability by shifting the burden to the Transmission Provider to justify the need for wind generators to comply with the same power factor requirement as non-wind generators. I find little comfort in the Commission's view that any reliability concerns can be addressed in the System Impact Study if the Transmission Provider proves that a wind generator's compliance with the reactive power factor standard is necessary. In my view, shifting the burden to Transmission Providers to make such a showing simply cannot be reconciled with the approach taken by the Commission in Order No. 2003 which presumes the need for all generators to comply with power factor requirement under "Good Utility Practice." [6]

As a result, I would have granted rehearing and returned to the approach proposed by the Commission in the NOPR of requiring all generators to meet the same power factor

---

[4] Order at P45.

[5] *Id*. ("One of these [technical] differences is that for wind plants, reactive power capability is a significant added cost, while it is not a significant additional cost for traditional generators.").

[6] Order No. 2003 at PP541-42.

standard absent a waiver by the Transmission Provider. Accordingly, I dissent in part from the order.

_____

Joseph T. Kelliher

Standard: BAL-003-1 Frequency Response and Frequency Bias Setting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in BAL-003-1/Comments**
R1. Each Balancing Authority shall review its Frequency Bias Settings by January 1 of each year and recalculate its setting to reflect any change in the Frequency Response of the Balancing Authority Area. R1.1. The Balancing Authority may change its Frequency Bias Setting, and the method used to determine the setting, whenever any of the factors used to determine the current bias value change. R1.2. Each Balancing Authority shall report its Frequency Bias Setting, and method for determining that setting, to the NERC Operating Committee.	This Requirement has been moved into BAL-003-1 Attachment A & FRS Form 1	Attachment A Each Balancing Authority shall report its previous year's Frequency Response Measure (FRM), Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO on FRS Form 1 by January 10 each year. If the ERO posts the official list of events after December 10, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1. AND FRS Form 1 Note : Balancing Authorities with variable Frequency Bias Settings shall calculate monthly average Frequency Bias Settings. The previous year's monthly averages will be reported annually on FRS Form 1.
R2. Each Balancing Authority shall establish and maintain a Frequency	This Requirement	R2. Each Balancing Authority not participating in Overlap Regulation Service shall implement the Frequency Bias Setting

Standard: BAL-003-1 Frequency Response and Frequency Bias Setting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in BAL-003-1/Comments**
Bias Setting that is as close as practical to, or greater than, the Balancing Authority's Frequency Response. Frequency Bias may be calculated several ways: **R2.1.** The Balancing Authority may use a fixed Frequency Bias value which is based on a fixed, straight-line function of Tie Line deviation versus Frequency Deviation. The Balancing Authority shall determine the fixed value by observing and averaging the Frequency Response for several Disturbances during on-peak hours. **R2.2.** The Balancing Authority may use a variable (linear or non-linear) bias value, which is based on a variable function of Tie Line deviation to Frequency Deviation. The Balancing Authority shall determine the variable frequency bias value by	is included in BAL-003-1 as described in the Proposed Language Section.	(fixed or variable) validated by the ERO, into its Area Control Error (ACE) calculation beginning on the date specified by the ERO to ensure effectively coordinated Tie Line Bias control. AND Attachment A Each Balancing Authority shall report its previous year's Frequency Response Measure (FRM), Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO on FRS Form 1 by January 10 each year. If the ERO posts the official list of events after December 10, Balancing Authorities will be given 30 days from the date the ERO posts the official list of events to submit their FRS Form 1. AND FRS Form 1 Note : Balancing Authorities with variable Frequency Bias Settings shall calculate monthly average Frequency Bias Settings. The previous year's monthly averages will be reported annually on FRS Form 1. AND

Standard: BAL-003-1 Frequency Response and Frequency Bias Setting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in BAL-003-1/Comments**
analyzing Frequency Response as it varies with factors such as load, generation, governor characteristics, and frequency.		A portion of this Requirement is being phased out in accordance with the process detailed in Attachment B. This phase out is intended to bring the Frequency Bias Setting closer or equal to the natural Frequency Response.
R3. Each Balancing Authority shall operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias, unless such operation is adverse to system or Interconnection reliability.	This Requirement has been moved into BAL-003-1 Requirement R3.	R3. Each Balancing Authority not receiving Overlap Regulation Service shall operate its Automatic Generation Control (AGC) in Tie Line Bias mode to ensure effectively coordinated control, unless such operation would have an Adverse Reliability Impact on the Balancing Authority's Area. In this instance, the Balancing Authority shall document the reasons for such operation.
R4. Balancing Authorities that use Dynamic Scheduling or Pseudo-ties for jointly owned units shall reflect their respective share of the unit governor droop response in their respective Frequency Bias Setting. R4.1. Fixed schedules for Jointly Owned Units mandate that Balancing Authority (A) that contains the Jointly Owned Unit must incorporate the respective share of the unit governor droop response for any Balancing	This Requirement has been removed from the BAL-003-1 standard.	This Requirement addresses how to calculate Frequency Bias Settings. This is no longer needed since the Frequency Bias Settings are calculated in FRS Form 1 using Frequency Response associated with the "official" list of events and a couple of "floor or ceiling" limits (% of peak load/gen and FRO). The entire calculation is built into the FRS Form 1 workbook.

Standard: BAL-003-1 Frequency Response and Frequency Bias Setting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in BAL-003-1/Comments**
Authorities that have fixed schedules (B and C). R4.2. The Balancing Authorities that have a fixed schedule (B and C) but do not contain the Jointly Owned Unit shall not include their share of the governor droop response in their Frequency Bias Setting.		
R5. Balancing Authorities that serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of the Balancing Authority's estimated yearly peak demand per 0.1 Hz change. **R5.1.** Balancing Authorities that do not serve native load shall have a monthly average Frequency Bias Setting that is at least 1% of its estimated maximum generation level in the coming year per 0.1 Hz change.	This Requirement has been moved into BAL-003-1 Requirement R5.	R5. Each Balancing Authority shall use a monthly average Frequency Bias Setting whose absolute value is at least equal to one of the following: • The minimum percentage of the Balancing Authority Area's estimated yearly Peak Demand within its metered boundary per 0.1 Hz change as specified by the ERO in accordance with Attachment B. • The minimum percentage of the Balancing Authority Area's estimated yearly peak generation for a generation-only Balancing Authority, per 0.1 Hz change as specified by the ERO in accordance with Attachment B.
R6. A Balancing Authority that is performing Overlap Regulation Service shall increase its Frequency	This Requirement has been	R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify its Frequency Bias Setting in its ACE calculation to be equivalent to the sum of the

Standard: BAL-003-1 Frequency Response and Frequency Bias Setting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in BAL-003-1/Comments**
Bias Setting to match the frequency response of the entire area being controlled. A Balancing Authority shall not change its Frequency Bias Setting when performing Supplemental Regulation Service.	moved into BAL-003-1 Requirement R4.	Frequency Bias Settings of the participating Balancing Authorities as validated by the ERO or calculate the Frequency Bias Setting based on the entire area being combined and thereby represent the Frequency Response for the combined area being controlled.

From: Monica Benson
To: monica.benson@nerc.net
Subject: NERC: Standards Announcement - Project 2007-12 Frequency Response | Ballot Pools, Formal Comment Period and Initial Ballot and Non-Binding Poll Information
Date: Tuesday, October 25, 2011 12:03:36 PM

Standards Announcement

Project 2007-12 Frequency Response

Ballot Pool Windows Now Open: Oct. 25 – Nov. 23, 2011
Formal Comment Period Open: Oct. 25 – Dec. 8, 2011
Initial Ballot and Non-Binding Poll Window: Nov. 29 – Dec. 8, 2011

Available Now

BAL-003-1 – Frequency Response and Frequency Bias Setting, an implementation plan and several additional associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Thursday, December 8, 2011. Ballot pools are being formed and the ballot pool windows are open through 8 a.m. Eastern on Wednesday, November 23.

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended March 7, 2011
- Frequency Response Standard Background Document – Provides an explanation of each of the proposed requirements; identifies how the proposed standard proposes to address FERC directives from Order 693; and on the last page provides an overview of the field trial (currently in Step 4)
- Attachment A – ERO's Process for assigning a Frequency Response Obligation and Frequency Bias Setting to each Balancing Authority
- Attachment B – ERO's Process for Adjusting Minimum Frequency Bias Setting
- FRS Form 1 (four versions - one for each of the four Interconnections) and FRS Form 2 (seven versions – two to collect data for Interconnections with a single Balancing Authority at two second and three second intervals; five to collect data for Interconnections with multiple Balancing Authorities at two second, three second, four second and five second intervals) – Both forms are proposed for the ERO's use (in conjunction with Attachment A) in determining each Interconnection's necessary amount of Frequency Response for allocation to Balancing Authorities. Instructions are now on the first page of each FRS Form 1 and FRS Form 2
- Mapping Document - Identifies each requirement in the already approved BAL-003-0.1b and identifies how that requirement has been treated in the revisions proposed in BAL-003-1.
- Unofficial comment form in Word format – This is for informal use when compiling

responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for BAL-003-1 and Associated VRFs/VSLs
Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of BAL-003-1, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with BAL-003-1. RBB members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pools to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)
The list server for the initial ballot is: bp-2007-12_Freq_Resp_in@nerc.com
Non-Binding Poll list server: bp-2007-12_NB_OCT2011_in@nerc.com

Instructions for Commenting
Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps
The drafting team is planning a webinar in November to explain changes to the most recent draft of BAL-003-1. The date and registration information will be announced as soon as the details are finalized. An initial ballot of BAL-003-1 will be conducted beginning on Tuesday, November 29, 2011 through 8 p.m. Eastern on Thursday, December 8, 2011.

Background
Frequency Response, a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load, is a critical component to the reliable operation of the bulk power system, particularly during disturbances and restoration. The proposed standard's intent is to collect data needed to accurately analyze existing Frequency Response, set a minimum Frequency Response obligation, provide a uniform calculation of Frequency Bias Settings that transition to values closer to Frequency Response, and encourage coordinated AGC operation. There is evidence of continuing decline in Frequency Response over the past 10 years, but no confirmed reason for the apparent decline. The proposed standard requires entities to provide data so that Frequency Response in each of the Interconnections can be analyzed, and the reasons for the decline in Frequency Response can be identified. Once Frequency Response has been analyzed and confirmed, requirements can be modified to maintain reliability.

Additional information is available on the project webpage.

A stakeholder interested in following the Frequency Response Standard Drafting Team's development of BAL-003-1 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail to: sarcomm@nerc.com. Please include the drafting team name in

your e-mail request.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

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

You have received this email because you are a registered representative in the Registered Ballot Body.

From: Monica Benson
To: monica.benson@nerc.net
Subject: NERC: Standards Announcement - Project 2007-12 Frequency Response | Ballot Pools, Formal Comment Period and Initial Ballot and Non-Binding Poll Information
Date: Tuesday, October 25, 2011 12:03:36 PM

Standards Announcement

Project 2007-12 Frequency Response

Ballot Pool Windows Now Open: Oct. 25 – Nov. 23, 2011
Formal Comment Period Open: Oct. 25 – Dec. 8, 2011
Initial Ballot and Non-Binding Poll Window: Nov. 29 – Dec. 8, 2011

Available Now

BAL-003-1 – Frequency Response and Frequency Bias Setting, an implementation plan and several additional associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Thursday, December 8, 2011. Ballot pools are being formed and the ballot pool windows are open through 8 a.m. Eastern on Wednesday, November 23.

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended March 7, 2011
- Frequency Response Standard Background Document – Provides an explanation of each of the proposed requirements; identifies how the proposed standard proposes to address FERC directives from Order 693; and on the last page provides an overview of the field trial (currently in Step 4)
- Attachment A – ERO's Process for assigning a Frequency Response Obligation and Frequency Bias Setting to each Balancing Authority
- Attachment B – ERO's Process for Adjusting Minimum Frequency Bias Setting
- FRS Form 1 (four versions - one for each of the four Interconnections) and FRS Form 2 (seven versions – two to collect data for Interconnections with a single Balancing Authority at two second and three second intervals; five to collect data for Interconnections with multiple Balancing Authorities at two second, three second, four second and five second intervals) – Both forms are proposed for the ERO's use (in conjunction with Attachment A) in determining each Interconnection's necessary amount of Frequency Response for allocation to Balancing Authorities. Instructions are now on the first page of each FRS Form 1 and FRS Form 2
- Mapping Document - Identifies each requirement in the already approved BAL-003-0.1b and identifies how that requirement has been treated in the revisions proposed in BAL-003-1.
- Unofficial comment form in Word format – This is for informal use when compiling

responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for BAL-003-1 and Associated VRFs/VSLs
Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of BAL-003-1, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with BAL-003-1. RBB members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pools to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)
The list server for the initial ballot is: bp-2007-12_Freq_Resp_in@nerc.com
Non-Binding Poll list server: bp-2007-12_NB_OCT2011_in@nerc.com

Instructions for Commenting
Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps
The drafting team is planning a webinar in November to explain changes to the most recent draft of BAL-003-1. The date and registration information will be announced as soon as the details are finalized. An initial ballot of BAL-003-1 will be conducted beginning on Tuesday, November 29, 2011 through 8 p.m. Eastern on Thursday, December 8, 2011.

Background
Frequency Response, a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load, is a critical component to the reliable operation of the bulk power system, particularly during disturbances and restoration. The proposed standard's intent is to collect data needed to accurately analyze existing Frequency Response, set a minimum Frequency Response obligation, provide a uniform calculation of Frequency Bias Settings that transition to values closer to Frequency Response, and encourage coordinated AGC operation. There is evidence of continuing decline in Frequency Response over the past 10 years, but no confirmed reason for the apparent decline. The proposed standard requires entities to provide data so that Frequency Response in each of the Interconnections can be analyzed, and the reasons for the decline in Frequency Response can be identified. Once Frequency Response has been analyzed and confirmed, requirements can be modified to maintain reliability.

Additional information is available on the project webpage.

A stakeholder interested in following the Frequency Response Standard Drafting Team's development of BAL-003-1 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail to: sarcomm@nerc.com. Please include the drafting team name in

your e-mail request.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

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

You have received this email because you are a registered representative in the Registered Ballot Body.

Discussion To Support The Development Of NPCC Industry Comments

For BAL-003-1 – Frequency Response and Frequency Bias Setting

Mike Potishnak

November 17, 2011

Introduction

Industry comments and initial balloting are due by December 8, 2001. As NPCC's representative on the Frequency Responsive Reserve Standard Drafting Team (FRSDT), perhaps sharing my perspectives on the development and merits of the version of BAL-003-1 under review may expedite the production of comments and balloting positions for the NPCC Balancing Authorities.

BAL-003-1 is the only standard being offered at this time in response to the Standard Authorization Request Form for Frequency Response. BAL-003-1 is applicable only to Balancing Authorities and Reserve Sharing Groups. A common concern that has been expressed in the industry is that the burden of compliance is being placed solely on Balancing Authorities while the main sources of discretional frequency response are generators. The next section of this document will address that concern.

The technical merits of BAL-003-1 of setting requirements for frequency response and frequency bias settings are discussed in the third section of this document. Implicit in this discussion is that requirements for Balancing Authorities to provide sufficient frequency response and have proper frequency bias settings in their AGC systems are necessary.

Summary recommendations concerning the support for this version of BAL-003-1 are provided in the final section of this document.

Requirements for Generators To Provide Frequency Response

The Standard Authorization Request Form (SAR) identifies the following entities to be within its scope: Reliability Authority, Balancing Authority, Generator Owner, Generator Operator, and Load-Serving Entity. However, the detailed description refers to generators only in item 6, which requires the collection of per generator performance data, but only when the Balancing Authority is deficient in meeting its Frequency Response Obligation.

While it is not clear whether the development of performance requirements for generators' governor response fits within this SAR, the FRSDT discussed such requirements at length during the development process. While sentiment was split, a key point made during the discussions was that innovative alternative sources for frequency response may be on the horizon. (ERCOT is already obtaining frequency response from loads.) And in the spirit of result-based standards, the Balancing Authority would have requirements for WHAT level of frequency response needs to be achieved, and they are free to determine HOW to achieve the targeted performance level. For example, ISOs that do not own generation may meet the requirement by placing the obligation solely on generation resources. However, a vertically integrated utility that owns generation and is also a Balancing Authority may seek alternative, more cost-effective methods than eliminating sliding pressure control in its conventional thermal generation fleet to restore governor response, given the heat rate improvements and dollars associated with sliding pressure control operation.

It has also been noted that ISOs not owning generation are subjected to compliance with CPS 1 and CPS 2 for regulation, and DCS for contingency reserve. So why should frequency response be any different? ISOs would need to find a

way to get adequate frequency response just as they have found ways to obtain adequate regulation and contingency reserve to be deployed.

In an attempt to find some middle ground, I have advocated the development of a generator governor response standard in which Balancing Authorities have the option of waiving the requirements to pursue the use of alternative resources. While discussions with WECC personnel indicated an interest in co-sponsorship of such a standard, no other NPCC Balancing Authority offered support during an informal TFCO discussion on the topic.

Technical Merits of BAL-003-1

Four documents will be discussed: the standard itself, its Attachments A and B, and its background document. The comments on each document will be sorted as either a "virtue" or a "vice".

BAL-003-1- Frequency Response and Frequency Bias Setting – **VIRTUES**

1. The 3 definitions offered are good, though the FRM definition should not refer to FORM 1.
2. An effective date for meeting the Frequency Response Obligation has a 2 year lead time.
3. Requirements R1 through R5 and their corresponding measures seem appropriate and clearly written.
4. The information in the compliance section seems reasonable.

BAL-003-1- Frequency Response and Frequency Bias Setting – **VICES**

1. The FRM definition should not refer to FORM 1.

2. The FRSDT should address the possibility for abuse by a Balancing Authority that is for the most part a generation only Balancing Authority, but they acquire a small amount of load to qualify under the first bullet of R5.
3. The violation severity levels for R1 seem to be reasonable. However, the technical writing needs to be enhanced for clarity.

BAL-003-1- Attachment A – **VIRTUES**

1. The event selection criteria are well-chosen.
2. The basic process for determining the Frequency Response Obligation is adequate.
3. The use of the median instead of the mean or linear aggression is the appropriate choice.
4. The standardized 18 to 52 second metric is appropriate for the Balancing Authorities of the Eastern Interconnection.

BAL-003-1- Attachment A – **VICES**

1. Criterion 5 needs to be re-written for clarity.
2. Criterion 7 refers to the "cleanest events". Perhaps a statement of what constitutes a "clean event" is needed to avoid possible controversy in the future.
3. The use of 59.6 Hz as the highest UFLS setting seems flawed. It should either be 59.7 Hz as a deliberate choice to protect Florida interests, or, it should be 59.5 Hz without concern for Florida's unique settings.
4. In the last 2 sentences at the end of the section on Frequency Response Obligation, it refers to an Interconnection being able to offer "alternate FRO protection criteria". It seems that the Interconnection should have been an integral part of establishing its obligation. Also, it states that the "ERO will confirm" the "alternate FRO protection criteria". Does this mean

the ERO unconditionally approves it, or evaluates with a right of rejection? Please clarify.

5. In the formula for determining the Balancing Authority's FRO allocation, installed capacity is used. Does the industry have a clear and consistent definition for installed capacity? Also, with greater wind energy development, the delivered capacity over longer time horizons will be substantially less than nameplate machine ratings. Also, the background document refers to the use of peak generation instead of installed capacity. Which shall be used? Please clarify.
6. Very recent studies have shown that the 18-52 second sampling interval does not work well for the Quebec Interconnection, in part due to the excellent and high level of response found in that Interconnection. The standard needs to be modified such that the sampling interval is that which works the best for each individual interconnection.
7. Attachment A needs to define the point A sampling interval.

BAL-003-1- Attachment B – **VIRTUES**

1. The process promotes better interconnected operations and has sufficient checks and balances to avoid an adverse reliability outcome.

BAL-003-1- Attachment B – **VICES**

1. None.

Frequency Response Standard Background Document – **VIRTUES**

1. This is a very useful document that should be maintained over time.

Frequency Response Standard Background Document – **VICES**

1. Cite Attachment B in addition to Attachment A in the discussion of requirement 1.
2. The Balancing Authority allocation method specified in this document does not agree with that in Attachment A.
3. Drop the speculation on page 4 that most Balancing Authorities will be compliant. While it may be a commonly held belief by many that there is adequate frequency response right now, that assessment should be made after a targeted level of reliability has been defined and approved. The same comment applies on page 12.
4. On page 6, drop the inappropriate recommendation of getting frequency response through supplemental regulation. It is inappropriate to try to substitute a "minute plus" product that is deployed centrally by the Balancing Authority for a "sub-minute" product that is deployed automatically without any Balancing Authority action. When a pseudo-tie is used, changes in the ACE values due to supplemental regulation are unrelated to and not coordinated with the need to deploy frequency response. Not only should this approach not be offered as an alternative, but the FRSDT should actively conduct research to determine if supplemental regulation via a pseudo-tie should be deliberately REMOVED from any actual net interchange calculation that may include it! This comment also applies to the mentioning of supplemental regulation on page 11 as well.
5. On page 7, the reference to a 24 hour window on each side of the frequency bias setting implementation date is inconsistent with the wording of the requirement. The requirement says that any time within the designated date is acceptable.
6. On page 8, the inclusion of "for training purposes" as a reason to not operate in tie line bias control should be dropped. This sort of training can be done in a training simulator. Alternatively, if it is determined that it should be supported, then the requirement needs to be reworded to allow it explicitly.

7. On page 14, the sentence: “This approach would only provide feedback for performance during that specific event and would not provide insight into the depth of response or other limitations” is difficult to understand. The paragraph would read better by simply dropping it.

Summary Of Recommendations

Of the 17 “vices” cited above, 13 of them are of a technical writing nature. The four substantive problems are:

- Using 59.6 Hz as an Eastern Interconnection UFLS instead of an actual value of either 59.5 Hz or 59.7 Hz
- Using installed capacity in determining the Frequency Response Obligation
- The sampling interval needs to be tuned on a per Interconnection basis to support HQTE’s characteristics
- Do not advocate the use of supplemental regulation as a method of procuring frequency response

I recommend supporting the standard, contingent upon resolving the above four substantive problems.

I recommend continuing to support the development of a governor response standard for generators that may be waived by Balancing Authorities at their option. Realistically, I do not believe that such a standard would be passed by the industry without such a waiver capability.

I do not recommend opposing BAL-003-1 solely because a governor response standard is not provided along with it at this time. FERC and NERC are committed to such a standard. If we do not work constructively to remove its present rough

edges, we may be forced to accept an inferior standard. Another risk is that FERC may impose its own standard should the industry fail to deliver, and that standard may be more onerous, noting the imposition of 1% of peak load level of governor response on Florida in a recent settlement.

Standard Development Roadmap

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

Development Steps Completed:

1. The Standards Committee approved the SAR for posting on January 13, 2005.
2. The SAR was posted for industry comment from January 17, 2005 through February 17, 2005.
3. Reply comments and a revised SAR were posted for a second industry comment period from April 4, 2006 through May 3, 2006.
4. Reply comments and a revised SAR were posted for a third industry comment period from February 8, 2007 through March 9, 2007.
5. Standards Committee approved moving the project into the standards development phase on July 12, 2007.
6. The Standards Committee appointed the Standard Drafting Team on August 13, 2007.
7. The draft standard was posted for a 30 day formal comment period from February 4, 2011 through March 7, 2011.

Proposed Action Plan and Description of Current Draft:

This is the second posting of the proposed standard and its associated documents for a 45 day formal comment period and a successive 10 day ballot, from October ~~21~~24, 2011through December ~~5~~7, 2011.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Respond to comments submitted within the comment period and with the successive ballot.	December, 2011
2. Conduct a recirculation ballot for ten days.	January, 2012
3. BOT adoption.	March, 2012

Definitions of Terms used in the Standard

~~**Single Event Frequency Response Data (SEFRD)**~~

~~The individual sample of event data from a Balancing Authority which represents the change in Net Actual Interchange (NI_A), divided by the change in frequency, expressed in MW/0.1Hz.~~

Frequency Response Measure (FRM)

The median of all the Frequency Response ~~Single Event Frequency Response Data~~ observations reported annually on FRS Form 1.

Frequency Response Obligation (FRO)

The Balancing Authority's share of the required Frequency Response ~~contribution to the total aggregate Frequency Response~~ needed for the reliable operation of an Interconnection ~~assigned by the ERO~~.

Frequency Bias Setting

A number~~value~~, ~~(~~either ~~a~~ fixed or variable ~~Frequency Bias)~~, usually expressed in MW/0.1 Hz, included in~~set into~~ a Balancing Authority's Area Control Error equation to account for~~that allows~~ the Balancing Authority's Frequency Response contribution ~~to contribute its Frequency Response~~ to the Interconnection, and discourage response withdrawal through secondary control systems.

A. Introduction

Title: Frequency Response and Frequency Bias Setting

Number: BAL-003-1

Purpose: To require sufficient Frequency Response from the Balancing Authority to maintain Interconnection Frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored. To ~~schedule and~~ provide consistent methods for measuring Frequency Response and determining the Frequency Bias Setting.

Applicability:

1.1. Balancing Authority

1.2. Reserve Sharing Group (where applicable)

Effective Date:

1.3. In those jurisdictions where regulatory approval is required, Requirements R2, R3 ~~and~~ R4 and R5 of this standard shall become effective the first calendar day of the first calendar quarter 12 months after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, Requirements R2, ~~and~~ R3, R4 and R5 of this standard shall become effective the first calendar day of the first calendar quarter 12 months after Board of Trustees adoption.

1.4. In those jurisdictions where regulatory approval is required, Requirements R1 of this standard shall become effective the first calendar day of the first calendar quarter 24 months after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, Requirements R1 of this standard shall become effective the first calendar day of the first calendar quarter 24 months after Board of Trustees adoption.

B. Requirements

R1. Each Balancing Authority (BA) or Reserve Sharing Group (RSG) shall achieve an annual Frequency Response Measure (FRM) (as detailed in Attachment A and calculated on FRS Form 1) that is equal to or more negative than its Frequency Response Obligation (FRO) to ensure that sufficient Frequency Response is provided by each BA or RSG to maintain an adequate level of Frequency Response in the Interconnection. *[Risk Factor: Medium][Time Horizon: Operations Assessment]*

~~**R1.**~~**R2.** Each Balancing Authority not participating in Overlap Regulation Service shall implement the Frequency Bias Setting (fixed or variable) validated~~provided~~ by the ERO, into its Area Control Error (ACE) calculation beginning on the date specified by the ERO to ensure effectively coordinated Tie Line Bias~~secondary~~ control~~, using the results from the calculation methodology detailed in Attachment A~~. *[Risk Factor: Medium][Time Horizon: Operations Planning]*

~~R2.~~R3. Each Balancing Authority not receiving Overlap Regulation Service shall operate its Automatic Generation Control (AGC) in~~on~~ Tie Line Bias mode to ensure effectively coordinated control, unless such operation would have an Adverse Reliability Impact on the Balancing Authority's Area. *[Risk Factor: Medium][Time Horizon: Real-time Operations]*

R4. Each Balancing Authority that is performing Overlap Regulation Service shall modify~~increase~~ its Frequency Bias Setting in its ACE calculation to be equivalent to the sum of ~~by combining~~ the Frequency Bias Settings of the participating Balancing Authorities as validated by the ERO or calculate the Frequency Bias Setting based on the entire area being combined and thereby represent the Frequency Response for the combined~~entire~~ area being controlled. *[Risk Factor: Medium][Time Horizon: Operations Planning]*

R5. In order to ensure adequate control response, each Balancing Authority shall use a monthly average Frequency Bias Setting whose absolute value is at least equal to one of the following: *[Risk Factor: Medium][Time Horizon: Operations Planning]*

- The minimum percentage of the Balancing Authority Area's estimated yearly Peak Demand within its metered boundary per 0.1 Hz change as specified by the ERO in accordance with Attachment B.
- The minimum percentage of the Balancing Authority Area's estimated yearly peak generation for a generation-only Balancing Authority, per 0.1 Hz change as specified by the ERO in accordance with Attachment B.

C. Measures

~~Measures for each Requirement will be provided in the second posting of the proposed standard.~~

M1. The Balancing Authority or Reserve Sharing Group shall have FRS Form 1 with data to show that its FRM is equal to or more negative than FRO to demonstrate compliance with Requirement R1.

M2. The Balancing Authority shall have evidence such as a dated document in hard copy or electronic format showing the ERO validated Frequency Bias Setting was entered into its ACE calculation on the date specified or other evidence to demonstrate compliance with Requirement R2.

M3. The Balancing Authority shall have evidence such as a dated operating log, database or list in hard copy or electronic format or operator interviews supported by other evidence showing the AGC operating mode including explanation when operating in other than Tie Line Bias mode to demonstrate compliance with Requirement R3.

M4. The Balancing Authority shall have evidence such as a dated operating log, database or list in hard copy or electronic format showing when Overlap Regulation Service is provided including Frequency Bias Setting calculation to demonstrate compliance with Requirement R4.

~~M1.~~M5. The Balancing Authority shall have evidence such as dated data plus documented formula to support the calculation retained in either hardcopy or electronic format showing the monthly average Frequency Bias Setting or other evidence to demonstrate compliance with Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

The Regional Entity is the Compliance Enforcement Authority except where the responsible entity works for the Regional Entity. Where the responsible entity works for the Regional Entity, the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity), to be responsible for compliance enforcement.~~Regional Entity shall serve as the Compliance Enforcement Authority.~~

1.2. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

Periodic Data Submittals

1.3. Data Retention

The Balancing Authority shall retain data or evidence to show compliance with Requirements R1, R2, R3, R4 and R5, Measures M1, M2, M3, M4, and M5 for the current year plus three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The Reserve Sharing Group shall retain data or evidence to show compliance with Requirement R1 and Measure M1 for the current year plus three calendar years unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Balancing Authority or Reserve Sharing Group is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the time period specified above, whichever is longer.

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

1.4. Additional Compliance Information

~~**R1 Supplemental Information**~~

~~Each Balancing Authority shall report its previous year's Frequency Response Measure (FRM) to the ERO on Form 1 by January 10 each year. If the ERO posts the official list of events after December 10, Balancing Authorities will be given 45 days from the date the ERO posts the official list of events to submit their FRS Form 1.~~

~~A Balancing Authority may elect to fulfill its Frequency Response Obligation by participating as a member of a Reserve Sharing Group (RSG). If a Balancing Authority elects to report as an RSG, the total of the participating Balancing Authorities' FRO will be compared to the total of the participating Balancing Authorities' FRM.~~

~~**R2 Supplemental Information.**~~

~~Each Balancing Authority shall report its current year requested Frequency Bias Setting and Frequency Bias type (fixed or variable) to the ERO on FRS Form 1 by January 10 each year. If the ERO posts the official list of events after December 10, Balancing Authorities will be given 45 days from the date NERC posts the official list of events to submit their FRS Form 1. Once the FRM and Frequency Bias Settings have been validated by the ERO, the ERO will disseminate the Frequency Bias Settings Report for all Balancing Authorities in each Interconnection along with the implementation date.~~

~~Balancing Authorities with variable Frequency Bias Settings shall calculate monthly average Frequency Bias Settings. The previous year's monthly averages will be reported annually on FRS Form 1.~~ For Interconnections that are also Balancing Authorities, Tie Line Bias control and Flat Frequency control are equivalent and either is acceptable.

2.0 Violation Severity Levels

R#	Lower VSL	Medium VSL	High VSL	Severe VSL
R1	The summation of the Balancing Authorities' FRM within an Interconnection was equal to or more negative than the Interconnection's FRO and the Balancing Authority's, or Reserve Sharing Groups, FRM was	The summation of the Balancing Authorities' FRM within an Interconnection was equal to or more negative than the Interconnection's FRO and the Balancing Authority's, or Reserve Sharing Groups, FRM was	The summation of the Balancing Authorities' FRM within an Interconnection did not meet its FRO and the Balancing Authority's, or Reserve Sharing Groups, FRM was less negative than its FRO by more than 1% but by at most	The summation of the Balancing Authorities' FRM within an Interconnection did not meet its FRO and the Balancing Authority's, or Reserve Sharing Groups, FRM was less negative than its FRO by more than 30% or by more

	less negative than its FRO by more than 1% but by at most 30% or 15 MW/0.1 Hz, whichever one is the greater deviation from its FRO	less negative than its FRO by more than 30% or by more than 15 MW/0.1 Hz, whichever is the greater deviation from its FRO	30% or 15 MW/0.1 Hz, whichever one is the greater deviation from its FRO	than 15 MW/0.1 Hz, whichever is the greater deviation from its FRO
R2	The Balancing Authority not receiving Overlap Regulation Service failed to implement the validated Frequency Bias Setting value into its ACE calculation on the date specified but did so within 5 calendar days following the date specified by the ERO.	The Balancing Authority not receiving Overlap Regulation Service implemented the validated Frequency Bias Setting value into its ACE calculation in more than 5 calendar days but less than or equal to 15 calendar days following the date specified by the ERO.	The Balancing Authority not receiving Overlap Regulation Service implemented the validated Frequency Bias Setting value into its ACE calculation in more than 15 calendar days but less than or equal to 25 calendar days following the date specified by the ERO.	The Balancing Authority not receiving Overlap Regulation Service did not implement the validated Frequency Bias Setting value into its ACE calculation in more than 25 calendar days following the date specified by the ERO.
R3	N/A	N/A	N/A	The Balancing Authority not receiving Overlap Regulation service failed to operate AGC in Tie Line Bias mode and such operation would not have had an Adverse Reliability Impact on the Balancing Authority's Area.
R4	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint	The Balancing Authority incorrectly changed the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services with combined footprint

	setting-error less than 5% of the correct value.	setting-error more than 5% but less than or equal to 15% of the correct value.	setting-error more than 15% but less than or equal to 25% of the correct value.	setting-error more than 25% of the correct value. OR The Balancing Authority failed to change the Frequency Bias Setting value used in its ACE calculation when providing Overlap Regulation Services.
R5	The absolute value of the Balancing Authorities' calculated monthly average Frequency Bias Setting was less than or equal to 5% below the minimum specified by the ERO.	The absolute value of the Balancing Authorities' calculated monthly average Frequency Bias Setting was more than 5% but less than or equal to 15% below the minimum specified by the ERO.	The absolute value of the Balancing Authorities' calculated monthly average Frequency Bias Setting was more than 15% but less than or equal to 25% below the minimum specified by the ERO.	The absolute value of the Balancing Authorities' calculated monthly average Frequency Bias Setting was more than 25% below the minimum specified by the ERO.

E. Regional Variance

None

F. Associated Documents

Attachment A - Frequency Response Standard Supporting Document~~Background Document~~

Attachment B – Process for Adjusting Bias Setting Floor

FRS Form 1

FRS Form 21 ~~Instructions~~

Frequency Response Standard Background Document

G. Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1		Complete Revision under Project 2007-12	Revision

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for BAL-003-1 – Frequency Response & Frequency Bias Setting Standard

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

BAL-003-0.1b ~~Requirements R1, R2, R3, R4 and R6~~ should be retired midnight of the day immediately prior to the Effective Date of~~when~~ BAL-003-1 in the Jurisdiction in which the new standard is becoming ~~becomes~~ effective.

~~BAL-003-0 Re1quirement R5 should be retired as outlined in the following table.~~

~~For those Balancing Authorities that serve native load:~~

- ~~May 2011 through December 2011 -0.8% of peak/0.1 Hz~~
- ~~January 2012 through December 2012 -0.6% of peak/0.1 Hz~~
- ~~January 2013 through December 2013 -0.4% of peak/0.1 Hz~~
- ~~January 2014 through December 2014 -0.2% of peak/0.1 Hz~~
- ~~January 2015 through -0.0% of peak/0.1 Hz~~

~~For those Balancing Authorities that do not serve native load:~~

- ~~May 2011 through December 2011 -0.8% of upcoming years maximum generation/0.1 Hz~~
- ~~January 2012 through December 2012 -0.6% of upcoming years maximum generation/0.1 Hz~~
- ~~January 2013 through December 2013 -0.4% of upcoming years maximum generation/0.1 Hz~~
- ~~January 2014 through December 2014 -0.2% of upcoming years maximum generation/0.1 Hz~~
- ~~January 2015 through -0.0% of upcoming years maximum generation/0.1 Hz~~

~~The FRR drafting team, NERC and the NERC Resources Subcommittee will observe the impact on frequency and will implement a reversion plan should frequency performance decline.~~

New or Modified Definitions

The following definitions shall become effective when BAL-003-1 Requirements R2, R3, R4 and R5 become effective:

116-390 Village Boulevard, Princeton, New Jersey 08540-5721
Phone: 609.452.8060 ▪ Fax: 609.452.9550 ▪ www.nerc.com

Frequency Response Measure (FRM): The median of all the Frequency Response observations reported annually on FRS Form 1.

Frequency Response Obligation (FRO): The Balancing Authority's share of the required Frequency Response needed for the reliable operation of an Interconnection.

Frequency Bias Setting: A number, either a fixed or variable, usually expressed in MW/0.1 Hz, included in a Balancing Authority's Area Control Error equation to account for the Balancing Authority's Frequency Response contribution to the Interconnection, and discourage response withdrawal through secondary control systems.

The existing definition of Frequency Bias Setting should be retired midnight of the day immediately prior to the Effective Date of BAL-003-1 in the Jurisdiction in which the new standard is becoming effective.

The proposed revised definition for "Frequency Bias Setting" is incorporated in the following NERC approved standards:

- BAL-001-0.1a Real Power Balancing Control Performance
- BAL-004-0 Time Error Correction
- BAL-004-1 Time Error Correction
- BAL-005-0.1b Automatic Generation Control

Compliance with Standards

Once this standard becomes effective, the responsible entities identified in the applicability section of the standard must comply with the requirements. These include:

- Balancing Authorities
- Reserve Sharing Groups

Proposed Effective Date

Compliance with BAL-003-1 shall be implemented over a two-year period, as follows:

- In those jurisdictions where regulatory approval is required, Requirements R2~~1~~, R3, R4 and R5~~4~~ of this standard shall become effective the first calendar day of the first calendar quarter 12 months after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, Requirements R2~~1~~, R3, R4 and R5~~4~~ of this standard shall become effective the first calendar day of the first calendar quarter 12 months after Board of Trustees adoption.
- In those jurisdictions where regulatory approval is required, Requirements R1~~2~~ of this standard shall become effective the first calendar day of the first calendar quarter 24 months after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, Requirements R1~~2~~ of this standard shall become effective the first calendar day of the first calendar quarter 24 months after Board of Trustees adoption.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title of Proposed Standard	Frequency Response
Request Date	11/25/06
Revised Date	06/30/07

SAR Requestor Information		**SAR Type** (Put an 'x' in front of one of these selections)	
Name	Terry Bilke	x	New Standard
Primary Contact	Terry Bilke	☐	Revision to existing Standard
Telephone	(317) 249-5463	☐	Withdrawal of existing Standard
Fax	(317) 249-5994		
E-mail	tbilke@midwestiso.org	☐	Urgent Action

Purpose/Industry Need

Frequency Response, a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load, is a critical component to the reliable operation of the bulk power system, particularly during disturbances and restoration. The proposed standard's intent is to collect data needed to accurately model existing Frequency Response. There is evidence of continuing decline in Frequency Response in the three Interconnections over the past 10 years, but no confirmed reason for the apparent decline. The proposed standard requires entities to provide data so that Frequency Response in each of the Interconnections can be modeled, and the reasons for the decline in Frequency Response can be identified. Once the reasons for the decline in Frequency Response are confirmed, requirements can be written to control Frequency Response to within defined reliability parameters.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies by double clicking the grey boxes.)*		
☒	Reliability Authority	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports interconnection frequency in real time
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation valid and balanced Interchange Schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >1year plan for the resource adequacy of its specific loads within a Planning Authority area.
☐	Transmission Planner	Develops a >1 year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator Area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☐	Transmission Owner	Owns and maintains transmission facilities
☐	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check boxes for all that apply by double clicking the grey boxes.)*	
☒	1. Interconnected bulk electric systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk electric systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk electric systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk electric systems.
☒	6. Personnel responsible for planning and operating interconnected bulk electric systems shall be trained, qualified and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk electric systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box by double clicking the grey area.)*
1. The planning and operation of bulk electric systems shall recognize that reliability is an essential requirement of a robust North American economy. Yes
2. An Organization Standard shall not give any market participant an unfair competitive advantage.Yes
3. An Organization Standard shall neither mandate nor prohibit any specific market structure. Yes
4. An Organization Standard shall not preclude market solutions to achieving compliance with that Standard. Yes
5. An Organization Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Detailed Description (Provide enough detail so that an independent entity familiar with the industry could draft, modify, or withdraw a Standard based on this description.)

The proposed technical/preparedness standard will require or provide the following:

1. Each Balancing Authority shall collect and provide data [scan rate tie deviation and frequency for up to 5* minutes per event] needed to model its sub-minute Frequency Response to loss of large generating units and load.

2. Each Balancing Authority shall report each loss of generation or load greater than the respective Interconnection reporting threshold to its Reliability Coordinator.

3. Each Reliability Coordinator will relay Frequency Response Standard (FRS) event information to other Reliability Coordinators in its Interconnection. The Interconnection Time Monitor will maintain a log of FRS events.

4. NERC will annually post a list of FRS events. These events will be used by Balancing Authorities to calculate and report their annual Frequency Response and Bias.

5. NERC, in conjunction with the respective Regions, will establish a Target Frequency Response for each Interconnection. Absent an agreement, the observed Frequency Response in the first year of the FRS will be used as a target.

6. Balancing Authorities with less than [75%]* of their share of Target Frequency Response shall provide generation-level data to their Region for use by Transmission Planners and Planning Coordinators.

    a. Each Generator Operator that operates a generator larger than [10 MW]*, shall provide data to its Balancing Authority, as required in item 6, to support this standard and for use in developing models of Frequency Response in the associated Interconnection.

    b. Load Serving Entities shall provide data, as required in item 6, to their BA and Region to support the standard.

*These values are representative and will be refined based on stakeholder input during the standard drafting phase.

Related Standards

Standard No.	Explanation
BAL-001-0 through BAL-006-0	Balancing Standards, version 0
Balance Resources and Demand draft standards	Balancing Resources and Demand BAL-007 through BAL-012 draft standards, are in standards development process

Related SARs

SAR ID	Explanation
Frequency Response SAR, version 0	Original Frequency Response SAR
MOD-027	Verification and Status of Generator Frequency Response. The proposed standard would provide a mechanism to validate compliance with MOD-027. The proposed standard could also provide a means to achieve MOD-027 (if the Balancing Authority implements on on-line measurement of generator frequency using SCADA data).

Regional Variances

Region	Explanation
ECAR	
ERCOT	Single Balancing Authority Interconnections calculate Frequency Response based on the change in generation (or load) rather than Tie-Line deviation (ERCOT).
FRCC	
MAAC	
MAIN	
MAPP	
NPCC	
SERC	
SPP	
WECC	

Related NERC Operating Policies or Planning Standards

ID	Explanation
MOD-013-0	The proposed standard would enable better input data to the modeling standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2007-12 Frequency Response

Ballot Pool Windows Now Open: Oct. 25 – Nov. 23, 2011
Formal Comment Period Open: Oct. 25 – Dec. 8, 2011
Initial Ballot and Non-Binding Poll Window: Nov. 29 – Dec. 8, 2011

Available Now

BAL-003-1 – Frequency Response and Frequency Bias Setting, an implementation plan and several additional associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Thursday, December 8, 2011. Ballot pools are being formed and the ballot pool windows are open through 8 a.m. Eastern on Wednesday, November 23.

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended March 7, 2011
- Frequency Response Standard Background Document – Provides an explanation of each of the proposed requirements; identifies how the proposed standard proposes to address FERC directives from Order 693; and on the last page provides an overview of the field trial (currently in Step 4)
- Attachment A – ERO's Process for assigning a Frequency Response Obligation and Frequency Bias Setting to each Balancing Authority
- Attachment B – ERO's Process for Adjusting Minimum Frequency Bias Setting
- FRS Form 1 (four versions - one for each of the four Interconnections) and FRS Form 2 (seven versions – two to collect data for Interconnections with a single Balancing Authority at two second and three second intervals; five to collect data for Interconnections with multiple Balancing Authorities at two second, three second, four second and five second intervals) – Both forms are proposed for the ERO's use (in conjunction with Attachment A) in determining each Interconnection's necessary amount of Frequency Response for allocation to Balancing Authorities. Instructions are now on the first page of each FRS Form 1 and FRS Form 2
- Mapping Document - Identifies each requirement in the already approved BAL-003-0.1b and identifies how that requirement has been treated in the revisions proposed in BAL-003-1.

- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for BAL-003-1 and Associated VRFs/VSLs

Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of BAL-003-1, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with BAL-003-1. RBB members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pool to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)
The list server for the initial ballot is: bp-2007-12_Freq_Resp_in@nerc.com
Non-Binding Poll list server: bp-2007-12_NB_OCT2011_in@nerc.com

Instructions for Commenting

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

The drafting team is planning a webinar in November to explain changes to the most recent draft of BAL-003-1. The date and registration information will be announced as soon as the details are finalized. An initial ballot of BAL-003-1 will be conducted beginning on Tuesday, November 29, 2011 through 8 p.m. Eastern on Thursday, December 8, 2011.

Background

Frequency Response, a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load, is a critical component to the reliable operation of the bulk power system, particularly during disturbances and restoration. The proposed standard's intent is to collect data needed to accurately analyze existing Frequency Response, set a minimum Frequency Response obligation, provide a uniform calculation of Frequency Bias Settings that transition to values closer to Frequency Response, and encourage coordinated AGC operation. There is evidence of continuing decline in Frequency Response over the past 10 years, but no confirmed reason for the apparent decline. The proposed standard requires entities to provide data so that Frequency Response in each of the Interconnections can be analyzed, and the

reasons for the decline in Frequency Response can be identified. Once Frequency Response has been analyzed and confirmed, requirements can be modified to maintain reliability.

Additional information is available on the project webpage.

A stakeholder interested in following the Frequency Response Standard Drafting Team's development of BAL-003-1 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail to: sarcomm@nerc.com. Please include the drafting team name in your e-mail request.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Standard Development Timeline

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

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)

Proposed Action Plan and Description of Current Draft

This is the ~~first~~third posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a ~~30~~45-day formal comment period concurrent with the formation of the ballot pool and the initial ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes~~, and proceed to~~ on second ~~comment~~posting	April - October ~~2010 – February~~ 2011
~~Second Comment Period~~	~~March – May 2011~~
Third Comment/Ballot period	~~June - July~~November-December 2011
Recirculation Ballot period	~~July - August~~December 2011
Receive BOT approval	~~September 2011~~February 2012

Effective Dates

~~1. The standard~~EOP-004-2 shall become effective on the first ~~calendar~~ day of the third calendar quarter after ~~the date of the order providing~~ applicable regulatory approval.

~~2.~~ In those jurisdictions where no regulatory approval is required, ~~the~~this standard shall become effective on the first ~~calendar~~ day of the third calendar quarter after Board of Trustees ~~adoption~~approval.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-~~1~~2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-~~1a~~2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.~~–~~ Retire CIP-008-4, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

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

~~**Impact Event: Any event which has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.**~~

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: ~~Impact~~ Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of ~~Impact Events~~events with the potential to impact reliability and their causes, if known, by the Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall mean:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange ~~Authority~~Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Distribution Provider

4.1.10. ~~4.1.10~~ Load Serving Entity

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

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

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

The development ~~may include~~included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards ~~(see tables for each standard at the end of this SAR for more detailed information).~~.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. ~~A "concepts paper" was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.~~

~~The~~
The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the ~~SDR~~DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the ~~SDR~~DSR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

~~The DSR SDT has used a working definition for "Impact Events" to develop Attachment 1 as follows:~~

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

~~The DSR SDT has proposed this definition for~~

Summary of Key Concepts

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

- Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion ~~in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT~~ of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage~~" and~~". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was ~~that of~~ sabotage or ~~merely~~ vandalism without the intervention of law enforcement~~ after the fact. This will~~. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard~~ and therefore it is inappropriate to attempt to define it.~~. The ~~Impact Events~~events listed in Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. ~~Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.~~

~~To support this concept, the~~ The types of events that are required to be reported are contained within Attachment 1. The DSR SDT has ~~provided specific event for reporting including types of Impact~~coordinated with the NERC Events ~~and timing thresholds pertaining to~~ Analysis Working Group to develop the ~~different types of Impact Events and who's responsibility for reporting~~list of events that are to be reported under ~~the different Impact Events. This information is outlined in Attachment 1 to the proposed~~ this standard. Attachment 1, Part A pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. Attachment 1, Part B covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed ~~changes do~~Standard does not include any real-time operating notifications for the ~~types of~~ events ~~covered by CIP-001, EOP-004. This~~listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. ~~TOP~~the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

~~The DSR SDT is proposing to consolidate disturbance and Impact Event reporting under a single standard. These two components and other key concepts are discussed in the following sections.~~

~~**Summary of Concepts**~~

- ~~A single form to report disturbances and Impact Events that threaten the reliability of the bulk electric system~~
- ~~Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements~~
- ~~Clear criteria for reporting~~
- ~~Consistent reporting timelines~~
- ~~Clarity around of who will receive the information and how it will be used~~

Data Gathering

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

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting ~~Impact Events.~~events. Certain outages, such as those due to vandalism and terrorism, ~~are~~may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those ~~Impact Events~~events which have the potential ~~of~~to impact a wider area ~~affect upon the industry which~~of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading ~~involving Impact Events.~~events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

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

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

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

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

Coordination of Local and State Law Enforcement Agencies with the FBI

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

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

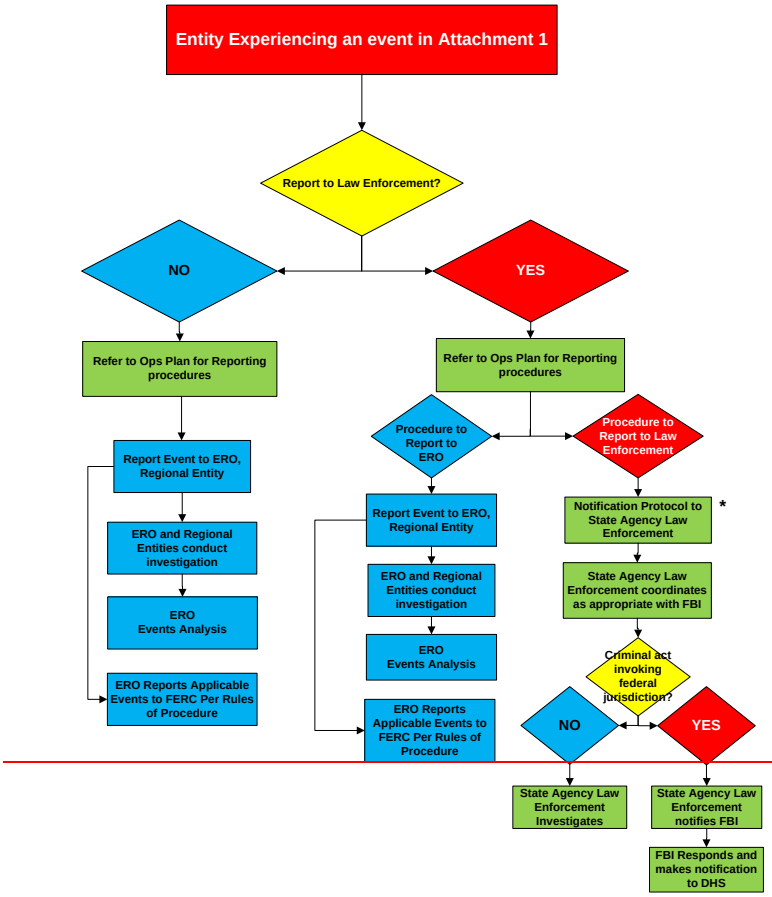
A similar law ~~enforecment~~enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the ~~Royla~~Royal Canadian Mounted Police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

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for ~~Impact Event EOP-004-2~~Reportable Events). Essentially, reporting an ~~Impact Event~~event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with ~~local~~ law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and

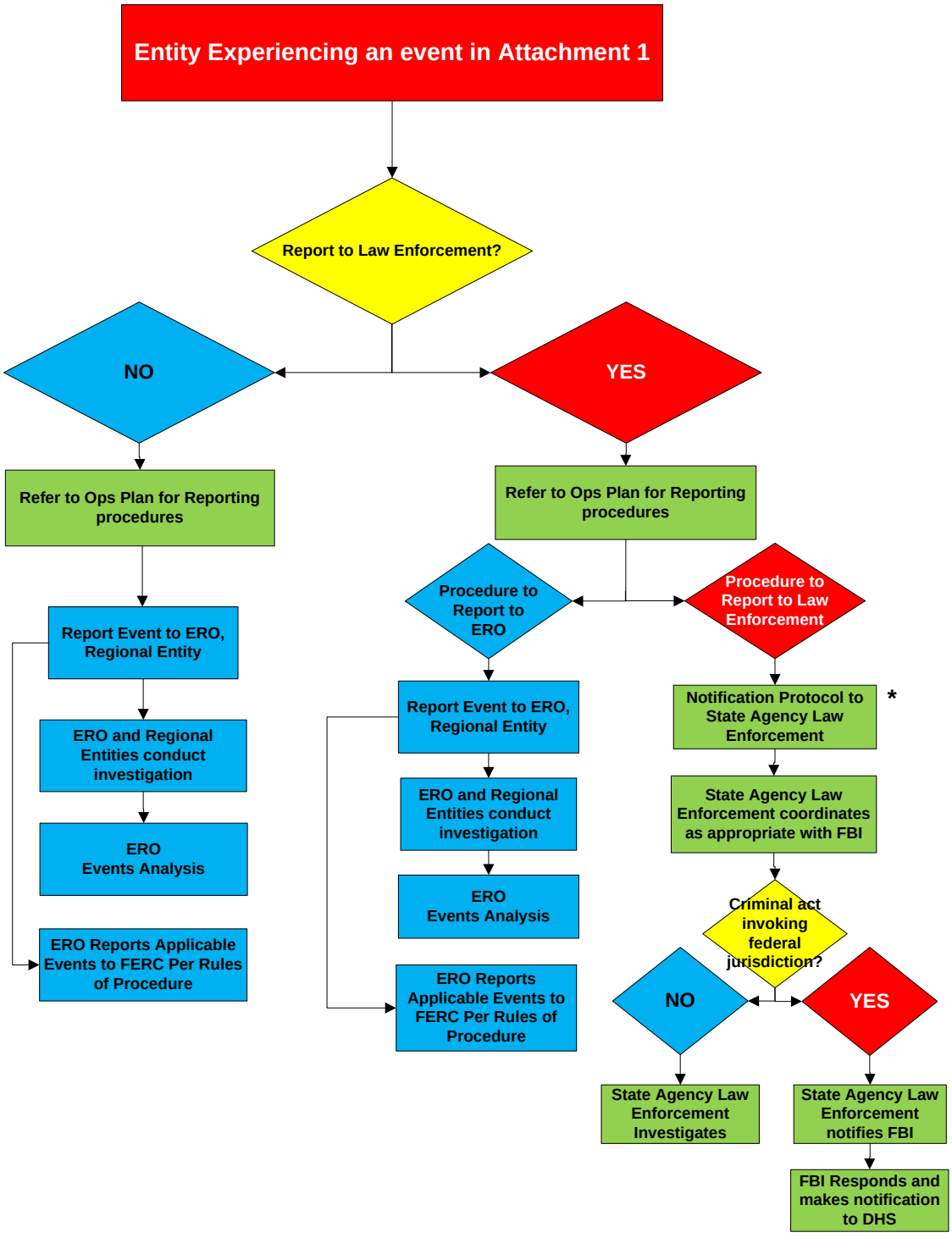
investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierarchy for Reportable Events



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

Reporting Hierarchy for Reportable Events



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

B. Requirements and Measures

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

1.1. ~~An Operating Process~~A process for identifying ~~Impact Events~~events listed in Attachment 1.

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

1.3. ~~An Operating Process~~A process for communicating ~~recognized Impact Events~~ events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel ~~notification(s).~~
- ~~External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC,~~ The Responsible ~~Entities'~~Entity's Regional Entity~~,~~
- Law ~~Enforcement, and~~ enforcement
- Governmental or ~~Provincial Agencies.~~provincial agencies

1.4. Provision(s) for updating the ~~Impact Event~~ Operating Plan within 90 calendar days of any change ~~to its content.~~ in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

~~1.4.~~

~~Rationale for R1~~

~~Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.~~

~~For the Impact Event Operating Plan, the DSR SDT envisions that Part 1.2 includes performing sufficient analysis and information gathering to be able to complete the report for reportable Impact Events. The main issue is to make sure an entity can a) identify when an Impact Event has occurred and b) be able to gather enough information to complete the report.~~

~~Part 1.3 could include a process flowchart, identification of internal positions to be notified and to make notifications, or a list of personnel by name as well as telephone numbers.~~

~~The Impact Event Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.~~

M1. Each Responsible Entity ~~shall~~will provide the current, dated, in force ~~Impact Event~~ Operating Plan ~~to the Compliance Enforcement Authority~~which includes Parts 1.1 - 1.5 as requested.

R2. Each Responsible Entity shall implement the parts of its ~~Impact Event~~ Operating Plan ~~documented in~~that meet Requirement R1~~ for Impact Events listed in Attachment 1 (~~, Parts ~~A~~1.1 and ~~B).~~1.2 for an actual event and Parts 1.4 and 1.5 as specified. *[Violation Risk~~:~~ Factor: Medium] [Time Horizon: ~~Real-time~~ Operations ~~and Same-day Operations]~~Assessment]*.

M2. ~~To the extent that an~~ Responsible ~~Entity has an Impact Event on its Facilities, the Responsible Entity~~Entities shall ~~documentation of~~ provide evidence that it implemented the ~~implementation~~parts of its ~~Impact Event~~ Operating ~~Plans. Such evidence could~~Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts, 1.4 and 1.5 as specified. Evidence may include, but is not limited to, an event report form (Attachment 2) or the OE-417 report submitted, operator logs, voice recordings, or ~~other notations and documents retained by the Registered Entity for each Impact Event.~~ dated documentation of review and update of the Operating Plan. (R2)

Rationale for R2
Each Responsible Entity must implement the various parts of Requirement R1. Parts 1.1 and 1.2 call for identifying and gathering information for actual events. Parts 1.4 and 1.5 require updating and reviewing the Operating Plan.

R3. Each Responsible Entity shall ~~conduct a test of~~ report events in accordance with its Operating ~~Process~~Plan developed to address the events listed in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*.

M3. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported. (R3)

~~Rationale for R3~~
~~The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized Impact Events is correct so that the entity can respond appropriately in the case of an actual Impact Event. The Responsible Entity may conduct a drill or exercise of its Operating Process for communicating recognized Impact Events as often as it desires but the time period between such drill or exercise can be no longer than 15 months from the previous drill/exercise or actual Impact Event (i.e., if you conducted an exercise/drill/actual employment of the Operating Process in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year)). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.~~

R4. Each Responsible Entity shall verify (through actual implementation for ~~communicating recognized Impact~~

R
E ing
P
e tual
e or
e g
e veen
te n the
p
c e
Operating Plan in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.
Evidence showing that an entity used the communication process in its Operating Plan for an actual event qualifies as evidence to meet this requirement.

~~Events~~an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement ~~R1~~1, Part 1.3, at least annually~~, (once per calendar year),~~ with no more than 15 calendar months between ~~tests.~~verification or actual implementation. *[Violation Risk~~:~~ Factor: Medium] [Time Horizon: ~~Long-term~~Operations Planning]*

~~**M3.** In the absence of an actual Impact Event, the~~**M4.** The Responsible Entity shall provide evidence that it ~~conducted a mock Impact Event and followed~~verified the communication process in its Operating ~~Process~~Plan for ~~communicating recognized Impact Events~~events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill or exercise may be used as evidence to meet this requirement. The time period between an actual ~~and~~event or ~~mock Impact Events~~verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation~~.~~ of a verification. (R3)

~~**R4.** Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning].*~~

~~**M4.** Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present and when internal personnel were trained on the responsibilities in the plan.~~

~~**R5.** Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. *[Violation Risk: Factor: Medium] [Time Horizon: Real-time Operations and Same-day Operations].*~~

~~**M5.** Responsible Entities shall provide evidence demonstrating the submission of reports using the plan created pursuant to Requirement R1 and Attachment 1 using either the form in Attachment 2 or the DOE OE-417 report. Such evidence will include a copy of the Attachment 2 form or OE-417 report submitted, evidence to support the type of Impact Event experienced; the date and time of the Impact Event; as well as evidence of report submittal that includes date and time.~~

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~;~~ or

~~**Compliance Monitoring and Enforcement Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

Third-party monitor without vested interest in the outcome for the ERO

.

1.2 Evidence Retention

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

Each Responsible Entity shall retain the current, in force document plus the 'dated revision history' from each version issued since the last audit for 3 calendar years for Requirement R1 and Measure M1.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3, R4, and Measures M2, M3, M4.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

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

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

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	~~Medium~~Lower	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an ~~Impact Event~~ Operating Plan but failed to include one of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has ~~a Impact Event~~an Operating Plan but failed to include two of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an ~~Impact Event~~ Operating Plan but failed to include three of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to include ~~all~~four or more of Parts 1.1 through 1.~~4~~5.
~~**R2**~~	~~Real-time Operations and Same-day~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity failed to implement its Impact Event Operating Plan~~

	~~Operations~~					~~for an Impact Event listed in Attachment 1.~~
~~R3~~R2	~~Long-term Planning~~Real-time Operations and Same-day Operations	Medium	1.1: N/A 1.2: N/A 1.4: The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to ~~conduct a test of its~~ update the Operating ~~Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 in~~Plan more than	1.1: N/A 1.2: N/A 1.4: The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to ~~conduct a test of its~~ update the Operating ~~Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3in~~Plan more than	1.1: N/A 1.2: N/A 1.4: The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to ~~conduct a test of its~~ update the Operating ~~Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 in~~Plan more than	1.1: The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to ~~conduct a test of its~~ implement the process for identifying events. 1.2: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			90 days of a change, but not more than 100 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 15 calendar months ~~but less~~after its previous review, but not more than 18 calendar months~~.~~ after its previous review.	100 days of a change, but not more than 110 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 18 calendar months ~~but less~~after its previous review, but not more than 21 calendar months after its previous review.	110 days of a change, but not more than 120 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 21 calendar months ~~but less~~after its previous review, but not more than 24 calendar months after its previous review.	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for gathering information for Attachment 2. 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating ~~Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 in~~Plan more than 120 days of a change.

						1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 24 calendar months after its previous review.
~~**R4**~~	~~Long-term Planning~~	~~Medium~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan l in more than 15 months but less than 18 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 months but less than 21 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 months but less than 24 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 24 months~~
~~**R5**~~**R3**	Real-time	Medium	The	The	The	The ~~Responsible~~

	Operations and Same-day Operations		~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~more than 24 hours but less than or equal to 36 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1.	~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than 36 hours but less than or equal to 48 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner,	~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than 48 hours but less than or equal to 60 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider,	~~Entity failed to submit a report in~~ Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 60 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner,

				Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in Attachment 1.	Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report in more than ~~1 hour~~2 hours but less than ~~2~~3 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 1 hour in Attachment 1.	Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than ~~2~~3 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 1 hour in Attachment 1. OR The ~~responsible entity~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to submit a report for an ~~Impact Event~~event in Attachment 1.

R4	Operations Planning	Medium	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 15 calendar months after its previous test, but not more than 18 calendar months after its previous test. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider,	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 18 calendar months after its previous test, but not more than 21 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 21 calendar months after its previous test, but not more than 24 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 24 calendar months after its previous test. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			~~Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan within the calendar year.~~			~~Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan.~~

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: ~~Impact~~ Events Table

NOTE: Under certain adverse conditions~~,~~ (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an ~~Impact Event~~event and issue a written ~~Impact~~ Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify ~~its Regional Entity(ies) and NERC, (e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422)~~parties per R1 and provide as much information as is available~~.~~ at the time of the notification. The affected Responsible Entity shall ~~then~~ provide periodic verbal updates until adequate information is available to issue a written ~~Impact~~ Event report.

~~EOP-004 — Attachment 1 – Actual Reliability Impact – Part A~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~Energy Emergency requiring Public appeal for load reduction~~	~~Initiating entity is responsible for reporting~~	~~Each public appeal for load reduction~~	~~Within 1 hour of issuing a public appeal~~
~~Energy Emergency requiring system-wide voltage reduction~~	~~Initiating entity is responsible for reporting~~	~~System-wide voltage reduction of 3% or more~~	~~Within 1 hour after event is initiated~~
~~Energy Emergency requiring manual firm load shedding~~	~~Initiating entity is responsible for reporting~~	~~Manual firm load shedding ≥ 100 MW~~	~~Within 1 hour after event is initiated~~
~~Energy Emergency resulting in automatic firm load shedding~~	~~Each DP or TOP that experiences the Impact Event~~	~~Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)~~	~~Within 1 hour after event is initiated~~
~~Voltage Deviations on BES Facilities~~	~~Each RC, TOP, GOP that experiences the Impact Event~~	~~± 10% sustained for ≥ 15 continuous minutes~~	~~Within 24 hours after 15 minute threshold~~
~~IROL Violation~~	~~Each RC, TOP that experiences the Impact Event~~	~~Operate outside the IROL for time greater than IROL Tv~~	~~Within 24 hours after Tv threshold~~
~~Loss of Firm load for ≥ 15 Minutes~~	~~Each RC, BA, TOP, DP that experiences the Impact Event~~	~~• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW~~ ~~• ≥ 200 MW for all other entities~~	~~Within 1 hour after 15 minute threshold~~
~~System Separation~~	~~Each RC, BA, TOP, DP that~~	~~Each separation resulting in an island of~~	~~Within 1 hour after occurrence is~~

~~EOP-004 – Attachment 1 – Actual Reliability Impact – Part A~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~(Islanding)~~	~~experiences the Impact Event~~	~~generation and load ≥ 100 MW~~	~~identified~~
~~Generation loss~~	~~Each RC, BA, GOP that experiences the Impact Event~~	~~• ≥ 2,000 MW for entities in the Eastern or Western Interconnection~~ ~~• ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection~~	~~Within 24 hours after occurrence~~
~~Loss of Off-site power to a nuclear generating plant (grid supply)~~	~~Each RC, BA, TO, TOP, GO, GOP that experiences the Impact Event~~	~~Affecting a nuclear generating station per the Nuclear Plant Interface Requirement~~	~~Report within 24 hours after occurrence~~
~~Transmission loss~~	~~Each RC, TOP that experiences the Impact Event~~	~~Three or more BES Transmission Elements~~	~~Within 24 hours after occurrence~~
~~Damage or destruction of BES equipment[1]~~	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the Impact Event~~	~~Through operational error, equipment failure, external cause, or intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~
~~Damage or destruction of Critical Asset~~	~~Applicable Entities under CIP-002 or its successor.~~	~~Through operational error, equipment failure, external cause, or intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~
~~Damage or destruction of a Critical Cyber Asset~~	~~Applicable Entities under CIP-002 or its successor.~~	~~Through intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~

~~[1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action; or iv) Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying inoperative.~~

~~EOP-004 – Attachment 1 – Potential Reliability Impact – Part B~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~Unplanned Control Center evacuation~~	~~Each RC, BA, TOP that experiences the potential Impact Event~~	~~Unplanned evacuation from BES control center facility~~	~~Report within 24 hour after occurrence~~
~~Fuel supply emergency~~	~~Each RC, BA, GO, GOP that experiences the potential Impact Event~~	~~Affecting BES reliability[2]~~	~~Report within 1 hour after occurrence~~
~~Loss of all monitoring or voice communication capability~~	~~Each RC, BA, TOP that experiences the potential Impact Event~~	~~Affecting a BES control center for ≥ 30 continuous minutes~~	~~Report within 24 hours after occurrence~~
~~Forced intrusion[3]~~	~~Each RC, BA, TO, TOP, GO, GOP that experiences the potential Impact Event~~	~~At a BES facility~~	~~Report within 1 hour after verification of intrusion~~

~~[2] Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.~~

~~[3] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).~~

~~Risk to BES equipment~~[4]	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event~~	~~From a non-environmental physical threat~~	~~Report within 1 hour after identification~~
~~Detection of a reportable Cyber Security Incident.~~	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event~~	~~That meets the criteria in CIP-008 (or its successor)~~	~~Report within 1 hour after detection~~

~~[4] Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment).~~

~~EOP-004 - Attachment 2: Impact Event Reporting Form~~

~~This form is to be used to report Impact Events~~ Reports to the ERO~~. NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports~~ should be submitted ~~via~~to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

~~Attachment 1 – Reportable Events~~				
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~	
~~Task~~		~~Comments~~		
~~1.~~ Destruction of BES equipment[5]	~~Entity filing the report (include company name and Compliance Registration ID number):~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the destruction of BES equipment	~~-~~Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
~~2.~~ Damage or destruction of Critical Asset per	Applicable Entities under CIP-002	Initial indication the event was due to operational error, equipment failure, external	~~Date and Time of Impact Event.~~	

[5] BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:	
Task		Comments		
CIP-002		cause, or intentional or unintentional human action.	Date: (mm/dd/yyyy) Time/Zone:The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
3. Damage or destruction of a Critical Cyber Asset per CIP-002	Applicable Entities under CIP-002.	Through intentional or unintentional human action.	Name of contact person: Email address: Telephone Number:The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
4. Forced intrusion[6]	Did the actual or potential Impact Event originate in your system?Each RC, BA, TO, TOP, GO, GOP that experiences the forced intrusion	Actual Impact Event ☐ Potential Impact Event ☐ Yes ☐ No☐ Unknown ☐At a BES facility	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	

[6] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

~~Attachment 1 – Reportable Events~~				
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~	
~~Task~~		~~Comments~~		
~~5.~~ Risk to BES equipment[7]	~~Under which NERC function are you reporting? (RC, TOP, BA, other)~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the risk to BES equipment	From a non-environmental physical threat	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
~~6.~~ Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP, ERO or RE that experiences the Cyber Security Incident	That meets the criteria in CIP-008	~~Brief Description of actual or potential Impact Event:~~ ~~(More detail should be provided in the Sequence of Events section below.)~~The parties identified pursuant to R1.3 within 1 hour of recognition of event.	

[7] Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:	
	Task	Comments		
7.	Generation tripped off-line*. MW Total List units tripped			
8. BES Emergency requiring public appeal for load reduction	Deficient entity is responsible for reporting	Each public appeal for load reduction	Frequency*. Just prior to Impact Event (Hz): Immediately after Impact Event (Hz max): Immediately after Impact Event (Hz min):The parties identified pursuant to R1.3 within 24 hours of recognition of the event.	
9. BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out*. (SpecifySystem wide voltage levelreduction of each facility listed).3% or	-The parties identified pursuant to R.1.3 within 24 hours of recognition of the event.	

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~
~~Task~~		~~Comments~~	
		~~more~~	
~~10.~~ BES Emergency requiring manual firm load shedding	~~Demand tripped (MW)*:~~ ~~Number of affected customers*:~~ ~~Demand lost (MW-Minutes)*:~~Initiating entity is responsible for reporting	FIRM~~Manual firm load shedding ≥ 100 MW~~	~~INTERRUPTIBLE~~The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
~~11.~~			
~~12.~~			
~~13.~~			

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~

	~~Task~~	~~Comments~~	
~~14.~~	~~Restoration Time*.~~	~~INITIAL~~	~~FINAL~~
	~~Transmission:~~		
	~~Generation:~~		
	~~Demand:~~		

~~15.~~ BES Emergency resulting in automatic firm load shedding	~~Each DP or TOP that experiences the automatic load shedding~~	~~Sequence of Events of actual or potential Impact Event (if potential Impact Event, please describe your assessment of potential impact to BES) :~~	~~The parties identified pursuant to R1.3 within 24 hours of recognition of the event.~~

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:
Task		Comments	
		Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	
Voltage deviations on BES Facilities	Each TOP that experiences the voltage deviation	± 10% sustained for ≥ 15 continuous minutes	The parties identified pursuant to R1.3 within 24 hours after 15 minutes of exceeding the threshold.
16. IROL Violation (all Interconnections) or SOL Violation (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation (WECC only)	Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report: Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for	The parties identified pursuant to R1.3 within 24 hours after exceeding the Tv threshold.

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~
~~Task~~		~~Comments~~	
		a time greater than the SOL Tv (WECC only).	
~~Loss of Firm load for ≥ 15 Minutes~~	~~Each BA, TOP, DP that experiences the loss of firm load~~	~~• ≥ 300 MW for entities with demand ≥ 3000 MW~~ ~~• ≥ 200 MW for all other entities~~	~~The parties identified pursuant to R1.3 the entity's within 24 hours exceeding the 15 minute threshold~~
~~17. System Separation (Islanding)~~	~~Identify any protection system misoperation(s)[8]:~~ Each RC, BA, TOP, DP that experiences the system separation	~~Each separation resulting in an island of generation and load ≥ 100 MW~~	~~The parties identified pursuant to R1.3 within 24 hours after occurrence is identified~~
~~Generation loss~~	~~Each BA, GOP that experiences the generation loss~~	~~• ≥ 2,000 MW for entities in the Eastern or Western Interconnection~~ ~~• ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection~~	~~The parties identified pursuant to R1.3within 24 hours after occurrence.~~
~~Loss of Off-site~~	~~Each TO, TOP that~~	~~Affecting a nuclear~~	~~The parties identified pursuant to R1.3 within 24 hours after~~

[8] ~~Only applicable if it is part of the impact event the responsible entity is reporting on~~

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~
~~Task~~		~~Comments~~	
~~power to a nuclear generating plant (grid supply)~~	~~experiences the loss of off-site power to a nuclear generating plant~~	~~generating station per the Nuclear Plant Interface Requirement~~	~~occurrence~~
~~Transmission loss~~	~~Each TOP that experiences the transmission loss~~	~~Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)~~	~~The parties identified pursuant to R1.3 within 24 hours after occurrence~~
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential event	Unplanned evacuation from BES control center facility	The parties identified pursuant to R1.3 within 24 hours of recognition of event.
~~18.~~ Loss of monitoring or all voice communication capability	~~Additional Information~~Each RC, BA, TOP that ~~helps to further explain~~ experiences the ~~actual~~ loss of monitoring or ~~potential Impact Event if needed.~~ all voice communication	Voice Communications: Affecting a BES control center for ≥ 30 continuous minutes Monitoring: Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency Analysis) are rendered inoperable.	The parties identified pursuant to R1.3 within 24 hours of recognition of event.

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~
~~Task~~		~~Comments~~	
	capability		

EOP-004 - Attachment 2: Event Reporting Form

EOP-004, Attachment 2: Event Reporting Form This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the actual or potential event originate in your system?	Actual event ☐ Potential event ☐ Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ public appeal ☐ voltage reduction ☐ manual firm load shedding ☐ firm load shedding(undervoltage, underfrequency, SPS/RAS) ☐ voltage deviation ☐ IROL violation	Written description (optional unless Other is checked):

EOP-004, Attachment 2: Event Reporting Form

This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

Task		Comments
	☐ loss of firm load ☐ system separation(islanding) ☐ generation loss ☐ loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of BES equipment ☐ damage or destruction of Critical Asset ☐ damage or destruction of Critical Cyber Asset ☐ unplanned control center evacuation ☐ fuel supply emergency ☐ loss of all monitoring or voice communication capability ☐ forced intrusion Risk to BES equipment ☐ reportable Cyber Security Incident ☐ other	

Guideline and Technical Basis

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

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and ~~is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.~~has developed updated standards based on the SAR.

The standards listed under the SAR are:

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

~~The DSR SDT also proposed to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security – Order 706 SDT (Project 2008-06).~~

~~The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.~~

~~This concept paper provides stakeholders with a proposed "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.~~

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

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

Summary of Concepts and Assumptions:

The Standard ~~***Will:*** Require use~~***:***

- Requires reporting of ~~a single form to report disturbances and "Impact Events~~"events" that ~~threaten~~impact or may impact the reliability of the bulk electric system
- ~~Provide~~Provides clear criteria for reporting
- ~~Include~~Includes consistent reporting timelines
- ~~Identify~~Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- ~~Provide~~Provides clarity around of who will receive the information

~~The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements~~

Discussion of Disturbance Reporting

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

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

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

Discussion of ~~"Impact~~ Event~~"~~ Reporting

There are situations worthy of reporting because they have the potential to impact reliability. ~~The DSR SDT proposes calling such incidents 'Impact Events' with the following concept:~~

> ~~An Impact Event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.~~

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

Examples of ~~Impact Events~~such events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation

- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?

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

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

~~The DST SDT discussed the reliability needs for Impact Event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.~~

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

Potential Uses of Reportable Information

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

Collection of Reportable Information or "One stop shopping"

~~The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate.~~

~~Specific reporting forms[9] that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form, or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for industry awareness. Applicability of the standard will be determined based on the specific requirements.~~

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

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

~~[9] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.~~

Unofficial Comment Form

Disturbance and Sabotage Reporting (Project 2009-01)

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the first formal posting for Project 2009-01—Disturbance and Sabotage Reporting. The electronic comment form must be completed by **December 12, 2011.**

2009-01 Project Page

If you have questions please contact Stephen Crutchfield at stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

Background

The DST SDT posted the draft standard EOP-004-2 for a formal comment period from March 9, 2011 through April 8, 2011. Based on stakeholder feedback, the DSR SDT made several revisions to the standard to improve clarity and address other concerns identified by stakeholders. The main stakeholder concerns were addressed as follows:

Definition of Impact Event. Many stakeholders disagreed with the need for the definition of "Impact Event" and felt that that the definition was ambiguous and created confusion. The DSR SDT agrees and has deleted the proposed definition from the standard. The list of events that are to be reported in Attachment 1 is inclusive and no further attempts to define "Impact Event" are necessary.

Timeframe for Reporting and Event. Many stakeholders raised concerns with the one-hour reporting requirement for certain types of events. The commenters believed that the restoration of service or the return to a stable bulk power system state may be jeopardized by having to report certain events within one hour. The DSR SDT agreed and revised the reporting time to 24 hours for most events, with the exception of damage to or destruction of BES equipment, forced intrusion or cyber related incidents.

VRFs. Many stakeholders suggested that the reporting of events after the fact only justified a VRF of "lower" for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment A. This is procedural in nature and justifies a "lower" VRF, as this requirement deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis of reported events is addressed through the NERC Events Analysis Program in accordance with the NERC Rules of Procedure.

The three remaining requirements in EOP-004-2 require entities affected by events to report those events based on the specifics in Attachment A (Requirement R3) and to test the communications protocol of their Operating Plan once per year (R4). Requirement R2 provides for implementation of the Operating Plan as it relates to Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 specifies that an entity is responsible for reporting events to the appropriate entities in accordance with the Operating Plan based on Attachment A. Requirement R4 is intended to ensure that an entity can communicate information about events. Some of these events are potential sabotage events, and communicating these events is intended to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events,

and the approved VRFs for each of the requirements is "medium." The proposed VRFs for EOP-004-2 are consistent with the existing approved VRFs for both EOP-004 and CIP-001.

Applicability. Commenters also had concerns about the applicability of the standard to Load Serving Entities, who may not own physical assets, as well as to the ERO and Regional Entity. The DSR SDT agrees that the Distribution Provider owns the assets per the Functional Model, however the LSE is an applicable entity under CIP-002, and under the CIP standards is responsible for reporting cyber security incidents. The ERO and RE are also responsible for reporting cyber security incidents under CIP-002. Therefore, the SDT determined that it was appropriate to include LSEs, the ERO and the RE in the applicability of EOP-004-2.

After the drafting team completed its consideration of stakeholder comments, the standards and implementation plan were submitted for quality review. Based on feedback from the quality review, the drafting team has made two significant revisions to the standard. The first revision is to add a requirement for implementation of the Operating Plan listed in Requirement R1. There was only a requirement to report events, but no requirement specifically calling for updates to the Operating Plan or the annual review. This was accomplished by having two requirements. The first is Requirement R2 which specifies that an entity must implement the Operating Plan per Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5:

> R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

The second Requirement is R3 which addresses Part 1.3:

> R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

The second revision based on the quality review pertains to Requirement R4. The quality review suggested revising the requirement to more closely match the language in the Rationale box that the drafting team developed. This would provide better guidance for responsible entities as well as provide more clear direction to auditors. The revised requirement is:

> R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.

You do not have to answer all questions. Enter all comments in Simple Text Format.

1. The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below.

☐ Yes
☒ No

Comments: We do not believe R4 is necessary, whether or not the process, plan, procedure, etc. is "verified" is of no consequence; if it is not viable upon event and when it is needed, as entity would not be able to meet R3. Therefore, it is in the best interest of the Responsible Entity to *periodically* review the process.

2. The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below.

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

☐ Yes
☒ No

Comments: The only true requirement that is results-based, not administrative and is actually required to support the Purpose of the Standard is R3. We strongly urge the SDT to delete the other Requirements.

3. The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below.

☒ Yes
☐ No

Comments:

4. Do you have any other comment, not expressed in questions above, for the DSR SDT?

Comments:

From: Monica Benson
To: monica.benson@nerc.net
Subject: NERC: Standards Announcement - Project 2009-01 Disturbance and Sabotage Reporting | Ballot Pool, Initial Ballot and Formal Comment Period Information
Date: Friday, October 28, 2011 11:26:43 AM

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Ballot Pool Window Now Open: Oct. 28 – Nov. 28, 2011
Formal Comment Period Open: Oct. 28 – Dec. 12, 2011
Initial Ballot Window: Dec. 2 – 12, 2011

Available Now

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Monday, December 12, 2011. Two ballot pools are being formed – one for balloting the standard, and a separate ballot pool for the non-binding poll of the associated VRFs and VSLs. The ballot pool window is open through 8 a.m. Eastern on Monday, November 28. ***(Please note that this is 8 a.m. on the Monday following Thanksgiving weekend – Registered Ballot Body members interested in joining the ballot pools for this project should plan accordingly).***

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended April 8, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-1a), and identifies how the requirement has been treated in the revisions proposed Draft 3 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for EOP-004-2 and Associated VRFs/VSLs
Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of EOP-004-2, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with EOP-004-2. RBB members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pool to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)

The ballot pool list server for the initial ballot is: bp-2009-01_DSR_in@nerc.com
The ballot pool list server for the non-binding poll is:
bp-2009-01_DSR_NB_2011_in@nerc.com

Instructions for Commenting
Please use this electronic form ONLY to submit comments. In order to avoid duplication, please indicate "submitted comments electronically" on the ballot and non-binding poll comment section to avoid duplication.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps
An initial ballot of EOP-004-2 will be conducted beginning on Friday, December 2, 2011 through 8 p.m. Eastern on Monday, December 12, 2011.

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

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

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" webpage or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" email list, send an email request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the email.

Standards Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on

stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

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

You have received this email because you are a registered representative in the Registered Ballot Body.

A. Introduction

1. Title: **Sabotage Reporting**

2. Number: CIP-001-1

3. Purpose: Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. Level 2: Not applicable.

2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. Level 4:.Not applicable.

E. Regional Differences

None indicated.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required

EOP-004-2 – Event Reporting

Prerequisite Approvals

Revisions to Sections 807 and 808 of the NERC Rules of Procedure
Addition of Section 812 to the NERC Rules of Procedure

Revisions to Glossary Terms

None

Applicable Entities

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider
Load-Serving Entity
Electric Reliability Organization
Regional Entity

Conforming Changes to Other Standards

None

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval.

Retirements

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

CIP-008-4 – Cyber Security - Incident Reporting and Response Planning: Retire R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

A. Introduction

1. Title: Disturbance Reporting

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Ballot Pool Window Now Open: Oct. 28 – Nov. 28, 2011
Formal Comment Period Open: Oct. 28 – Dec. 12, 2011
Initial Ballot Window: Dec. 2 – 12, 2011

Available Now

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Monday, December 12, 2011. Two ballot pools are being formed – one for balloting the standard, and a separate ballot pool for the non-binding poll of the associated VRFs and VSLs. The ballot pool window is open through 8 a.m. Eastern on Monday, November 28. ***(Please note that this is 8 a.m. on the Monday following Thanksgiving weekend – Registered Ballot Body members interested in joining the ballot pools for this project should plan accordingly).***

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended April 8, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-1a), and identifies how the requirement has been treated in the revisions proposed Draft 3 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for EOP-004-2 and Associated VRFs/VSLs

Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of EOP-004-2, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with EOP-004-2. RBB

members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pool to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)

The ballot pool list server for the initial ballot is: bp-2009-01_DSR_in@nerc.com

The ballot pool list server for the non-binding poll is:
bp-2009-01_DSR_NB_2011_in@nerc.com

Instructions for Commenting

Please use this electronic form ONLY to submit comments. In order to avoid duplication, please indicate "submitted comments electronically" on the ballot and non-binding poll comment section to avoid duplication.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

An initial ballot of EOP-004-2 will be conducted beginning on Friday, December 2, 2011 through 8 p.m. Eastern on Monday, December 12, 2011.

Background

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

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

Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" e-mail list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the e-mail.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are four requirements in EOP-004-2. Requirement R1 was assigned a "Lower" VRF while Requirements R2, R3 and R4 were assigned a "Medium" VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which functional entities are required to have procedure(s) for recognition of events, gather information for completing an event report, and communicating with other entities. The VRFs are only applied at the Requirement level and each Requirement Part is treated equally.
- FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have procedure(s) for recognition of events, gather information for completing an event report, and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. Most event reporting requirements in Attachment 1 are

for 24 hours after an event has occurred. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have a procedure(s) is not likely to directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system if an entity cannot report an event and that event led to other preventable events on the BES had the report been made in a timely fashion. Development of the procedure(s) is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contain only one objective which is to have procedure(s). The content of the procedure is specified in Parts 1.1-1.5. Since the requirement is to have a procedure(s), only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R4 is a requirement for entities to report events using the procedure(s) for recognition of events per Requirement R1. The Standard Drafting Team views this as an aspect of implementing the Operating Plan for reporting events. The act of reporting in and of itself is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R5 mandates that report events per their procedure(s). Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.

- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R5 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R4 is a requirement for entities to report events using the procedure(s) for recognition of events per Requirement R1. The act of reporting in and of itself is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R5 mandates that report events per their procedure(s). Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R5 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R4:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 specifies a time frame in which to verify the communications protocols developed in the procedures pursuant to Requirement R1. Both requirements have a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to verify a communications protocol could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system if an entity cannot report an event and that event led to other preventable events on the BES had the report been made in a timely fashion. Therefore this requirement was assigned a medium VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. Since the Requirement has four Parts, the VSLs were developed to count a violation of each Part equally. Therefore, four VSLs were developed.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2.	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is for entities to implement the Operating Plan for event reporting. There are four Parts that are addressed under this requirement. Parts 1.1 and 1.2 are only applicable for an actual event and are binary in nature. Parts 1.4 and 1.5 require updates or reviews based on certain intervals. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If the update or review is not performed, then the VSL is Severe.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2.	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R4:

R#	Compliance with NERC's Revised VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3.	Meets NERC's VSL guidelines - Severe: The performance or product measured does not substantively meet the intent of the requirement.	The most comparable VSLs for a similar requirement is EOP-008-0, R1.7 which calls for an annual update to a plan. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the verification of the communication protocol. If the verification is not achieved, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

BES Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter ~~or Physical Security Perimeter of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System, or
- Results in unauthorized physical access into a Defined Physical Boundary .

BES Cyber System

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

BES Cyber System Information

Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.

BES Reliability Operating Services

BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:

Dynamic Response to BES conditions

Actions performed by BES Elements, Facilities or systems automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response

- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - Current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

Balancing Load and Generation

Activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation Operating Service include, but are not limited to:

- Calculation of ACE
  - Field data sources (real time tie flows, frequency sources, time error, etc)
  - Software used to perform calculation
- Unit commitment
  - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc), load schedules
- Load management
  - Ability to identify load change need
  - Ability to implement load changes
- Demand Response
  - Ability to identify load change need
  - Ability to implement load changes
- Manually Initiated Load shedding
  - Ability to identify load change need
  - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time

- Start units and provide energy

Controlling Frequency (Real Power)

Activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency Operating Service include, but are not limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics
  - Software to calculate unit adjustments
  - Transmit adjustments to individual units
  - Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

Controlling Voltage (Reactive Power)

Activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage Operating Service include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources
  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

Managing Constraints

Activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)

- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's

Identify and monitor Flowgates

Monitoring & Control

Activities, actions, and conditions that provide monitoring and control of BES elements.

An example aspect of the Monitoring and Control Service is, but is not limited to:

- All methods of operating breakers and switches (such as SCADA)

Restoration of BES

Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES Operating Service include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

Situational Awareness

Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness Operating Service include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis
- Frequency monitoring

Inter-Entity Real-Time Coordination and Communication

Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives

CIP Exceptional Circumstance

A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Inter-utility exchange of BES reliability or operability data,
- Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,
- Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,
- Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES
- Coordination of BES restoration activities.

Cyber Assets

Programmable electronic devices ~~and communication networks~~ including the hardware, software, and data in those devices.

Defined Physical Boundary ("DPB")

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled.

Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." *Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security.*

Electronic Access Control or Monitoring Systems

Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems

Electronic Access Point ("EAP")

An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets.

Electronic Security Perimeter ("ESP")

~~The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.~~
A collection of Electronic Access Points that protect one or more BES Cyber Systems.

External Connectivity

Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity

The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access

Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Intermediate Device

A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset.

Reportable BES Cyber Security Incident

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Transient Cyber Asset

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Physical Security Perimeter

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. **Title:** Cyber Security — BES Cyber Asset and BES Cyber System Categorization

2. **Number:** CIP-002-5

3. **Purpose:** To identify and categorize BES Cyber Assets and BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Assets and BES Cyber Systems could have on the reliability of the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

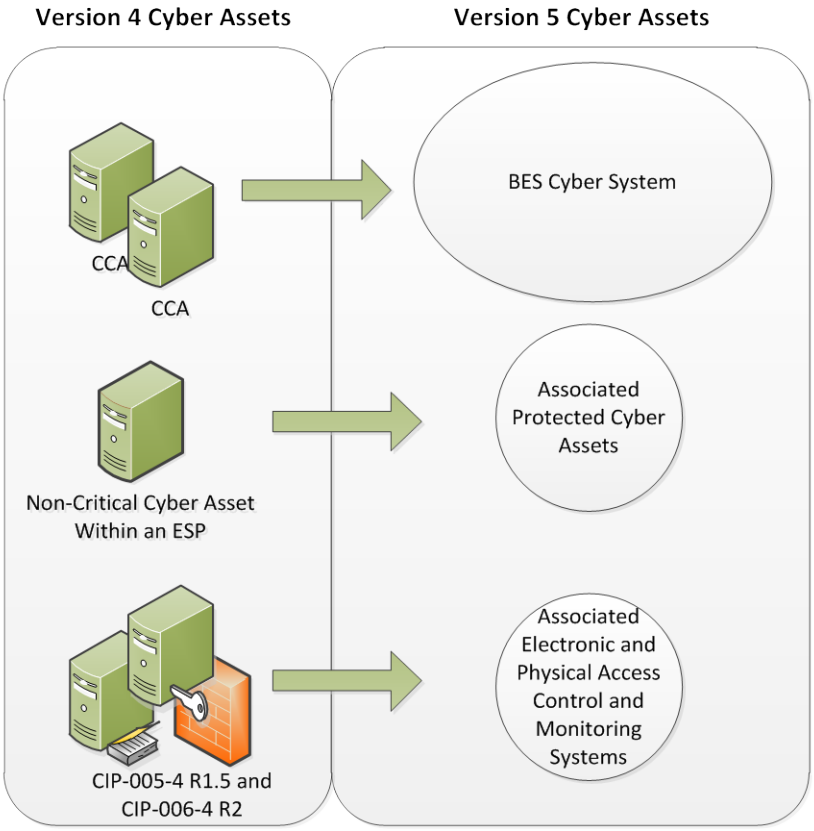
4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Background:

This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems and BES Cyber Assets based on their impact on the real-time operation of the Bulk Electric System (BES). Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets. The CIP Cyber Security Standards use this term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term BES Cyber System is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System or they might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

BES Reliability Operating Services

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Assets and BES Cyber Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber Assets perform or support any BES Reliability Operating Service. These services are functions that provide services for the reliable operation of the BES and are based on the functions defined in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES Cyber Assets and BES Cyber Systems that perform or support BES Reliability Operating Services. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliability and operability of the BES. To provide a better defined time horizon than “real-time”, BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES cyber assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems and their BES Cyber Assets into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. All other BES Cyber Systems are deemed to be Low Impact.

This general process of categorization of BES Cyber Systems and BES Cyber Assets based on impact on the BES Reliability Operating Services is consistent with risk management approaches for the purpose of application of cyber security controls in the rest of Version 5 cyber security standards.

Requirements and Measures

Rationale – R1:

Cyber Assets and Cyber Systems have varying impact on the reliability and operability of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as required in R1 and list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.

Rationale – R2

The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2)

B. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, 5% or fewer of High and Medium Impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 or fewer High and Medium Impact BES Cyber Assets have not been identified or categorized or have	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 5% but less than or equal to 10% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact and BES Cyber Assets, more than 5 but less than or equal to 10 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High or Medium Impact BES Cyber Assets, more than 10% but less than or equal to 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High or Medium Impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, more than 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of High and Medium Impact BES Cyber Assets in accordance with part 1.1 for more than 30, but less than or equal to 40 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 40, but less than or equal to 50 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 50, but less than or equal to 60 calendar days following the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 60 calendar days following the completion of the change.
R2	**Operations Planning**	**Lower**	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 30, but less than or equal to 40 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 40, but less than or equal to 50 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 50, but less than or equal to 60 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 60 calendar days of the latest required date.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			latest required date.	latest required date.	latest required date.	

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

None.

CIP-002-5 - Attachment I

Impact Categorization of BES Cyber Assets and BES Cyber Systems

1. High Impact Rating (H)

Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator or Transmission Owner that includes control of one or more of the assets identified in criteria 2.2, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 or 2.12 below.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below.

2. Medium Impact Rating (M)

Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:

2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.2. An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

2.4. Each Blackstart Resource identified in its Transmission Operator's restoration plan.

2.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource

- Up to and including the first interconnection point of the generation unit(s) to be started, or

- up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or
- up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.

2.6. Transmission Facilities operated at 500 kV or higher.

2.7. Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations and where the "total weighted aggregate value" of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.

Voltage Value of a Line	Weight Value per Line
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.8. Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".

2.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.

In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."

2.10. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.11. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations.

In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."

2.12. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by its regional load shedding program.

2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation.

3. Low Impact Rating (L)

All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H) or Section 2 Medium Impact Rating (M).

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more **BES Reliability Operating Services**." The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability operations service, which determines what each entity needs to address with their CIP program. The following provides guidance for Responsible Entities to determine applicable Reliability Operations Services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that should be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, GO)
  - Zone protection for breaker failure (TO)
  - Breaker protection (TO)
  - Current, frequency, speed, phase (TO, GO)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flowgates (TOP, RC)
-

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include, but are not limited to:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination and Communication

The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include, but are not limited to:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC standard EOP-005.

Similarly, it is expected that only Load Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the systems are assumed to be vulnerable) and a probability of threat

of 1 (100%). The criteria in attachment 1 provide a measure of the impact on the reliability and operability of the BES.

Responsible Entities are required to identify and categorize those systems that have high and medium impact. Other BES Systems and BES Cyber Assets are deemed to be low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System. While the criteria are based on the scope of the BES asset, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term “Facilities”, it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems . Generation Facilities are separately discussed in the Generation section below.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- A BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact

This category includes those BES Cyber Systems, used by and at Control Centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), Transmission Owner (TO) or Generation Operator (GOP), as defined in the NERC Functional Model. While those entities that have been registered as the above named Functional Entities are specifically referenced, it must be noted that there may agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control

Centers that perform these functional obligations must be subject to categorization as High Impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP or GOP facilities.

Medium Impact

Generation

The criteria in Attachment 1, Medium Impact that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.4, 2.5, 2.11 and 2.13.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as Medium Impact. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in

the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such BES facilities would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then BES Cyber Systems for that unit must be categorized as Medium Impact.

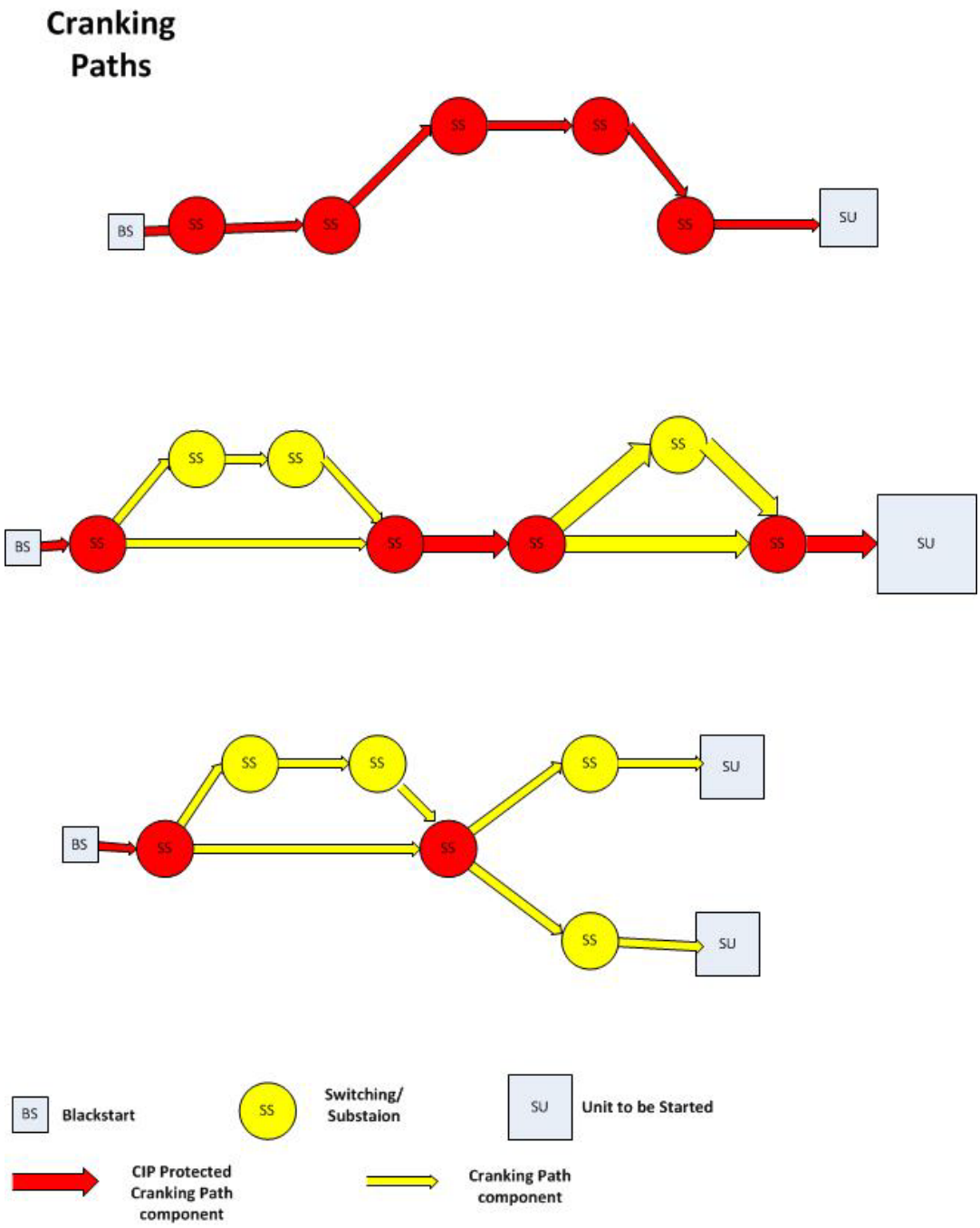
- In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium Impact. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.

  Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.

The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.



- Part 2.11 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as Medium Impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it

operates outside of the parameters it was designed for. Generation Owners and Operators which own BES Cyber Systems for such systems and schemes must designate them as Medium Impact.

- Part 2.13 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generation Operator for an aggregate generation of 300 MW or higher. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as Low.

Transmission

Parts 2.1, 2.2, 2.5-2.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a system to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). For the WECC region where IROLs are not defined, alternative criteria are defined.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.6 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the Medium Impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a facility for a Medium Impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.7 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

- Parts 2.8 and 2.9 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

Alternate thresholds are used for WECC, where IROLs are not used.

- Part 2.10 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.11 designates as Medium Impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

  For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.

- Part 2.12 designates as Medium Impact those BES Cyber Systems for systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of criterion 2.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Medium Impact.

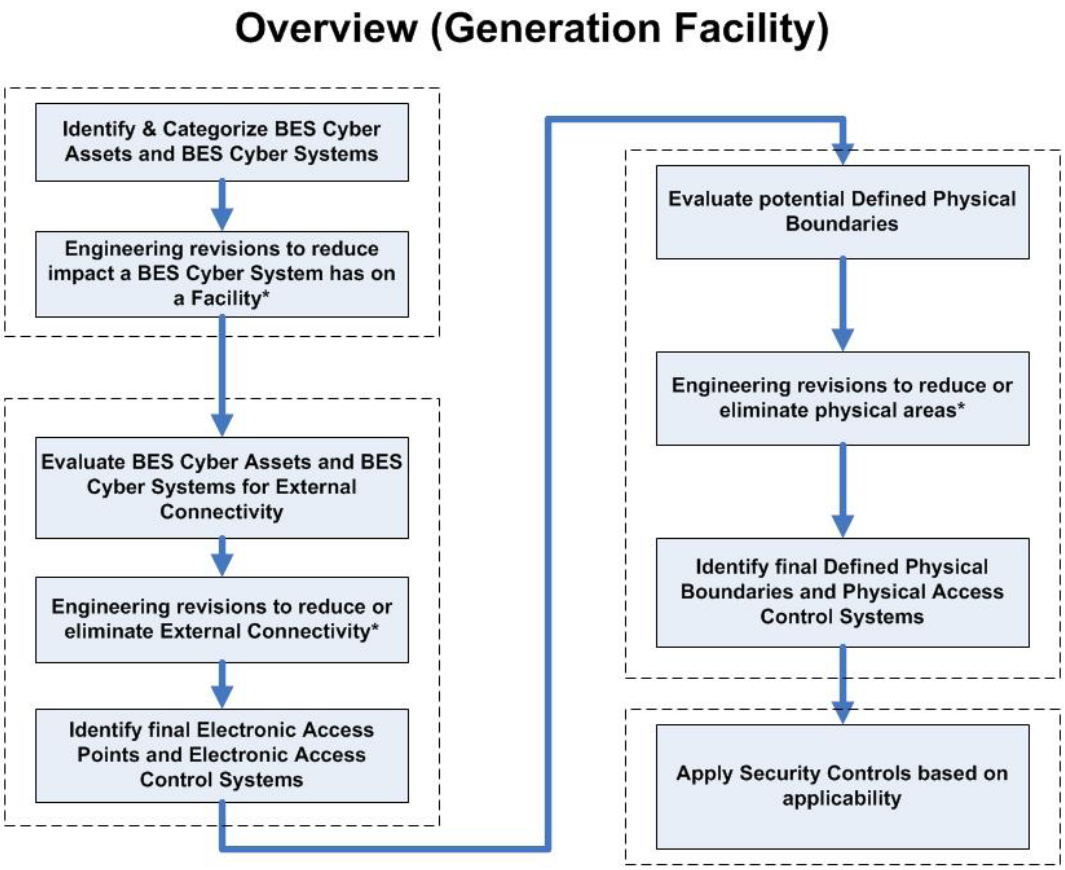
  Within an operational environment the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.13 categorizes as Medium Impact those cyber systems used by and at Transmission Operators and Owners Control Centers not already categorized as High Impact.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: Standard CIP-003-5 requires that Responsible Entities have minimum security management controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-003-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Except for R1, R5 and R6, Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with

a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The identification and documentation of the single CIP Senior Manager and any delegations ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43.

In FERC Order 706, paragraph 296, it requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the responsible entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent

R1. Each Responsible Entity shall identify, by name, a CIP Senior Manager. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance

R2 Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** Personnel Security
- **1.2.** Electronic Security Perimeters
- **1.3.** Remote Access
- **1.4.** Physical Security
- **1.5.** System Security
- **1.6.** Incident Response
- **1.7.** Recovery Plans
- **1.8.** Configuration Change Management
- **1.9.** Information Protection
- **1.10.** Provisions for declaring and responding to CIP Exceptional Circumstances

M2. Evidence may include, but is not limited to:

1. One or more documented cyber security policies, and
2. Records that indicate the required ten topics were implemented.

Rationale – R3:

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the

R3. Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy, and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

Rationale – R4:

The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.

R4. Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

- Policies are accessible on the corporate Intranet site
- Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized
- Policies are posted on company bulletin boards
- Policies are accessible to individuals with all types of job functions that have access to BES Cyber Systems
- Dated training records to show that individuals have received periodic training on necessary elements of the cyber security policy

Rationale – R5:

In FERC Order 706, paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations in order that this line of authority is clear and apparent from the documented delegations.

R5 The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to:

- A dated document, signed by the CIP Senior Manager listing personnel (by title) who are delegated the authority to approve or authorize specifically identified items (i.e. substation maintenance manager may authorize unescorted physical access to substation control houses), or
- A dated document, signed by the CIP Senior Manager listing individuals who are delegated the authority to approve or authorize specific actions by requirement (i.e., 'name of individual' who may approve CIP-002-5 R3), or
- A dated document, signed by the CIP Senior Manager delegating to a named individual the authority for all approvals in CIP-002-5 and CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; a dated document, signed by the previous named individual delegating to a 3rd named individual the authority for all approvals in CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; and a dated document, signed by the 3rd named individual delegating to each of the plant managers (by title) the authority for all approvals and authorizations required in CIP-004-5 through CIP-011-1 for each of the their plants, respectively.

Rationale – R6:

The intent of the SDT is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authoritv.

R6. Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change[2]. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or positions of any delegations, that is current to within 30 days with the name or position of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity.
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

[2] Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

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

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

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	**N/A**	The Responsible Entity has not identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R2	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required parts 2.1 to 2.10.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has made some but not all individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.	The Responsible Entity has not made any individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by position or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R2:

The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics or may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In this case of a high-level umbrella policy, it would be expected that the entity provide the high-level policy as well as the additional documentation in order to prove compliance with CIP-003-5 R2. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

2.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

2.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

2.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating interactive remote access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls

2.4 Physical Security

- Strategy for protecting cyber assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

2.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

2.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

2.7 Recovery Plans

- Availability of spare components
- Availability of system backups

2.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

2.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

2.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to Responsible Entity's security policies since it considers this a general management issue that is not within the scope of a compliance requirement. The SDT considers this an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5 R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but rather the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, this requirement may be met through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to their organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
   - A Transmission Protection System required by a NERC or regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
- A Transmission Protection System required by a NERC or regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-004-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1

require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed.
Reference to prior version: *CIP-004-4 R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized access receives this awareness. Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems contains the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for
   - the visitor control program;
   - electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Define the roles that require training.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role based training program is to understand what roles your people have to help plan what training modules you need to provide.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.1*		**Change Rationale:** *Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the visitor control program.	Evidence may include, but is not limited to, training material on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *Personnel administering the* ***visitor control program*** *and/or providing escort should be part of the core training; FERC Order 706 - paragraph 432.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on handling of BES Cyber System Information and storage media.	Evidence may include, but is not limited to, training material on the handling of BES Cyber System Information, including storage media.
Reference to prior version: *CIP004-4 R2.2.3*		**Change Rationale:** *Core training on the **handling of BES Cyber System (**not Critical Cyber Assets**) Information**, with the addition of **storage media;** FERC Order 706 -paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16)*	
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on identification of a potential BES Cyber Security Incident and associated notifications.	Evidence may include, but is not limited to, training material on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *CIP004-4 R2.2.4 (new; implied but not stated in CIP-004 or CIP-008)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order 706 - paragraph 413; Related to CIP-008 & DHS Incident Reporting requirements for those with roles in incident reporting.*	
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order 706 - paragraph 413.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Minor wording changes.*	
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order 706 - paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring access, dated individual training records, the date access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4 R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order 706 - paragraph 431 is detailed in CIP-003-5..*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4 R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

Rationale for R4: To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	An initial personnel risk assessment that includes identity verification.	Acceptable evidence must include the documented risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.
Reference to prior version: *NEW*		**Change Rationale:** *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.4.
Reference to prior version: *CIP-004-4 R3.3*		**Change Rationale:** *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment.[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before access was authorized; • Dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized.
Reference to prior version: *CIP-004-3 R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update each personnel risk assessment at least once every seven calendar years after the initial personnel risk assessment.	Evidence may include, but is not limited to, current and former personnel risk assessment records.
Reference to prior version: *CIP-004-4 R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*		**Change Rationale:** *CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system generated list of people with unescorted physical access through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4 R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access and a system generated list of personnel who have access • Documentation of the dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access.
Reference to prior version: *CIP 004-4 R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including (i) a dated listing of all accounts/account groups or roles within the system, (ii) a summary description of privileges associated with each group or role, (iii) accounts assigned to the group or role and (iv) dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4 R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to documentation of the review including (i) a dated listing of authorizations for BES Cyber System information, (ii) any privileges associated with the authorizations, and (iii) dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4 R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

Summary of Changes: Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]*

M7. Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination.	Evidence may include, but is not limited to (i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	Evidence may include, but is not limited to, (i) workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed.
Reference to prior version: *CIP-004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	Evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 386 directs modifications to the Standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revoking of access and dated within thirty calendar days of the termination.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within thirty calendar days of the termination • Workflow or sign-off form showing password reset within thirty calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007 R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did not provide on-going security awareness reinforcement on at least a quarterly basis. (1.1)	The Responsible Entity did not document or implement a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include training for one or more of the roles as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	N/A	N/A	The Responsible Entity trained some but not all individuals authorized for electronic or unescorted physical access at least once every calendar year, but not to exceed 15	The Responsible Entity trained some, but not all individuals authorized for electronic or unescorted physical access prior to their being granted such access, except in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					months between training. (3.2)	policy-identified CIP Exceptional Circumstances. (3.1) OR The Responsible Entity did not fully implement its cyber security training program.
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	The Responsible Entity did not have a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day**	**Medium**	N/A	N/A	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations				did perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances, but the personnel risk assessments are not updated at least once every seven years. (5.2)	did not perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances. (5.1) OR The Responsible Entity did not have a documented process for personnel risk assessments.
R6	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			functions. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions. (6.3)	functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3) OR The Responsible Entity did not perform a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical or electronic access to BES Cyber Systems. (6.4) OR The Responsible Entity did not verify provisioned accounts/account groups or role categories and their specific, associated privileges according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.5) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6) OR The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7) OR The Responsible Entity did not have a documented process for access management.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	**Same Day Operations and Operations Planning**	**Medium**	N/A	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for one individuals who was terminated, resigned, reassigned, or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2) OR The Responsible Entity did not have a documented process for access revocation.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities from Table R4. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of “role appropriate” as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-011-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their

identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

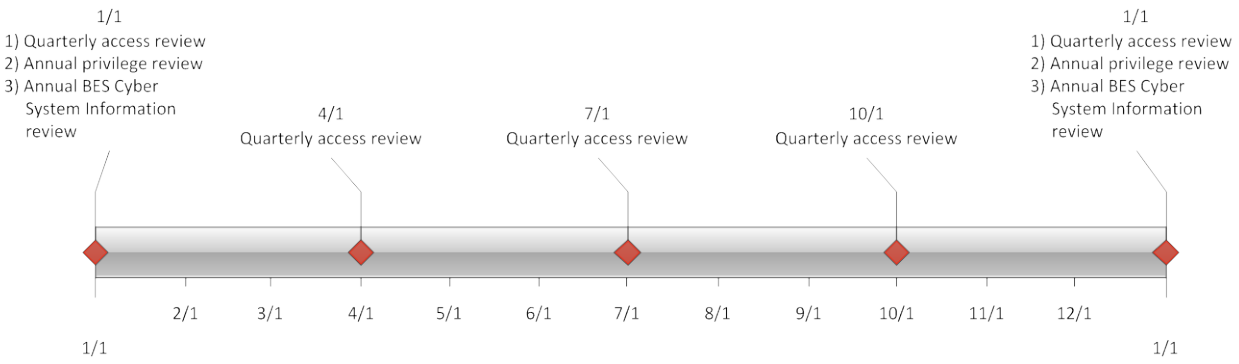
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e. least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g. system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in R6 is included below.



Separation of duties should be considered when performing the reviews in R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resource personnel are notified of the termination and works with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resource personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	No action is required.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications

of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in 7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents an Entity from performing all of the access revocation at the time termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-5

3. Purpose: Standard CIP-005-5 requires the identification of all Electronic Access Points on the Electronic Security Perimeter(s), the protection of the communication through those points, and specific protections for interactive user remote access.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional reliability standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-005-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.3	Electronic Access Points at High Impact BES Cyber Systems Electronic Access Points at Medium Impact BES Cyber Systems with External Routable Connectivity.	Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only explicit access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005 R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP.*	
1.4	Electronic Access Points that use dial-up access for non-Interactive Remote Access at High Impact BES Cyber Systems Electronic Access Points that use dial-up access for non-Interactive Remote Access at Medium Impact BES Cyber Systems.	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to a documented process identified in Requirement R1, Part 1.4 that describes how the Responsible Entity is providing authenticated access through each dial up Electronic Access Point.
Reference to prior version: *CIP-005 R2.3*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure", which is that the BES Cyber System should not be directly accessible with a phone number only*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.5	Electronic Access Points with External Routable Connectivity at High Impact BES Cyber Systems Electronic Access Points with External Routable Connectivity at Medium Impact BES Cyber Systems at Control Centers.	A documented method for detecting malicious communications at each EAP.	Evidence may include, but is not limited to: • Configuration files of an intrusion detection systems deployed at an EAP • Logs that were generated by an intrusion detection system • Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (*intrusion detection systems / intrusion protection systems*) a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Remote Access Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Note that a UserID is not considered an authentication factor.
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access OR The Responsible Entity did not establish Electronic Access Points to control and secure access to its BES Cyber Systems OR The Responsible Entity did not establish explicit inbound and outbound access permissions at each identified EAP that utilizes routable protocols OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not perform authentication before establishing connectivity with the BES Cyber System for an EAP that uses dial-up access OR The Responsible Entity did not deploy methods to detect malicious communications.
R2	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not implement an Intermediate Device between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005 R1 requires that BES Cyber Systems must be segmented from other systems of differing trust levels by requiring controlled electronic access points between the different trust zones. ESP's also are used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capabilities.

BES Cyber Systems are to be protected by Electronic Access Points (EAP's) that control traffic into and out of the BES Cyber System. Responsible Entities (RE's) should know what traffic needs to cross an EAP and document those justifications and insure the EAP's limit the traffic to only those known, justified communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

This requirement applies only to communications for which 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols and dialup modems. Direct serial, non-routable connections are not included.

The intent of securing dialup connectivity is to prevent situations where connectivity is established directly to the BES Cyber Asset with only a phone number. If a dialup modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is not functioning as an Electronic Access Point. The requirement calls for some form of authentication of the calling party when connectivity is granted to the BES Cyber Asset. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version	Date	Action	Change Tracking
		FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Approved by the NERC Board of Trustees	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: Standard CIP-006-5 requires the implementation of a physical security plan for the protection of BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-006-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required. in the documented processes.. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 were intended to constitute a physical security program, though there was no specific requirement dictating the need for such a program, only physical security plans.

Added details to address FERC Order 706, paragraph 572 directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address FERC Order 706 p575 directive.

R1. Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*

M1. Evidence must includes each of the documented physical security plan or plans that collectively include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Associated Physical Access Control Systems Low Impact BES Cyber Systems.	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c R2.1 for Physical Access Control Systems* *New Requirement for Low Impact BES Cyber Systems*		**Change Description and Justification:** *To allow for programmatic protection controls as a baseline, this includes how the entity plans to protect Low Impact BES Cyber Systems and does not require detailed list of individuals with access.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access to reflect the change from Physical Security Perimeter to Defined Physical Boundary. The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section .*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order 706 p572 related directives for physical security defense in depth.* *FERC Order 706 p575 directives addressed by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered defined physical boundary(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated.
Reference to prior version: *CIP006-4c R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section..*	
1.5	Associated Physical Access Control Systems	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated
Reference to prior version: CIP006-4c R2.2		**Change Description and Justification:** *Addresses the old CIP-006-4c R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into Defined Physical Boundaries and additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Defined Physical Boundaries that show the date of entry into Defined Physical Boundaries.
Reference to prior version: CIP-006-4c R6		**Change Description and Justification:** *CIP-006-4c R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the* Defined Physical Boundary*.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section .*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Defined Physical Boundaries protecting BES Cyber Systems or Electronic Access Control Systems as applicable in table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M2. Evidence must include the documented visitor control program that collectively includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Defined Physical Boundaries and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c R1.6.2*		**Change Description and Justification:** *No change.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	Evidence may include, but is not limited to, a visitor control program that provides logging of the entry and exit of visitors including date, time, and visitor name along with the individual point of contact; dated visitor logs for each Defined Physical Boundary that include the same required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Addressed multi entry requirements and added the point of contact which is the person who can be considered the sponsor for the visitor. There is no need to document the escort or handoffs between escorts.*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order 706, paragraph 581 directives for test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Evidence must include each of the documented maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Maintenance and Testing Program			
Part	**Applicability**	**Requirement**	**Measures**
3.1	Associated Physical Access Control Systems Locally mounted hardware or devices associated with Defined Physical Boundaries	Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	Evidence may include, but is not limited to a maintenance and testing program that provides for testing the Physical Access Control Systems and locally mounted hardware or devices associated with Defined Physical Boundaries prior to commissioning and at least once every 24 calendar months thereafter, and provides additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed at least once on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c R8.1*		**Change Description and Justification:** *Added details to address FERC Order 706 p581 directives to test more frequently than every three years. It was felt annually testing was too often.*	
3.2	Associated Physical Access Control or Monitoring Systems	Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	Evidence may include, but is not limited to, availability of the outage records.
Reference to prior version: *CIP-006-4c R8.3*		**Change Description and Justification:** *Outage records shall be generated but the retention period is addressed in the retention section.*	

C. Compliance

1. Compliance Monitoring Process

5.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For responsible entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

5.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

5.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

5.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry. (Part 1.7)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems (Part 1.5)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized access through any access point in a Defined Physical Boundary. (Part 1.4) OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. OR The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems. (Part 1.3)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity included a visitor control program in its	The Responsible Entity included a visitor control program in its	The Responsible Entity has failed to include or implement a visitor

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			physical security plan, but did not log each of the entry and exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact.	physical security plan, but it does not meet the requirements of continuous escort.	control program to provide required escorted access of visitors within any Defined Physical Boundary protecting BES Cyber Systems.
R3	**Long Term Planning**	**Lower**	N/A	The Responsible Entity has documented and implemented a maintenance and testing program, but the testing is not performed on a cycle of not more than 24 months.	The Responsible Entity has documented and implemented a maintenance and testing program, but not all outage records regarding access controls, logging, and alerting are generated as required.	The Responsible Entity has not documented and implemented maintenance and testing programs.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Defined Physical Boundary.

Methods to alert on physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order 706 p572 directive, directed the intent of utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Defined Physical Boundaries, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin-code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in

combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e. key or card key) would provide access through both.

Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Defined Physical Boundary. This includes motion sensors, electronic lock control mechanisms and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor and logging systems or hardware at access points are broken or unavailable.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: Standard CIP-007-5 requires the implementation of technical mechanisms for reducing the risk of loss of availability due to degradation and misuse of BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-007-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	Evidence may include, but is not limited to, documentation of the need for each network-accessible port and screen shots showing the accessible ports of BES Cyber Assets.
Reference to prior version: *CIP-007-4 R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or BES Cyber Asset basis. The list could be sorted by BES Cyber System or source.
Reference to prior version: *New*		**Change Rationale:** *Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or updates released by the documented sources, and a dated remediation plan showing how the vulnerability will be addressed.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process for remediation, including any exceptions for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Exports from automated patch management tools that provide installation date; • Verification screen captures that show BES Cyber System Component software revision; • Registry exports that show software has been installed; • Evidence that affected services have been disabled; • Implementation evidence of software configuration changes recommended by the operating system or Control System vendors.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable components of a BES Cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

The requirement for Maintenance Cyber Assets or media in 3.4 is intended to ensure that devices used for maintenance do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System.

This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection.

Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (i.e. through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disarm or remove identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (i.e. quarantine, alert, etc.) to detected malicious code; • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii) either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.2*		**Change Rationale:** *See the Summary of Changes.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log each Transient Cyber Asset connection.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets.
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4 R5 and CIP-007-4 R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor”.

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types.
Reference to prior version: *CIP-005-4 R3, CIP-007-4 R5, R5.1.2 R6.1, R6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	Evidence may include, but is not limited to paper or system-generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screen-shots showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Detect and activate a response to event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, (i) dated event logging failures and screen-shots showing how real-time alerts were configured (ii) dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security-related event logs beyond ninety days up to the evidence retention period.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.5*		**Change Description and Justification:** *Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4 R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the Standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table 5 – System Access Controls and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Validate credentials before granting electronic access to each BES Cyber System.	Evidence may include, but is not limited to, documentation describing how users are authenticated before being granted access and demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System.
Reference to prior version: *CIP-007-4 R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4 R5.2, R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4 R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.4	All Responsible Entities	Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	Evidence may include, but is not limited to: • Demonstration showing default vendor passwords have been changed, sampled on a locational basis. • Records of a procedure that passwords are changed when new devices are deployed. • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4 R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length, complexity and periodicity of changing passwords. • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R5.3*		**Change Rationale:** *CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process..*	
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Screen-shots of the account-lockout parameters • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not document the logical network accessible ports and include why the ports are necessary.	The Responsible Entity did not disable or restrict access to unnecessary logical network accessible ports. OR The Responsible Entity did not disable or restrict the use of unnecessary physical ports used for network connectivity, console commands, or removable media.
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not identify a source or sources that are monitored for the release of security related patches, hotfixes, and/or updates for all software and firmware

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated with the BES Cyber System or BES Cyber Assets. OR The Responsible Entity did not identify applicable security related patches, hotfixes, and/or updates and create a remediation plan, or revise an existing remediation plan within 30 days of release from the identified source. OR The Responsible Entity did not implement the remediation plan as required, except for CIP Exceptional Circumstances.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code on all Cyber Assets, Transient Cyber Assets and removable media.	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not disarm or remove identified malicious code. OR Where signatures or patterns are used, the Responsible Entity did not deploy method(s) to update malicious code protections within 30 days of signature or pattern update availability.
R4	**Same Day Operations and Operations**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to review a summarization of	The Responsible Entity failed to identify and implement methods to generate real-time alerts for event logging	The Responsible Entity failed to identify and implement methods to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessment			logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures, and activate a response before the end of the next calendar day.	failures, and activate a response to rectify the event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System generated security-related events for at least the last 90 consecutive days, where technically feasible.	generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to identify and implement methods to log generated events that it determines necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared, default, and other generic account types. OR The Responsible Entity	The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					failed to implement procedures to identify the individuals with authorized access to shared accounts.	The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of BES Cyber Assets by requiring entities to disable known unnecessary ports. The intent is for the entity to know what is accessible on their assets and systems, why they are needed, and disable or restrict access to all other ports.

1.1. For the logical network ports this is most often accomplished by disabling the corresponding service or program that is listening on the port. It can also be accomplished through using host-based firewalls or other means on the device to restrict access. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary.

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Defined Security Boundary in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem or inserting a USB drive with auto-run capability. In cases where the Component cannot logically restrict physical ports, entities should have clear signs or obstructions indicating the unnecessary ports are not to be used.

Requirement R2:

The intent of R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; its main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. *Documenting the source is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.* The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors

could all be sources to monitor for release of security related patches, hotfixes, and/or updates. In the event that software or firmware is no longer supported by a software or firmware vendor or Control System vendor it can be noted in your source document. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system.

2.2. The intent is for Responsible Entities to perform an assessment of security related patches as they are released from their monitored source and create a remediation plan for applicable patches as to how the vulnerability will or has already been remediated. An assessment should consist of determination of the applicability of the entity's specific environment and systems. IF the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, and the steps the entity has previously taken or will take. If the entity has to take steps to mitigate this new vulnerability, the remediation plan will include a timeframe. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

Common malware introduction methods include web browsing, email attachments, and portable storage media. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each component. Rather, the Responsible Entity determines on a BES Cyber System basis which components have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional anti-virus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or components that are of identical architecture, they may provide one process that describes how all the components are covered.

For malware detection technologies that are updated in response to evolving threats or depend on signatures of known attacks, the entity must specify how those updates are tested before implementation. The testing should not negatively impact the reliability of the BES. The testing is focused on the update itself and if it will have an adverse impact on the BES Cyber System. The testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production. This includes the instance where the update may provide a "false positive."

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the Standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent that if a device cannot log a particular event that a TFE must be generated. The intent is that if any of the items in the bulleted list (for example, user logouts) can be

logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the cyber asset and the logging system if the cyber asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Data Base.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.3. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	1 year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	2 years or more

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008)
2. SC authorized moving the SAR forward to standard development (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: Standard CIP-008-5 requires the identification, classification, response, and reporting of BES Cyber Security Incidents related to BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-008-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -a**pplies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a

Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP 4 directs further external reporting actions and timing requirements. When a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: (FERC directives, most significant items, summary of smaller items)

R1. Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	Processes to identify, classify, and respond to BES Cyber Security Incidents.	Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.2	All Responsible Entities	A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of process(es) that provide guidance or thresholds for determining which BES Cyber Security Incidents are also Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.3	All Responsible Entities	Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that addresses roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communication processes or procedures.
Reference to prior version: *CIP-008 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R2: Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	All Responsible Entities	When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged. Allows deviation from plan during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.2	All Responsible Entities	Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.3	All Responsible Entities	Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	Evidence may include, but is not limited to, dated documentation related to Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Summary of Changes: Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment and Real-Time Operations]*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	All Responsible Entities	Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Included requirement for review after testing or actual response based on review of DHS controls*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not define the roles and responsibilities of response personnel, or does not define incident handling procedures, or does not communicate the incident to appropriate organizations.	The Responsible Entity has not developed a BES Cyber Security Incident response plan to identify, classify, and respond to BES Cyber Security Incidents. OR The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not identify Reportable BES Cyber Security Incidents.
R2	**Operations Planning** **Real-time Operations**	**Lower**	N/A	N/A	N/A	The Responsible Entity does not use its BES Cyber Security Incident response plan when an incident occurs. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has not tested the execution of its BES Cyber Security Incident response plan once each calendar year, not to exceed 15 calendar months between executions of the plan.
R3	**Operations Assessment** **Real-time Operations**	**Lower**	N/A	N/A	The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. OR The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans within 30 calendar days of any	The Responsible Entity has not reviewed the results of each of its BES Cyber Security Incident response plan(s), test or actual incident response, within 30 calendar days of execution. OR The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					system, organizational, or technology change that impacts one of the response plans.	updates to all responsible personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials

Requirement R1:

A Reportable BES Cyber Security Incident is a BES Cyber Security Incident that results in a necessary response action. A response action can fall into one of two categories: necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions should be designated as necessary.

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Assets and Systems

2. Number: CIP-009-5

3. Purpose: Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-009-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The

referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For

example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.

Summary of Changes:

Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but is not limited to one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009 R1.1*		**Change Description and Justification:** *Reworded to address FERC Order 706 P694 and simplify the wording.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders, including identification of the individuals responsible for recovery efforts.
Reference to prior version: *CIP-009 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System.
Reference to prior version: *CIP-009 R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Part**	**Part**	**Part**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence of the verification that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	Evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order 706, paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.28 Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	Evidence may include, but is not limited to, dated evidence of a test of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-009 R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC Requirements (739, 748) related to testing of backups.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to: • Dated evidence of an operational exercise initially upon the effective date of the standard and at least once every 39 calendar months between exercises, that demonstrates recovery in a representative environment; • An actual incident response occurred within the 39 calendar month timeframe that implemented the recovery plans.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Addresses FERC Requirement (725) to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies.
Reference to prior version: *CIP-009 R1*		**Change Description and Justification:** *Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Medium**	N/A	N/A.	The Responsible Entity has developed recovery plans, but the plans do not address all of the requirements included in Items 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Assets and BES Cyber Systems that address the conditions for activation, including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to BES Cyber System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
R2	**Long Term**		N/A	N/A	The Responsible Entity has not tested the	The Responsible Entity has failed to conduct a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning	**Lower**			information used in the recovery of BES Cyber Systems that is stored on backup media initially and at least once each calendar year not to exceed 15 calendar months between tests. OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 years, not to exceed 39 calendar months between tests, that is an operational exercise in a representative environment to demonstrate readiness.	recovery plan test initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between tests.
R3	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has not reviewed and	The Responsible Entity has not reviewed its

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					documented the results of its recovery plan test or actual incident recovery within 30 calendar days of its execution. OR The Responsible Entity has not updated its recovery plan based on any documented deficiencies or lessons learned within 30 calendar days of its execution.	recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced. OR The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel within 30 calendar days of completing the updates.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS)

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Configuration Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: Standard CIP-010-1 requires that Responsible Entities have minimum configuration management and vulnerability assessment controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-010-1

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System; • A record in an asset management system that identifies the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic approval (performed by the individual with the authority to authorize the change) in a change management system for each change; • A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.
Reference to prior version: *CIP-007-3 R9* *CIP-003-3 R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3 R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to: • For changes that impacted the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change; • For changes that impacted the CIP-009-required recovery plan of a BES Cyber System, a dated recovery plan, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3 R9*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence includes, but is not limited to a list of security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ,paragraphs 397, 609, 610, and 611*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4 and CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547* *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems	Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new BES Cyber Asset) and the output of the tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items with proposed dates of completion, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3 R4.5* *CIP-007-3 R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for since the last completed audit or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	**N/A**	The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has established a configuration management program, but failed to establish a documented baseline. OR The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity has established a configuration management program, but with respect to the	The Responsible Entity has not established any configuration management programs. OR Did not implement a configuration management program.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					changes in the baseline configuration, did not determine the required cyber security controls that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.	
R2	**Operations Planning**	**Lower**	**N/A**	**N/A**	The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months but less than 18 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an Active Vulnerability Assessment on a new BES Cyber Asset prior to adding it to an applicable BES Cyber System. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months but less than 24 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				performed a vulnerability assessment more than 18 months but less than 21 months since the last assessment on one of its applicable BES Cyber Systems.		OR The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an Active Vulnerability Assessment in a test environment that models the baseline configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).

The Control Center test environment should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, patch level, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple.

Additionally, the entity should note that wherever a test environment is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a control center BES Cyber System which may not be able to be replicated such as a legacy map-board controller or the numerous data communication links from the field or to other control centers (such as by ICCP).

Requirement R2:

It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the Standards Drafting Team understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should not that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well documented in the initial NOPR from FERC as well as FERC Order 706. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

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

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: Standard CIP-011-1 requires that Responsible Entities have protection controls in place to protect BES Cyber System Information.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 The following are exempt from Standard CIP-011-1:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The intent of the information protection processes is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes:

Requirement R4.1 was moved to the definition of BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	One or more methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Access control and handling procedures for BES Cyber System Information.	Evidence may include, but is not limited to: • Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process; • Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; • Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "Implement handling and access control" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3 R4.3*		**Change Rationale:** *No significant changes*	

Rationale – R2:

The intent of the media reuse and disposal processes is to prevent the unauthorized dissemination of BES Cyber System Information upon media reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of BES Cyber Asset media[2], the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.
Reference to prior version: *CIP-007-3 R7.2*		**Change Rationale:** *(FERC Order 706 - p. 631) Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was purged or destroyed prior to its disposal.
Reference to prior version: *CIP-007-3 R7.1*		**Change Rationale:** *Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

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

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented one or more BES Cyber System Information protection processes that include one or more methods to identify BES Cyber System Information and one or more access control and handling procedures for BES Cyber System Information, but has failed to assess adherence, either initially upon the effective date of the standard or periodically, to its BES Cyber System Information protection processes.	The Responsible Entity has not implemented one or more BES Cyber System Information protection processes. OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more access control and handling

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures for BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the media disposal or reuse processes, including the recording of the media purge or destruction, were not followed.	The Responsible Entity has not documented or implemented any media disposal or reuse process to prevent the unauthorized retrieval of BES Cyber System Information from the media.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Entities are free to utilize existing change management and asset management systems. However, the information contained within these systems must be evaluated as the information protection requirements still apply.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, responsible entities still have the flexibility to do this if they so desire. As long as the entity's information protection program includes all required elements, additional classification levels can be created that go above and beyond the requirements.

This requirement is not intended to cover publicly available information such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Information handling procedures should detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into 4 categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly erased using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2008-06 Cyber Security Order 706
Draft CIP-002-4 Informal Review

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed CIP-002-4 changes. These standards were posted for a 30-day informal comment period from May 4, 2010 through June 3, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 119 sets of comments. The complete record of comments submitted is posted on the Project 2008-06 Version 4 CIP Standards page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards, Herb Schrayshuen at (404) 446-2560 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

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

Index to Questions, Comments, and Responses

1. Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification..... 16

1.a. BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation. 16

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES. 48

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:..... 74

2. The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement. 95

3. Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 109

4. Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement..... 130

5. Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall: 146

6. CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 163

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 184

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement. 239

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference? 267

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 284

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement 296

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 311

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification 352

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 366

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 378

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 400

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification. 421

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 433

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification. 439

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification. 445

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 455

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 463

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 483

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 495

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 519

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 530

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification. 542

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 552

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification. 559

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 567

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification..... 573

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 586

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 599

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 610

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 615

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?..... 664

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 678

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification. 706

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 717

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification. 726

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 745

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification. 752

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification. 765

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 770

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 784

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided? 788

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 794

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 803

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 807

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 817

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 824

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 840

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible. 846

54. Do you have any other comments to improve this version of draft standard CIP-011-1? 860

The Industry Segments are:

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

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Larry Bugh	ReliabilityFirst Staff										
2.	Group	Ruth Blevins	Dominion Resources Services, Inc.										
3.	Group	Guy Zito	Northeast Power Coordinating Council										
4.	Group	Kenneth D. Brown	Public Service Enterprise Group companies										
5.	Group	Sasa Maljukan	Hydro One										
6.	Group	David Grubbs	Garland Power and Light										
7.	Group	Roger Powers	CWLP Electric Transmission, Distribution and Operations Department										
8.	Group	Guy Andrews	GTC & GSOC										
9.	Group	Tommy Drea - CIP Compliance	Dairyland Power Cooperative										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Joseph DePoorter	Madison Gas and Electric Company										
11.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										
12.	Group	Denise Koehn	Bonneville Power Administration										
13.	Group	Steve Alexanderson	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group										
14.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates										
15.	Group	Mark Stefaniak	Detroit Edison										
16.	Group	Frank Gaffney	Florida Municipal Power Agency										
17.	Group	Nathan Mitchell	APPA Task Force										
18.	Group	Sheryl Byrd	GE Energy										
19.	Group	Ben Li	IRC Standards Review Committee										
20.	Group	John Van Boxtel	WECC										
21.	Individual	Brent Ingebrigtson	E.ON U.S.										
22.	Individual	Ronald J Slack	Exelon Corporation										
23.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
24.	Individual	John Lawrence	Reliability & Compliance Group										
25.	Individual	Rick Terrill	Luminant										
26.	Individual	Linda Jacobson	FEUS										
27.	Individual	Robert Ulmer	American Transmission Company										
28.	Individual	John Brockhan	CenterPoint Energy										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
29.	Individual	Susan Kurtain	Regulatory Compliance										
30.	Individual	Paul Reymann, CEO	ReymannGroup, Inc.										
31.	Individual	Silvia Parada Mitchell	NextEra Energy Corporate Compliance										
32.	Individual	Boyd Nation	Southern Company										
33.	Individual	Tracey Stewart	Southwestern Power Administration										
34.	Individual	Donald Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition										
35.	Individual	David Batz	EEI										
36.	Individual	Tom Bradish	RRI Energy										
37.	Individual	Dora Moreno	Southern California Edison Company										
38.	Individual	Sandra Shaffer	PacifiCorp										
39.	Individual	Jana Van Ness	Arizona Public Service Company										
40.	Individual	Casey Hashimoto	Turlock Irrigation District										
41.	Individual	Ken Stratton	US Army Corps of Engineers, Omaha District										
42.	Individual	Michael Gammon	Kansas City Power & Light										
43.	Individual	John Alberts	Wolverine Power										
44.	Individual	Mike Hendrix	Idaho Power Company										
45.	Individual	Tony Dodge	BCTC										
46.	Individual	Greg Froehling	Green Country Energy										
47.	Individual	Roger Fradenburgh	Network & Security Technologies Inc										
48.	Individual	John Alberts	Wolverine Power										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
49.	Individual	John Kutzer	Consultant										
50.	Individual	Melissa Kurtz	USACE - Omaha Anchor										
51.	Individual	James Stanton	SPS Consulting Group Inc.										
52.	Individual	Michael Puscas	Northeast Utilities System										
53.	Individual	Roger Pan	Emerson Process Management										
54.	Individual	Jo Ann Newton	PNM Resources, Inc.										
55.	Individual	John Hughes	Electricity Consumers Resource Council (ELCON)										
56.	Individual	Ted Risher	Ingleside Cogeneration, LP										
57.	Individual	Thad Ness	American Electric Power										
58.	Individual	Ed Goff	Progress Energy (non-Nuclear)										
59.	Individual	Mark Thompson	Alberta Electric System Operator										
60.	Individual	Dan Roethemeyer	Dynegy Inc.										
61.	Individual	CJ Ingersoll	Constellation Energy Control and Dispatch, LLC										
62.	Individual	Daniel Duff	Liberty Electric Power, LLC										
63.	Individual	Jonathan Appelbaum	The United Illuminating Co										
64.	Individual	Greg Hataway	Powersouth Energy Cooperative										
65.	Individual	Kasia Mihalchuk	Manitoba Hydro										
66.	Individual	Steven Belle	SCE&G										
67.	Individual	William Gross	Nuclear Energy Institute										
68.	Individual	Randy Schimka	San Diego Gas and Electric Co.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
69.	Individual	Brandy A. Dunn	Western Area Power Administration										
70.	Individual	Eric Scott	Ameren										
71.	Individual	Jim Simpson	Allegheny Energy Supply										
72.	Individual	Neal Williams	Poplar Bluff Municipal Utilities										
73.	Individual	E Hahn	MWDSC										
74.	Individual	Ed Nagy	LCEC										
75.	Individual	Paul Crosby	Platte River Power Authority										
76.	Individual	Showin Fu	US Army Corps of Engineers										
77.	Individual	SPP RE Staff	Southwest Power Pool Regional Entity										
78.	Individual	William F. Watson	Old Dominion Electric Cooperative										
79.	Individual	Michael R. Lombardi	Northeast Utilities										
80.	Individual	Shawn Barrett	Michigan Public Power Agency										
81.	Individual	Fred Meyer	The Empire District Electric Company										
82.	Individual	Darryl Curtis	Oncor Electric Delivery LLC										
83.	Individual	Andres Lopez	USACE HQ										
84.	Individual	Peter Yost	Con Edison of New York										
85.	Individual	Bill Keagle	BGE										
86.	Individual	Michael Albosta	SRW Cogeneration Limited Partnership										
87.	Individual	Martin Bauer	US Bureau of Reclamation										
88.	Individual	Bob Mathews	Pacific Gas & Electric Company										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
89.	Individual	Barbara Kedrowski	We Energies										
90.	Individual	Saurabh Saksena	National Grid										
91.	Individual	Sungly Chiu	LADWP										
92.	Individual	Kenneth A. Goldsmith	Alliant Energy										
93.	Individual	Amir Y. Hammad	Constellation Power Source Generation										
94.	Individual	Kevin Cyr	Seattle City Light										
95.	Individual	Steve Newman	MidAmerican Energy Company										
96.	Individual	Bob Case	Black Hills Corporation										
97.	Individual	Jason Marshall	Midwest ISO										
98.	Individual	Steve Toth	Covanta Energy										
99.	Individual	Jon Kapitz	Xcel Energy										
100.	Individual	William J. Smith	Allegheny Power										
101.	Individual	Donovan Tindill	Matrikon Inc.										
102.	Individual	Patrick Stava	Nebraska Public Power District										
103.	Individual	Greg Rowland	Duke Energy										
104.	Individual	Kathleen Goodman	ISO New England Inc										
105.	Individual	David Martorana	Tenaska										
106.	Individual	Doug Hohlbaugh	FirstEnergy Corporation										
107.	Individual	John Falsey	Edison Mission Marketing and Trading										
108.	Individual	Stephen C. Knapp	Constellation Energy Commodities Group Inc.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
109.	Individual	Eric Ruskamp	Lincoln Electric System										
110.	Individual	Randi Woodward	Minnesota Power										
111.	Individual	Kevin Koloini	American Municipal Power										
112.	Individual	Dave Norton	Entergy										
113.	Individual	Christine Hasha	ERCOT ISO										
114.	Individual	John Allen	City Utilities of Springfield, Missouri										
115.	Individual	Rex A Roehl	Indeck Energy Services, Inc										
116.	Individual	Cynthia Broadwell	Progress Energy - Nuclear Generation										
117.	Individual	Dan Rochester	Independent Electricity System Operator										
118.	Individual	Catherine Koch	Puget Sound Energy										
119.	Individual	Ernie Hayden	Verizon Business										

1. **Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.**

   1.a. **BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.**

Summary Consideration:

Many commenters expressed concerns about the inclusion of software and data within the definition of BES Cyber System Component. One commenter observed that the definition should only include devices with routable connectivity. Many observed the laundry list of functions should be removed and replaced with the function that is more specific to the operation of the BES. A number of commenters proposed alternative language for the definition.

The SDT considered these comments and decided to define the term BES Cyber Asset to focus on the "real-time" impact on the "Reliability Operating Services" of the BES, which include those functions performed for the reliable operation of the BES. This definition now provides the foundation for the definition of BES Cyber Systems. In addition, the SDT has included clarification in the definition on the 15-minute characterization of "real-time."

The new proposed definition of **BES Cyber System** is: *One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.*

The new proposed definition of **BES Cyber Asset** is: *A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.*

The SDT has also modified the definition of Cyber Asset to make it more specific to the device and remove ambiguity on the exact nature of what is included in the definition of the Cyber Asset.

#	Organization	Yes or No	Question 1.a. Comment
1.a	WECC		Although this language is directly from the Federal Power Act, describing electronic devices as “hardware, software and data” is redundant and inaccurate. Electronic software and data reside on some type of hardware in all cases. Suggest removing the parenthetical as it is confusing and data is addressed later in the definition and the definition is clearer without it.If data is to be addressed in the standard it should be defined and addressed separately. The word “organized” is imprecise in this context; “Implemented,” “deployed,” or “utilized” may be a better word.The following rewrite is one proposed alternative.BES Cyber System Component - A programmable electronic device utilized in a BES Cyber System.
2.a	BGE	Agree with proposed definition	1.a and 1.b should be reversed. Disposition should be defined.
3.a	Old Dominion Electric Cooperative	Agree with proposed definition	Agreement is under the assumption that the present NERC definition of BES (e.g. =>100 kV) stands.
4.a	Progress Energy - Nuclear Generation	Agree with proposed definition	Define Disturbance
5.a	Florida Municipal Power Agency	Agree with proposed definition	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:”A programmable electronic device which responds to a BES condition or Disturbance, or enables control and operation of the BES.”For the following reasons: (i) “one or more” seems to

#	Organization	Yes or No	Question 1.a. Comment
			describe a system, not a singular component; (ii) we do not understand how “data” can be a component; and (iii) we do not understand the value of the “laundry list” of things components do and believe the focus should be on how the component impacts the BES.
6.a	Bonneville Power Administration	Agree with proposed definition	Greatly improved. Use of "...which respond..." clarifies that the standard is talking about control systems. However, please leave the parenthetical "(including hardware, software and data)" out. It is a bit confusing since data can't do any of the things listed. By definition a cyber system is made up of the hardware, the software and the data that allows it to operate. It appears that the punctuation in this definition is incorrect. We suggest:”One or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data which respond to a BES condition or Disturbance or enables control and operation.”
7.a	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
8.a	National Grid	Agree with proposed definition	National Grid agrees with the definition but seeks clarification from the SDT if the examples cited below will be considered as BES Cyber System Component:1) As part of the Burn Management System (BMS) in the power plant, the programmable PLC device is used along with the connected thermo-couples to monitor the temperature for fuel burning. If the temperature readings are wrong, the PLC can be programmed to take action to increase the fuel input or to limit/shutoff the fuel. This could have an immediate or short term effect (within 15 minutes). The amount of fuel determines what the output of the unit will be. Is the PLC or the entire BMS (including the PLC) BES Cyber Component? 2) Generating plant connects to Transmission Substation. There are programmable microprocessor relays installed within the substation for power plant / transmission line protection. Are these microprocessor relays BES Cyber Components?

#	Organization	Yes or No	Question 1.a. Comment
			3) The new BES Cyber System Component could also include the Exciter system that exists at Northport PS. Once again, could the PLC or the entire system, including the computer, be part of the BES Cyber Systems? 4) Another system that potentially could be included under the newer broad definition would be the Precipitator Rapper system. This system has a PLC that handles the Rappers. The system is not critical to Operations, however, under a broad definition that includes the 15-minute rule, if the Rappers failed, the unit(s) could be limited due to environmental compliance. The Precipitator Rappers are not connected to any network and are isolated.
9.a	Dairyland Power Cooperative	Agree with proposed definition	Shorten the name to BES Cyber Component.
10.a	Reliability & Compliance Group	Agree with proposed definition	The definition is O.K. Need to add BES to Disturbance and BES to enable control and operation. It would be more helpful if the definition “BES” were included in this document
11.a	Black Hills Corporation	Agree with proposed definition	The definition should include tie back to “BES Cyber System” as inserted above.
12.a	FEUS	Agree with proposed definition	The drafting team should consider clarifying; or enable or control and operation "of BES" or "greater than xxkV" This could be interpreted as an RTU in a 13.8kv sub serving only customer load.
13.a	PacifiCorp	Disagree with	: PacifiCorp agrees with EEI’s suggested alternative definition::BES Cyber System Component - One or more programmable electronic devices (including hardware)

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems o media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to the reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance the reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. In addition, the definition of "programmable" should be provided. Is a device that is "set" considered to be programmable?
14.a	Allegheny Energy Supply	Disagree with proposed definition	1) Does this definition need to cover more than a single device since a BES Cyber System is a collection of these? 2) Software and data should not be included in this definition. Protection of the software and data should be included in security requirements but not in the definition itself. Additionally these are both terms that are easily interpreted in different ways.3) It is difficult to get a clear understanding of what the terms "disposition" and "maintenance" mean in this context.4) Suggest: BES Cyber System Component - A programmable electronic device (including hardware), that is part of a BES Cyber System, providing input/output, processing, information storage, communications, human interaction (display, trending, alarming / alerting, input, etc.),

#	Organization	Yes or No	Question 1.a. Comment
			or maintenance, which is necessary for a BES Cyber System to fully perform its function.
15.a	Consultant	Disagree with proposed definition	1. Inclusion of the word 'communication' would seem to imply that communication equipment is included in the definition. Should be clarified to clearly state what aspects of communication, if any, is included.2. A 'component' would seem to be inconsistent with 'organized for the...' A component performs an activity, the 'system' would consist of 'components organized for the...'3. Software and Data are not programmable devices. Device implies hardware; if software and data are to be included the component definition should be clarified. What is software in terms of the definition? Operating system, application, database, word processing, executable files, scripts, and batch files...4. Component is singular - programmable electronic devices is plural. This is inconsistent. Suggest identifying a component (hardware, software, or data) as singular terms.5. I think "data" should be removed from this definition. Suggested new definition: BES Cyber System Component: hardware or software that performs one of the following functions (1) input, (2) processing, (3) storage, or (4) output of data that enables control or operation of a BES Cyber System.5.BES condition has no meaning. It is not a defined term, and therefore is vague. Suggest removing this wording or clarifying the intent.6. "... enable control or operation." - Of what, and when. All the time or only during a Disturbance? Needs clarification of the intent of this phrase.7. devices... for... display of data..." It is unclear how a display device could be compromised resulting in a degradation of the BES? 8. There is published literature that addresses the concepts of Cyber-Physical Systems that distinguishes between 'hardware components', 'software components', and 'bridge components' as the makeup of cyber-physical systems. This would appear to be a better framework for defining components than the listing of multiple functions, which dims the "bright lines" for consistently defining and categorizing the many variations and configurations within the industry.
16.a	Progress Energy (non-Nuclear)	Disagree with proposed	1. We feel programmable electronic devices is too broad. Also, it seems that there should be a distinction between firmware versus a traditional OS.2. From a generation perspective, these would be likely be in scope and shouldn't be - foundation field bus, device Net, smart transmitters (Rosemount), RS232/485 Serial connections and

#	Organization	Yes or No	Question 1.a. Comment
		definition	electronic protection relaying. We need to know if this would include DCS “Smart” field instrumentation using non-routable network protocols such as Foundation Fieldbus, DeviceNet, Hart, etc. Just about every instrument connected to plant automation system is a programmable electronic device. Per CIP 11 definitions of routable and non-routable they would be considered non-routable. We need examples of components included and components that would not be included. Possibly include examples for generation facilities, ECC’s and transmission. This could include Generator Protection Panels, PLC’s, EX2000 Generator exciter, Bentley Nevada vibration system, Medium Voltage Switch gear protective relays, motor protection relays, etc, etc. These are all “Programmable” and can be accessed via non-routable, ISO layer 1&2 hardware programming by MODBUS. All these devices are already INSIDE the protected Electric and Physical perimeter umbrella.3. The Standards definitions still seem to still be written to traditional PC and IT Business platforms. The standards need to be written to target single use industrial control systems.4. Based on this definition a microprocessor relay associated with a transmission line would be in consideration as a cyber component. If a device has burned in programming, maybe it is considered but classified low impact. User programmable devices may be a higher impact. Many programmable devices may not support use banners. Redundancy will not allow us to remove devices from scope.5. This reads like an ‘or’ definition. In that case, communication connectivity is not required for a device to be considered as a cyber system component. That needs to be very clear since with past standards we were evaluating based on external connectivity and routable vs. non-routable protocols.6. What constitutes a BES "condition"? 7. If definition is limited to the "organized" Cyber subsystems (e.g. 1.b. below) we can work with that. Attachment II appears to define the impact per Cyber System not component level. Suggest removal of component level definition and focus on system level issues.8. Proprietary protocols should not be included.9.Need clarification on what ‘programmable’ means. Recommended definition: Capable of dynamically accepting a sequence of operations to be automatically performed (a device which includes only firmware defined logic which cannot be dynamically changed - such as an EPROM - would not be included). Consider clarification between

#	Organization	Yes or No	Question 1.a. Comment
			programmable and configurable.10. Strike “one or more” because “one or more” implies a system not a component
17.a	Platte River Power Authority	Disagree with proposed definition	A “System Component” should be singular. For example: BES Cyber System Component - A programmable electronic device (to include the hardware, software and data) used for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which responds to a BES condition or disturbance; or enables control and operation.
18.a	LCEC	Disagree with proposed definition	A BES Cyber System Component should not be described as "One or more". Systems can contain more than one component but components should not consist of more than one device. Enable control and operation needs to describe what is being controlled or operated.
19.a	USACE - Omaha Anchor	Disagree with proposed definition	A) This definition could include phone systems - which according to the committee were not meant to be included in this standard. Has any thought been given to an exclusion table or specifically excluding telephone systems? B) Has any thought been given to separating out classification by operating system (OS)? - Ex. Windows, Unix, Solaris - high OS; PLC - low OS or general computing device. We are still going to have TFE issues with a lot of the low OS components.
20.a	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: Question 2 indicates that the definition of BES Cyber System bounds the scope to real-time operations systems, yet it is not clear from the proposed definition of BES Cyber System Component. Consider revising to:”One or more programmable electronic devices (including hardware, software and data) organized for the real-time collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.”Lastly, the term “organize for” should be clarified by description such that a set of one-or-more programmable electronic devices constituting a BES Cyber System Component may be treated as a single system with respect to the application of requirements in CIP 011-1. This would preclude a debate

#	Organization	Yes or No	Question 1.a. Comment
			about how far down into an electronic device(s) the analysis must be performed. For example, a device with two programmable logic controllers on a single board may be treated as one BES Cyber System Component rather than individually as two BES Cyber System Components. Another example might include a turbine control system with vibration monitors. The collection of programmable electronic devices supporting the turbine control system including the monitors is a single BES Cyber System Component.
21.a	NextEra Energy Corporate Compliance	Disagree with proposed definition	At the workshop the drafting team requested that the industry point out comments that move the Version 4 forward, and any fatal flaws. The comments of NextEra Energy (and its affiliates, which include NextEra Resources and Florida Power & Light Company) (NextEra) will focus on constructive comments and fatal flaws. At this time, it appears that CIP-010 does not provide the proper foundation to build a CIP Standard that is well defined, so that the industry, the Regional Entities, NERC and FERC can all understand what is being protected, what is not being protected, or what should be protected via CIP-011. CIP-010 is thus fatally flawed. It is our opinion that CIP-010 should not offer the industry, auditors and regulators such flexibility to second guess each other, which is seen currently. Rather CIP-010 should have very clear definitions of what is the Control Center, what are the Transmission and Generation Cyber Systems that need to be protect and what are the BES Cyber System Components that must be protected for the identified Cyber Systems associated with Control Centers, Generators and Transmission. The flexibility protective options and performance based approach should be in CIP-011. Accordingly, NextEra requests that the drafting team develop a specific definition of what is and is not a BES Cyber System for Control Centers, for Generators, for Transmission - and list for each the BES Cyber Components that need to be protected in each. Given the short period of time from the workshop to these comments, NextEra was not able to propose definitions or lists, but NextEra will be working such and proposing them in the future. NextEra strongly recommends that the drafting team reconsider its flexibility approach in CIP-010 and requests, from the industry, specific definitions of what is and is not a BES Cyber System for Control Centers, for Generators, and for Transmission and a list for each of the BES Cyber Components that need to be protected in each. In this spirit, NextEra recommends the following edits.BES Cyber

#	Organization	Yes or No	Question 1.a. Comment
			System Component - A programmable electronic device (including hardware, software and data) listed below. At Control Centers, BES Cyber System Components are:(List)At Transmission Facilities, BES Cyber Systems Components are:(List)At Generation Facilities, BES Cyber Systems Components are:(List)
22.a	BCTC	Disagree with proposed definition	BCTC does not consider this a good definition as more clarity is required. The following are specific areas where BCTC feels the definition should be revised: - removal of the word “communication” “software” and “data” are not programmable devices. Their placement within the definition is confusing The definition is very “loose”. BCTC would like the definition to be more clear as to what is a cyber system component (i.e. must such a component have a routable protocol, etc.) - right now we find it difficult to grasp this concept based on the current definition When referring to BES System Components (and BES System) clarification is required as to whether we are referring to just ‘production’ environments; development or quality assurance environments are excluded from scope? If you have components of the BES Cyber System (i.e. EMS) which are considered LOW impact, can you segregate/ isolate these devices on a separate network segment w/ firewall so that these components remain categorized as LOW or must everything be considered HIGH impact if any of the components are classified as HIGH?
23.a	Manitoba Hydro	Disagree with proposed definition	BES Cyber System Component” definition needs to be clarified. The defining characteristics of the device should be clearly enumerated by using appropriate punctuation. Placement of semi-colons is confusing as drafted. Example: “A programmable electric device that: (a) is organized for the collection of... and (b) either: (i) responds to a BES condition or Disturbance; or ii) enables control and operation.
24.a	Luminant	Disagree with proposed definition	Better definition on "Data” should potentially be limited to the hardware that stores the data and not the data itself. This should exclude Black start radio systems and in plant personnel communications systems such as 450 Mhz radio systems. The semicolon after Disturbance should be removed.

#	Organization	Yes or No	Question 1.a. Comment
25.a	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.a	ERCOT ISO	Disagree with proposed definition	Consider: "One or more programmable electronic devices (including hardware, software and data) designed for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
27.a	Tenaska	Disagree with proposed definition	Data integrity is out of scope because SCADA, EMS and DCS systems have software to recognize bad data. Also the display of data should be out of scope there are BES Cyber System Components that if compromised will not affect the reliability of the BES i.e. PI historian's. The Pi Historian is used to display and store data and is not used respond to a BES condition or Disturbance; or enable control and operation.
28.a	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	Data should not be included as part of a device. Communications paths should not be included.
29.a	US Army Corps of Engineers, Omaha District	Disagree with proposed definition	define term disposition [of data]
30.a	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	Delete the term BES condition from the definition.

#	Organization	Yes or No	Question 1.a. Comment
31.a	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	Delete the term maintenance and condition from the definition. The term maintenance, as used in the BES Cyber System Component statement, does not have direct impact to the reliability of the BES. Define the term disposition and describe how it applies to BES Cyber System Component.
32.a	CenterPoint Energy	Disagree with proposed definition	Disagree - CenterPoint Energy believes the definition should include a reference to an external communication connection. A disconnected cyber system component is secure. An unintended consequence of this definition may be that entities will install communication connections to isolated cyber system components to remotely manage access requirements of the standard. This defeats the benefits of isolation as a security measure. This definition as currently written would also include programmable electronic devices located in control cabinets mounted on yard equipment within the substation yard. Applying certain requirements of the current draft standards to such equipment is extremely problematic.
33.a	E.ON U.S.	Disagree with proposed definition	E ON U.S believes one or more electronic devices used exclusively to display data should not be considered a BES Cyber System Component
34.a	FirstEnergy Corporation	Disagree with proposed definition	FirstEnergy Summary Response: FirstEnergy (FE) appreciates the hard work of the CIP Standards Drafting Team in developing the version 2 CIP standards and the quick implementation of Commission directed changes reflected in version 3 CIP standards. FE strongly supports the work of the CIP SDT to develop further enhancements to the cyber security standards that improve reliability while providing clarity and certainty. Protecting and guarding against unauthorized access to cyber systems used in the protection and control of the bulk electric system is a reliability priority that FE shares. It is clear that the NERC CIP standards drafting team's fundamental approach is well-intentioned, but will result in a significant diversion of resources away from making concrete, tangible enhancements to the existing framework of cyber protections. FE

#	Organization	Yes or No	Question 1.a. Comment
			fundamentally endorses enhancements to the critical infrastructure protection standards that improve security, clarity, and certainty, but strongly believes that wholesale restructuring of the existing CIP standards is not necessary and may be counter-productive to those goals. While there are some that conclude it is not feasible to sufficiently enhance the underlying approach embodied in the existing CIP standards, these conclusions disregard the considerable investment in people, tools, and processes to address these requirements that would be abandoned in favor of an alternate formulation. Building from the existing CIP approved standards and implementation investments, while strengthening the standards to provide needed clarity and certainty offers a far expedited path to enhance cyber security, also providing greater confidence in the strength of the cyber protections in effect across the industry. A fundamental aspect the SDT proposed abandoning is the Critical Asset determination approach in favor of a wholesale impact categorization structure that introduces different terminology, concepts, and uncertainties, while offering little added clarity. We support the teams guiding principles - leveraging investments in current standards, minimizing the need for TFEs, reducing administrative overhead, etc. - however the proposed standards do not seem to practically meet the primary need for BES security. The key guiding principal for the enhanced cyber standards is clarity to which assets of the bulk electric infrastructure require cyber risk protection. The impact categorization depicted in Attachment II is a significant improvement in achieving a consistent approach for determining high impact critical assets representing the backbone of the bulk electric system. FE encourages the drafting team to focus its efforts on further developing Attachment II to obtain industry consensus on high impact assets and incorporate the work into the existing CIP-002 for consistent Critical Asset determination. To the extent essential, this work could further be integrated within the existing standards to determine another category of less-critical assets to the security of the BES, requiring respectively lesser degree of cyber security protection. Enhancing bulk electric system cyber security does not require a paradigm shift from approaches integrated into existing cyber security programs. We encourage the drafting team to maintain continuity and leverage significant industry investments in implementation of cyber

#	Organization	Yes or No	Question 1.a. Comment
			security protections undertaken over the last half-decade to achieve conformance with the CIP standards. The underlying work of the SDT reflected in the proposed CIP-010 and CIP-011 standards represent important enhancements that can, and should, be integrated with the existing CIP standard architecture, and avoid introducing new set of methodologies, definitions, and requirements that will require virtually every aspect of utility implementation to be restructured - policies, procedures, training, systems, drawings, contracts, data, compliance monitoring tools, forms, etc. These proposed changes offer little improvement in cyber security protection over what can be promptly gained by enhancing the existing standards. While the multilevel categorization is well intended, we believe the maximum security improvements can be more promptly achieved by integrating with the existing infrastructure protection requirements. In sum, FirstEnergy endorses an approach that allows for enhancements of existing implementation that affords more certainty and clarity, and avoids approaches that involve revamping the entire design of cyber protection implementation. Namely, we would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- using the standards drafting team work as an input to the enhancements of the existing standards. Enhance the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure. We appreciate the drafting team's careful consideration of FE's views on the appropriate path forward in further enhancing the bulk electric system protections against unauthorized access to cyber assets. Although FE does not align with the team's overall approach we have thoroughly reviewed the proposed standards and offer constructive feedback to the specific questions asked by the drafting team. It's noted that our individual question responses in many instances do not reflect our primary position of enhancing BES cyber security in a manner that retains the framework and terminology of the existing standards. These responses are provided in order to provide clarity to the extent the concepts may be incorporated into revision of

#	Organization	Yes or No	Question 1.a. Comment
			the CIP-002 through CIP-009 standards. - - - - - - - - - - - - - Question 1.a Response: Suggested alternative definition:"BES Cyber System Component - One or more programmable electronic devices (hardware or software) relied upon to respond to a BES Contingency or Disturbance and supports control and operation of a critical BES Facility."Reasons for suggested changes: o The middle portion of the BES Cyber System Component definition is confusing and provides little value for distinguishing BES Cyber System Components from other components. The terms collection, storage, processing, maintenance, use, sharing, communication, disposition, or display do not add clarity and can be removed to simplify. The inclusion of the term "data" requires clarification. It's not clear how data can be considered a programmable electronic device. FE's proposal removes this term. The term 'BES condition' is vague and open to interpretation. We suggest use of the NERC defined term for Contingency. The team should also clarify for industry if configurable, but non-programmable devices are to be considered as BES Cyber System Components. Also it should be clear that communication media (fiber, wiring) and transport devices (SONET, Microwave, etc) installed between BES Cyber System Components are excluded.
35.a	ReliabilityFirst Staff	Disagree with proposed definition	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, ". . . (including each device's hardware, software and data). . ."
36.a	GTC & GSOC	Disagree with proposed definition	GTC and GSOC are concerned that there may be a component of a BES Cyber System which does not meet this definition of a BES Cyber System Component. If the intent is to apply a cyber security control to a BES Cyber System Component, the SDT should be careful that the definition indeed captures all of the individual devices that make up a BES Cyber System. We recommend the following definition. "A programmable electronic device (including the hardware, software and data necessary for the proper performance of its function) necessary for a BES Cyber System to perform its core functions."

#	Organization	Yes or No	Question 1.a. Comment
37.a	Matrikon Inc.	Disagree with proposed definition	I agree with this definition, but ask for a label/definition/category for those cyber systems that do not “respond to a BES condition or Disturbance; or enable control and operation” as they will exist in the field and will need to be labeled consistently across different entities/regions. Case and point, Responsible Entities could call them “Cyber System Components” or “Cyber Components” or “Discrete Cyber Assets” or “Cyber Assets”, all having the same meaning but different label for the Auditors to understand. I understand it is not a priority for the SDT to label those cyber assets not subject to NERC CIP compliance, but it would provide consistency for labeling those systems which have been evaluated, and confirmed no relationship to the Bulk Electric System.
38.a	American Municipal Power	Disagree with proposed definition	I disagree with the definition on the terms that it may introduce unnecessary or inappropriate interpretations.
39.a	Southwestern Power Administration	Disagree with proposed definition	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
40.a	Wolverine Power	Disagree with proposed definition	I have a concern relating to the definition of "BES generation" vs. "BES transmission”. The NERC definition for BES transmission is clear (100kV+), but NERC defers to each regional entity to define "BES generation “Acknowledgment of the regional entity's right to define what constitutes "BES generation" is important to the application of CIP-010 and CIP-011:As I read the standard, any generation determined to be "BES" in CIP-010/-011 must then automatically be categorized as "high, medium, or low" critical impact (per Attachment 2 of CIP-010). - Even the "low" impact introduces and mandates several cyber controls be in place. So my question is: (How do you objectively determine if specific generation resources really have a material effect on the BES? Some situations are obvious (reliability "must-run" resources on the grid for example) - But just because

#	Organization	Yes or No	Question 1.a. Comment
			a generation facility eventually interconnects with BES doesn't necessarily mean it's material to the BES. So the question of what constitutes "BES generation" is an important to clarify with respect to the application and ramifications of these proposed standards. Proposed Solution: Make reference to (explicitly mention in the standards) each regional entity's definition of "BES generation". In RFC's case, BES generation is defined as: (1) individual generation resources larger than 20 MVA or a generation plant with aggregate capacity greater than 75 MVA that is connected via a step-up transformer(s) to facilities operated at voltages of 100 kV or higher. This provides necessary clarity with respect to applying these standards. Generation listed as "blackstart" for a small TOP's restoration plan isn't necessarily material to the BES just because it can be argued that it eventually interconnects somehow with the BES - Clarity and bright line definition of BES generation is important to interpretation of this standard. The regional entities have provided clarification, and it should be acknowledged in these standards.
41.a	Green Country Energy	Disagree with proposed definition	I suggest adding "primary level" to the phrase enable control and operation. So that it would read enable primary level control and operation. I also request a definition of "respond to a BES condition" from a generator operator perspective.
42.a	Lincoln Electric System	Disagree with proposed definition	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
43.a	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET,

#	Organization	Yes or No	Question 1.a. Comment
			Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the Bested terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
44.a	The Empire District Electric Company	Disagree with proposed definition	Please consider the more simple definition: BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
45.a	US Army Corps of Engineers	Disagree with proposed definition	Please define the term disposition [of data].
46.a	Puget Sound Energy	Disagree with proposed definition	Puget Sound Energy feels that "as owned or operated by the entity" needs to be added to the definition. As the definition is currently written, the standard could be applied to telecommunication links (or the Internet) that are completely out of an entity's control to implement requirements mandated in CIP-011. Also please provide examples of how "data" is a "programmable electronic device". It seems that the hardware and software

#	Organization	Yes or No	Question 1.a. Comment
			can be programmable, but the data itself must actually reside on hardware so it's unclear how to consider it a component solely by itself.
47.a	Madison Gas and Electric Company	Disagree with proposed definition	Recommend that the word "Disturbance" be removed from the definition since the NERC definition broadens the full meaning of BES Cyber System Component. A BES condition contains both normal and emergency statuses of the BES and a disturbance is a sub component of a BES condition (taking a normal condition to an emergency condition). Disturbance reporting is currently contained in EOP-004-1 and the reporting requirements of EOP-004-1 go beyond this Project and will lead to more confusion and redundancy within the NERC Standards. Recommend that the modifier of BES be added to "or enable control and operation of the BES". Recommend changing the phrase, "display of data" to "display of data about the BES" as it is BES data and BES operation that are of interest. The new definition should read: One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of BES data; which respond to a BES condition; or enable control and operation of the BES.
48.a	Hydro One	Disagree with proposed definition	Recommend the following definition - "A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System".
49.a	ISO New England Inc	Disagree with proposed definition	Recommend the following definition - A programmable electronic device (including hardware and software) utilized as a part of a BES Cyber System.
50.a	Northeast Power Coordinating Council	Disagree with proposed	Recommend the following definition - A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System.

#	Organization	Yes or No	Question 1.a. Comment
		definition	
51.a	San Diego Gas and Electric Co.	Disagree with proposed definition	SDG&E recommends removing “data” and “display of data” from the definition because these terms are too vague and can potentially include many devices that should not be in-scope with these Standards (TV Monitors, strip chart recorders, digital displays, and other lower-level devices that have very little or no impact on cyber security or the reliability of the BES).SDG&E recommends the removal of the term “enable control or operation”. This seems vague and may unnecessarily roll up isolated devices (especially at substations or at Generating stations) that “enable control and operation” but have very little to do with the reliability of the BES. Many of these devices are isolated and have a very low risk of impacting the reliability of the BES.SDG&E also recommends the removal of the terms “collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data”. These terms do not help to clearly identify in-scope components and just confuse the issue as entities brainstorm all the nuances of those terms. In exchange for removing the terms identified above, we are suggesting a new revised definition for BES Cyber System Component. The centerpiece of our new suggested definition revolves around the use of a routable protocol or dialup connection, which has strong ties back to CIP-002-2 and contains terms that compliant entities are already familiar with. Suggested Revised Definition for BES Cyber System Component - One or more programmable electronic devices utilizing a routable protocol or dialup connection (including software) which is used to monitor, control, or operate the BES. In addition to revising this definition, SDG&E also recommends that the drafting team release a document (perhaps a FAQ or Guideline) that steps through examples for various entities to show what devices / facilities would be in-scope with the requirements in CIP-010. We suggest this because we believe that the current Standard as proposed will bring an enormous amount of components and systems into scope that will require substantial resources to be compliant with the Standard. Will the reliability of the BES increase by the same substantial amount?
52.a	Regulatory Compliance	Disagree with	Some components such as the display of data may not impact real time operation. More

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	clarification is needed or strike the display of data from the definition.
53.a	IRC Standards Review Committee	Disagree with proposed definition	Some devices may meet the definition of BES Cyber System Component, particularly "enable control and operation" but have little to no impact to the BES if unavailable or compromised because operators may have alternative means to provide the same functionality. Is the intent of this phrase in the definition to expand the applicability of the term to components that are not related to BES condition or Disturbance? Or is it meant to apply only to those components that respond to BES condition or Disturbance?
54.a	Network & Security Technologies Inc	Disagree with proposed definition	Suggest striking "data" from the proposed definition. Cyber Systems and/or their components perform various operations with data (create it, store it, modify it, send or receive it, etc.), and data is of course fundamental to reliable, computer-aided or controlled operation of the BES, but it is not a "programmable electronic device."
55.a	Entergy	Disagree with proposed definition	Suggest: "or more" should be stricken; 'component' should be singular - a discrete unit. "Or more" is appropriate in the BES Cyber System definition below.
56.a	Allegheny Power	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
			Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
57.a	EEI	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Alternatively, BES Cyber System could be defined before BES Cyber System Component. This would follow a top town approach. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage,

#	Organization	Yes or No	Question 1.a. Comment
			maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. SUGGESTION: Reorder positions to place "BES Cyber System" prior to "BES Cyber System Component", this follows a top down approach. BES Cyber System - A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.BES Cyber System Component - One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. Control Center - A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple sites. Also consider removing the word communications. This would include any connection via leased lines or other third party data circuits.
58.a	Duke Energy	Disagree with proposed definition	Suggested clarifying change as follows: "One or more electronically programmable devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
59.a	Alberta Electric System Operator	Disagree with proposed definition	The AESO would like to see a more detailed definition of "enable control and operation" and a definition of "BES condition".
60.a	APPA Task Force	Disagree with proposed definition	The APPA Task force disagrees with the current definition and would like to point out areas where it can be improved. Foremost, we feel the whole standard revolves around the concept of routable protocol. Since this is a common theme of a number of the requirements we feel this should be included in the definition. Also we think the current definition tries to cover a laundry list of functions which complicates the definition. We provide the following edited version for the drafting team's

#	Organization	Yes or No	Question 1.a. Comment
			consideration: BES Cyber System Component -A programmable electronic device connected via routable protocol, which responds to a BES condition or Disturbance, or enables control and operation of the BES. If the drafting team does not use this version we at least request that adding “connected via routable protocol” be included in some manner in the definition that is used.
61.a	Wolverine Power	Disagree with proposed definition	The concepts of "BES" and "critical", as they relate to generation, need to be revisited and clarified -For example - A BES generator, that is used only occasionally, for peaking purposes, and is not black start capable, may logically be declared as "non critical" using the current NERC CIP guidelines - but under these proposed standards, as I read them, this example might be forced to be considered as "low impact".(low criticality vs. not critical)The existing CIP standards allow for a logical separation between "BES and Critical" (i.e. just because a generator is BES doesn't automatically mean it's critical to the BES - how it's used should be taken into consideration) Under these proposed standards, as I read them, any generation resource identified as BES, automatically must be characterized as "low impact" at a minimum. I believe there should be some language in the standard that 1) takes into account the regional entity's right to define what constitutes BES generation; and 2) Doesn't force a "low impact" by default on any and all "BES" generation, without due consideration of its actual use and true impact on the BES.
62.a	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with proposed definition	The current standard limits its applicability to those systems with routable protocols or dial-up access. That limits the applicability of the CIP standards to those systems that are accessible and therefore vulnerable. This proposed standard will impose the CIP requirements on all programmable equipment regardless of its accessibility to external forces. A cyber system inside a generator accessible only to generator staff is as critical to its function as any pump or valve. The security measures safeguarding the pump and the valve should also be sufficient for the cyber system. Only those cyber systems accessible to the outside world require additional, special security requirements. Similar comments were made by many parties in response to the definitions in the proposed

#	Organization	Yes or No	Question 1.a. Comment
			version 4 CIP standards.
63.a	Southwest Power Pool Regional Entity	Disagree with proposed definition	The definition as written could be read to imply that data is a BES Cyber System Component. Data is not a programmable electronic device; however data can reside on a programmable electronic device. The definition should be clarified to make it clear to the reader that the programmable electronic device includes any software and/or data residing on the hardware. Also, consider changing “or enable control and operation” to “or enable control, operation, and/or situational awareness.”
64.a	MWDSC	Disagree with proposed definition	The definition is confusing with disconnected phrases and will be subject to many interpretations. What’s the difference between a “condition” and a Disturbance? The NERC Glossary defines Disturbance as 3 events which should cover all relevant conditions. The proposed definition may be interpreted to include a condition on a local BES system which will not create a Disturbance to an interconnected system. For example, a relay for a transmission/distribution bank breaker may operate and drop the distribution voltage load connected to that BES substation, but not create any Disturbance to other systems. The term "control and operation" was changed from prior draft to "monitoring and control" -see Attachment I under CIP-010. Also, it is unclear who controls and operates the component. In the extreme, a smart grid meter on a distribution circuit could be a “programmable electronic device” which responds to or enables control of a BES condition by reducing or dropping load. Suggest changing definition as follows: "BES Cyber System Component - One or more programmable electronic devices connected to the BES (including hardware, software and data), organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, and which respond to a BES Disturbance affecting an interconnected BES system or enable monitoring and control of the BES by a Transmission Operator, Generator Operator, or Balancing Authority."
65.a	USACE HQ	Disagree with proposed	The definition is still too broad. The definition includes “software and data” as devices, but when someone thinks of a device usually it is a physical component. I think the intended of the team is to state that the software and the data must be included as part

#	Organization	Yes or No	Question 1.a. Comment
		definition	of the device definition, therefore I suggest changing the definition from a "programmable electronic devices (including hardware, software and data)" to "programmable electronic devices (including its components such as hardware, software and data)". Also, the definition is broad enough that test environments and maintenance devices can be included in the definition. CIP-011-1, page 22, states that "devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System". I suggest that the exclusion of devices "not permanently connected to (the) BES Cyber Systems" be explicitly present in the definition of BES Cyber System Component. Lastly, I suggest that all the definitions, in both CIP-010-1 and CIP-011-1 be present together to make it easier for the reader to understand all the new language introduced to the standards
66.a	Kansas City Power & Light	Disagree with proposed definition	The definition is too broad regarding the application of the data used by programmable devices. The proposed definition would include devices used for system analysis or system maintenance with historical data (e.g. Disturbance Monitoring Equipment (DME)). The important considerations are for those devices for the processing and use of data in the real time control of the BES. Recommend modification of the current definition to: One or more programmable electronic devices (including hardware, software and data) organized for the processing and use of data for the purpose of control and operation of the BES.
67.a	US Bureau of Reclamation	Disagree with proposed definition	The definition needs to clarify that the phrase "or enable control and operations" applies only to Cyber System Components that enable the control or operation of BES Assets. It will also need to define the term BES Assets.
68.a	Exelon Corporation	Disagree with proposed definition	The definition should only contain elements that are directly associated with obtaining and using data in support of reliable real-time operations or a device that would automatically respond to an adverse condition on the BES. Specifically the elements in the proposed definition of storage, maintenance, sharing and disposition should not be included. The display of data is also not needed as the display of data would be covered

#	Organization	Yes or No	Question 1.a. Comment
			by the "use" element. The definition needs to be more definitive with the term "programmable electronic devices" and their potential to impact the BES. The definition should consider whether a device can be controlled or operated via remote communication. Disturbance (as defined in the Glossary of Terms Used in NERC Reliability Standards April 20, 2010) is too vague and casts too wide a net and is not in synch with EOP-004. The term "BES condition or disturbance" needs to be clarified. Exelon has a concern that this definition may be interpreted differently in each region.
69.a	Con Edison of New York	Disagree with proposed definition	The Drafting Team (DT) should not include collection, storage, maintenance, use; sharing, communication, disposition, and display of data in the definition because these components cannot respond to a BES condition and may add ambiguity to the definition. By including these words, the Standard is implying that company networks outside of the EMS (e.g. PI) may be included as BES Cyber Systems. Suggested alternative definition: "Any microprocessor-based programmable electronic device used to enable control and operation of a BES element."
70.a	Electricity Consumers Resource Council (ELCON)	Disagree with proposed definition	The existing standard applies to systems with routable protocols or dial-up access. That limits the application of the CIP standards to systems that are accessible and therefore vulnerable. The proposed new standard will impose the CIP requirements on all programmable equipment regardless of its accessibility by external threats. Only those cyber systems accessible to the outside world require special security requirements.
71.a	SCE&G	Disagree with proposed definition	The language "enable control and operation" needs to be better defined. What constitutes control?
72.a	Indeck Energy Services, Inc	Disagree with proposed	The phrase "which respond to a BES condition or Disturbance" doesn't differentiate a component that takes action directly because of the BES condition or Disturbance and one that takes action when told to do so following a BES condition or Disturbance. For example, an under-frequency relay will take action on its own (e.g. trip) upon measuring

#	Organization	Yes or No	Question 1.a. Comment
		definition	the frequency and time corresponding to its setpoint, whereas, a generating unit without a governor will increase generation when the ISO, RTO or TO requests it to do so following the BES condition or Disturbance. The second system shouldn't be categorized as a BES Cyber System Component based on its action following a BES condition or Disturbance. --------- [suggestion] "One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which independently respond to a BES condition or Disturbance."
73.a	Oncor Electric Delivery LLC	Disagree with proposed definition	The purpose of a "component" is to collect, store, process, etc DATA. Data should not be included in the specification of a "component". It should read, "One or more programmable electronic devices (including hardware and software) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
74.a	LADWP	Disagree with proposed definition	The term "organized" seems to broaden the scope of a BES Cyber System Component to any device that may not be utilized but could be utilized in the BES system. A clearer definition needs to be made.
75.a	American Electric Power	Disagree with proposed definition	The term "programmable electronic devices" is general and vague. For example, based on this definition it is not clear how it will align with transmitters and other microprocessor systems. AEP suggests that the drafting team develop a definition that provides more clarity as to what is to be considered in scope. AEP suggests using the wording of NIST SP800-82 sections 2.3.1 and 2.3.2 to clarify the control system components that need to be evaluated for security controls.
76.a	Public Service Enterprise Group companies	Disagree with proposed	The text in brackets "(including hardware, software and data)" is not clear. These items are not types of "programmable electronic devices". Does a specific piece "software" or "data" collection constitute a "BES Cyber System Components"? This text needs to be

#	Organization	Yes or No	Question 1.a. Comment
		definition	dropped or a clearer definition is required.
77.a	Minnesota Power	Disagree with proposed definition	This definition is generally acceptable, with clarification or correction regarding the following items: o What if the device is not programmable, rather defined to perform one function (i.e., coded in firmware)? These types of devices still could have security flaws. What is meant by “disposition” of data? Disposition of data is typically a maintenance function performed after-the-fact which would not have a real-time impact on the BES. There are corporate system which ultimately receive, display and/or act upon data pertaining to the BES. These are not for real-time operations, and should immediately be recognized as out of scope. This definition should reference “real-time operations” or “BES Reliability” to clarify the intended scope. Minnesota Power recommends the following revised definition:"One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, or display of data which, in real-time, respond to a BES condition or Disturbance or enable control and operation."
78.a	Ameren	Disagree with proposed definition	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. The last sentence "which respond to a BES condition" is too encompassing, and the term Disturbance is also. Also, if “communication” devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of BES Cyber System Component includes “disposition.” This phrase should either be defined more precisely or removed.
79.a	Midwest ISO	Disagree with proposed definition	This definition is overly broad and seems to miss the point that the information technology is there to support the operation of the BES and not vice versa. For example, collection and storage of data does not impact the operation of the BES and should not even be considered unless the facility can be used to control or manipulate the operation. Furthermore, what does it mean to respond to a BES condition? Suggest modifying the definition to: One or more programmable electronic devices (including

#	Organization	Yes or No	Question 1.a. Comment
			hardware and software) organized to enable control, operation and protection of equipment.
80.a	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree with proposed definition	This is a vast improvement over "Bulk Electric System Subsystem," and agrees with the focus on the cyber system up front rather than round about. However, there is room for further improvement. The present proposed definition can include programmable relays with no network connection at all - serial or addressable - to cell phones used to receive SCADA alarms. The main focus of the Standard is to protect BES Cyber Systems that are vulnerable to network/Internet based attack, or infection from malicious software. Secondary is the need for physical protection; however, all critical facilities whether cyber or not in nature need physical protection. Therefore in light of this, restricting to components that are vulnerable to remote attack via a network, the Internet, or the inadvertent infection of malware is advised. It should be recognized that not all programmable electronic devises are subject to "cyber attack," and should be excluded. "including hardware" may fail to clarify what is included; does this include a network and supporting equipment connected to the BES Cyber System Component such as a printer, or does it imply only the programmable electronic device itself? The use of "respond to" implies automatic operations the BES Cyber System performs and the additional qualifiers "control and operation" implies programmable equipment that only supplies monitoring data of the BES is outside the CIP scope. This does not appear to cover the required need for BES operator situational awareness of the electrical condition of the BES, and partially negates the BES Cyber System definition below.CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent.CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
81.a	Pepco Holdings, Inc. - Affiliates	Disagree with proposed	We agree with EEI's comments including the position on software and data. In addition, there seems to be a potential for confusion by including "one or more" in the definition. Because there does not seem to be a clear distinction between BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
		definition	Component and a BES Cyber System, it would seem like a BES Cyber System Component could qualify as a BES Cyber System.
82.a	We Energies	Disagree with proposed definition	We Energies agrees with the EEI Suggested alternative definition and explanation: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
83.a	Garland Power and Light	Disagree with proposed definition	We have concerns about data being included in the definition - Many of the CIP requirements are difficult to document or comply with for the data.

#	Organization	Yes or No	Question 1.a. Comment
84.a	Southern Company	Disagree with proposed definition	We recommend the following definition: One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. This definition should be moved to after the definition of BES Cyber System to reflect a top-down approach. If the list of functions is found to be necessary, communication should be removed or, at least, limited to communication outside the BES Cyber System.
85.a	Alliant Energy	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
86.a	MRO's NERC Standards Review Subcommittee	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
87.a	Constellation Power Source Generation	Disagree with proposed definition	What is the definition of the term “BES condition”? It is not a term in NERC’s Glossary of Terms. It needs a local definition much like other terms have been defined in these standards. Using the definition proposed for a BES Cyber System Component, is the intent to include electronic meters such as Nexus Meters? They do not respond to a BES condition, but they do display data. Constellation’s interpretation would be that they are out of scope, but that may not be the intent of the SDT.
88.a	Verizon Business	Disagree with proposed definition	The definition should be specific to the Bulk Electric System to ensure that it does not include generation facilities used on distribution systems or non-BES facilities. This change could be accomplished by adding to the end of the sentence "... on the Bulk Electric System (>100 kv)."

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Summary Consideration:

Many conmmentors observed that the definition of the 15-minute window was too ambiguous. Others observed that a 30-minute window would be more in alignment with other reliability standards. Many commenters observed that the impact was too vaguely described in the definition, and the scope was too broad.

The SDT has carefully reviewed the 15-minute window and has concluded that 15 minutes was more representative of a real-time impact. Some reliability standards cite 30 minutes as recovery times, others cite 15 minutes. The SDT believes that a 30 minute window may include more systems that would not have a "real-time" effect on the reliability of the BES. The SDT has shifted the BES impact aspect of the definition of BES Cyber Systems to the definition of BES Cyber Assets, with clearer definitions of the impact, with respect to "BES Reliability Operating Services", and specific reference to BES "real-time" reliability operations.

The new definition of **BES Cyber System** is:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 1.b. Comment
1.b	BGE	Agree	1.a and 1.b should be reversed.
2.b	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:"One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, or restrict control and operation of the BES within 30 minutes."For the following reasons: (i) see comments to Question 2 for time considerations; and (ii) including that phrase loss of situational awareness is superfluous since it restricts control and operation of the BES and is therefore included in that term.

#	Organization	Yes or No	Question 1.b. Comment
3.b	Puget Sound Energy	Agree	Generally agree, however it is unclear how to use the 15 minutes very meaningfully and how that will be tested in an audit.
4.b	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
5.b	Green Country Energy	Agree	Please define "affect situational awareness"
6.b	Reliability & Compliance Group	Disagree	: There needs to be more clarification about what it means to “restrict control and operation.” If you lose backup control, does this restrict control and operation if you still have primary control? Also, provide a definition of situational awareness in the standard at this point and capitalize the term.
7.b	Oncor Electric Delivery LLC	Disagree	“Systems” are categorized as high, medium and low, entities will tend to identify “Cyber System” at the lowest level possible. We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems.
8.b	Indeck Energy Services, Inc	Disagree	1) The phrase “if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause” is too broad with the word “could”. The proper standard should be “is highly likely to cause.” 2) Situational Awareness is defined as the state of the BES. If this means that it includes systems and data used in the State Estimator, then it should specify that. The more specific the definition, the more certainty that BES ALR will be assured. 3) In FERC Order 706, NERC was required to “provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset.” The only guideline that this definition provides is that the Cyber System could cause a disturbance. Spread across the nine Functions in Attachment I, this is patently incomplete as guidelines. For each of the Functions, some basis for a risk assessment should be outlined. [suggestion] “As to function Controlling Voltage (Reactive Power), any BES facility (asset) capable of providing <100 MVARS is not a BES Cyber Asset as to this function.” 4) [suggested replacement language] "As determined through the application of the Registered

#	Organization	Yes or No	Question 1.b. Comment
			Entity's risk based assessment methodology, one or more BES Cyber System Components which, if rendered unavailable, degraded, compromised, or misused, is highly like to cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
9.b	Progress Energy (non-Nuclear)	Disagree	1. Need a better statement of what 'within 15 minutes' means. Is 15 minutes considered real time operation? Most disturbances will occur in milliseconds. Is there a basis for 15 minutes? A malicious code could lie dormant for extended periods of time, but if activated may have an immediate impact. The term misused is very subjective and may need clarification. The 15 minute window may be good in that it possibly excludes equipment such as circuit breaker hydraulic, pneumatic and gas systems which may cause a breaker to be removed from service but not within 15 minutes. 2. With the 15 minute definition and using organized subsystem concept from 1.a. we can design Cyber (sub)Systems' delineation to effectively minimize impact on BES (see question 7 below). Limit Medium, High impact to a select few subsystems with the rest Low impact. Alternatively the entire plant control system would be viewed as one large Cyber System (High Impact) with the resultant full CIP requirements.3. Rules regarding redundancy need to be clearly defined. The 15 minute window brings redundancy into the picture.4. Need clarification of the terms 'compromised' and 'misuse'.5. Need to know if this would include DCS networks that do "batch" (non-continuous) type control. Some examples would include coal/limestone/gypsum conveying, limestone slurry processing, etc. These processes have inherent storage capabilities that far exceed the 15 minute rule.
10.b	Consultant	Disagree	1. The term would appear to imply that the "one or more BES Cyber System Components" perform a function related to the BES, for example, voltage control, generation control, transmission control, etc. The definition does not appear to address a "Cyber System", it appears to address just a "pile of components". If the answer is just the impact as it applies to a "pile of components", then this term would seem unnecessary as the "pile of components" is covered by the BES Cyber System Components term. It would seem that this definition should distinguish between

#	Organization	Yes or No	Question 1.b. Comment
			components, such as multiple desktop computers and servers as individual devices and their installed software (BES Cyber System Components), and the collection of those components networked and programmed to function as an Energy Management System (BES Cyber System).2. This clarification then raises the question whether the threat ("degraded, compromised, or misused") is a threat to components or a threat to systems. If the component is threatened then the system is threatened, but is there a mechanism to threaten the system without threatening the components? 3. This clarification would have an impact on the methodology for identifying affected assets.
11.b	Entergy	Disagree	A) How is “restrict” defined? How will this be audited? Suggest: Consider deletion B) Many things can “affect” situational awareness of the BES? Suggest “could...adversely affect.” C) How much loss of situational awareness does it take to adversely affect the BES? We lose it all the time and keep on running (e.g., temporarily using state estimators) Suggest: Consider deletion D) How much of the BES is at issue? Suggest: “...could, within 15 minutes, cause a Disturbance in that part of the BES falling under the aegis of the Responsible Entity.”
12.b	Nuclear Energy Institute	Disagree	Agree with the exception that: The word “could” is ambiguous. Propose changing could to would. Additionally, this definition does not maintain alignment with the definition of “reliable operation” provided in Section 215 of the Federal Powers Act: “The term “reliable operation” means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” The definition of BES Cyber System should be revised. An acceptable definition would be:”One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” Lastly, it should

#	Organization	Yes or No	Question 1.b. Comment
			also be clarified that a single facility may have BES Cyber Systems that have different impact categorizations. Upon initial read, it would seem that if the one system in a generating station has a power capability of 2,000MW, then every BES Cyber System at the station is High Impact, which is inappropriate.
13.b	GTC & GSOC	Disagree	Although we appreciate that it is extremely difficult to define this concept, the current definition is too expansive. The phrase "affect situational awareness of the BES" could be interpreted to include the loss of a single status point. Such a minor outage would "affect situational awareness of the BES" but only to a trivial extent. The same could be said with respect to control. We suggest an alternative below. In addition, CIP 010 creates the definition above and then qualifies it in R1 to include only the BES Cyber Systems that "enable one or more functions defined in CIP 010 -1 Attachment I". But CIP 011 has no such qualification (except in its purpose statement), so in theory CIP 011 could apply to a more expansive set of assets than CIP 010. We recommend that the qualifications in R1 be incorporated into the definition. The clarification regarding maintenance devices that is currently in the local definition for maintenance devices (R26) should be part of this definition. Finally, the term "owned" is too narrow; theoretically an entity could absolve itself of all CIP compliance responsibility by leasing its systems. As noted in response to question 10 below, perhaps the concept of “responsible for” would be more appropriate than “owns.” We recommend the following definition: One or more BES Cyber System Components which: 1) Performs one of the following functions-Dynamic Response-Balancing Load and Generation-Controlling Frequency (Real Power-Controlling Voltage (Reactive Power)-Managing Constraints-Monitoring & Control-Restoration of BES-Situational Awareness-Inter-Entity Real-Time Coordination, and 2) if rendered unavailable, degraded, compromised, or misused, could, within 15 minutes: (a) cause a disturbance to the BES; (b) restrict control and operation of the BES to the extent an entity can no longer fulfill its obligations under Reliability Standards; or (c) degrade situational awareness to the extent that an entity can no longer maintain an accurate view of the operational status of the portion of the BES it is responsible for. 3) Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered

#	Organization	Yes or No	Question 1.b. Comment
			part of a BES Cyber System.
14.b	BCTC	Disagree	BCTC recommends the following aspects of this definition be revisited: Â reword "within 15 minutes" to "15 minutes or less" the 15 minute threshold is considered adequate for high impact systems but feel that the threshold would not be the same for medium and low impact systems; for low impact systems, for example, the threshold could be as high as 24 hours before any potential impact to the BES would be realized.
15.b	Network & Security Technologies Inc	Disagree	Believe the 15-minute threshold, while intended to distinguish systems required for and/or affecting real-time ops from others, could have a number of unintended consequences. Entities inclined to "game the system" could declare none of their cyber systems would impact the BES if lost or compromised for at least 20 minutes. How would such a claim be verified or disproven? Moreover, wouldn't a 15-minute threshold compel the establishment of cyber security incident response and/or recover plans with an often unrealistic time to complete of 15 minutes? That this is a difficult problem is understood - at a minimum the SDT might consider adding language to CIP-010 and 011 indicating this definition should not be interpreted as requiring a 15-minute recovery time interval for BES Cyber Systems.
16.b	Platte River Power Authority	Disagree	BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a real-time deadline to be missed resulting in a Disturbance to the BES, or restricting control and operation of the BES, or affecting situational awareness of the BES.
17.b	Minnesota Power	Disagree	BES Cyber System should be defined as "physical or logical set of one or more BES Cyber System Components which if rendered unavailable, degraded or compromised, could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES or restrict control and operation of the BES."
18.b	WECC	Disagree	Change "affect situational awareness" to "loss of situational awareness". Also is Situational Awareness defined? The 15-minute criterion seems arbitrary and unneeded.

#	Organization	Yes or No	Question 1.b. Comment
			The ability to negatively impact the BES is an attribute that either exists or does not regardless of time factors. The time element should be removed.Bulletizing the list of impacts would better format the definition.The following rewrite is proposed; BES Cyber System - One or more BES Cyber System Components deployed for: The control and operation of the BES; or Collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data used in control and operation decision making for the BES. These systems, if rendered unavailable, degraded, compromised, or misused could cause one or more of the following; A Disturbance to the BES; or Restrict control and operation of the BES; or o Affect situational awareness of the BES.
19.b	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.b	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree	Comments to Question 1.a above apply here also. Additionally, this definition would be difficult to apply for many entities. For example, how would a GOP determine if a problem at a generation plant would, within 15 minutes, cause a Disturbance to the BES if a BES Cyber System is rendered unavailable, degraded, compromised, or misused? In most cases, our experience with plant trips, equipment malfunctions and forced shoutdowns has indicated no effect on the interconnected grid.Guidance will be needed on how entities who do not operate the BES and do not have access to BES studies can determine if their facility will cause a Disturbance to the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.
21.b	ERCOT ISO	Disagree	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
22.b	Southwest Power Pool Regional Entity	Disagree	Consider changing “One or more BES Cyber System Components...” to “One or more logically related BES Cyber System Components...” Also, is the term “Disturbance” well understood? The three definitions found in the NERC Glossary of Terms (April 20, 2010) use vague terms that may be open to interpretation by the reader. Similarly, the term “affect situational awareness” is sufficiently vague to be unclear exactly what is meant.

#	Organization	Yes or No	Question 1.b. Comment
			Without precise definitions, the entity and auditor may have different interpretations of the terms.
23.b	Constellation Energy Commodities Group Inc.	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Suggest that the time horizon be changed to within 10 minutes to remain consistent with the Area Control Error requirements. As stated in NERC documentation: DCS measures if a control area is meeting its reserve requirements. These reserves include contingency reserve and regulating reserve. The control area must: 1) recover from the contingency and 2) regulate to load changes over the ten minutes, but the control area need not correct control error that existed before the contingency.If the control area or reserve sharing group recovers ACE to zero or to the level of ACE prior to the first contingency within ten minutes of the start of the second contingency then count two contingencies as recovered 100% within 10 minutes. BAL-001-0.1a - Real Power Balancing Control PerformanceIn order to ensure that the average ACE calculated for any ten-minute interval is representative of that ten-minute interval, it is necessary that at least half the ACE data samples are present for that interval.
24.b	Constellation Energy Control and Dispatch, LLC	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon

#	Organization	Yes or No	Question 1.b. Comment
			to directly operate equipment.
25.b	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes this definition is ambiguous. The NERC glossary definition of "Disturbance" is very broad and "affect situational awareness" is also ambiguous. In addition the word “could” as used in “...could, within 15 minutes, cause a Disturbance...” is problematic. “Could”, under what circumstances or what system conditions? Further clarification is required.
26.b	Turlock Irrigation District	Disagree	Disagree because this definition would include communication systems which are currently exempt from the CIP Standards and would therefore represent a major expansion of the cope of the CIP Standards. Was this the intention of the SDT?
27.b	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Disturbance has no metrics in its definition: “1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.” Therefore any “unplanned event that produces an abnormal system condition” on the BES must be included. Coupled with the broad definition of BES Cyber System Component, almost all programmable electronic devices will be included. Consider the following: loss of a programmable relay and its redundant backup will create the loss of protection on the BES facilities it is assigned to; these relays are not networked with any other cyber systems. The loss, say from malicious physical tampering from a disgruntled employee within the substation, is the unplanned event; and the resulting loss of BES transmission protection is the abnormal system condition. Therefore, it appears that the programmable relays must be included as a BES Cyber System even though the only way to compromise these components is through direct physical contact.If the definition of BES Cyber System Component is expanded to include monitoring ability, “situational awareness of the BES” should be clarified to encompass the electrical status of the BES. Otherwise, situational awareness can include video surveillance and security equipment that is programmable. Security systems should not be considered except where they help protect Medium or High Impact BES Cyber System Components and BES facilities. The cell phone

#	Organization	Yes or No	Question 1.b. Comment
			mentioned in 1.a. above is a BES Cyber System if it displays BES alarms. CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent. CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
28.b	National Grid	Disagree	Do not have a clear understanding of the "within 15-minutes" interval to have an impact on the system. It appears that this clause applies only to control operations such as opening and closing of a breaker. In substations where protection and control are integrated it would be possible to make changes that will take longer than 15 minutes to impact the BES. What type of contingencies will be considered for the 15 minute time horizon? (n-1, n-2 or none). Also, many of the cyber systems are programmable devices. The cyber security could be compromised in real time and the detrimental effect can be achieved after a programmed time interval. This issue requires to be addressed in the definition. There is also no link between attachment I and definition of BES Cyber System. Suggest tying attachment I with definition of BES Cyber System. National Grid proposes the following definition: One or more BES Cyber System Components which execute(s) or enable(s) one or more functions essential to the reliable operation of the BES and which, if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness.
29.b	Dominion Resources Services, Inc.	Disagree	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES. In addition, Dominion proposes to replace the phrase "or affect situational awareness of the BES" with "or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator." This modification is reflected in the revised definition below: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable,

#	Organization	Yes or No	Question 1.b. Comment
			degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES; or restrict control and operation of the BES; or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator.
30.b	E.ON U.S.	Disagree	E ON U.S. believes the term "affect situational awareness" is overbroad. E.ON U.S. suggests that this term should be rewritten as "degrade situational awareness." Also, "Unavailable" is not clearly defined. E.ON U.S. believes that it would be helpful if one could determine "no impact" assessments
31.b	Exelon Corporation	Disagree	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..."
32.b	Progress Energy - Nuclear Generation	Disagree	For nuclear purposes the use of the word "component" conflicts with the definition in 1a. A system contains components rather than a component being a system.
33.b	USACE - Omaha Anchor	Disagree	Further clarify Disturbance to the BES - potentially consider "negative Disturbance"
34.b	USACE HQ	Disagree	Given that BES Cyber System is based on the definition of BES Cyber System Components, which I disagree with, I must also disagree with this one. Furthermore, the use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit.
35.b	Southwestern Power Administration	Disagree	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components which control a BES Facility(s) and/or process data for the real time operation of the BES. To define the scope of applicability for the CIP standards, real time is considered to be the operational time horizon of approximately 15 minutes.

#	Organization	Yes or No	Question 1.b. Comment
36.b	The Empire District Electric Company	Disagree	I disagree with the proposed definition please consider the simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components and associated communication network(s), which control a BES Facility(s) and/or gather data for the real time operation of the BES.
37.b	Kansas City Power & Light	Disagree	Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study. Recommend the following definition for consideration: One or more BES Cyber System Components that provide support for facilities that have been identified as critical to the reliability of the BES.
38.b	Ingleside Cogeneration, LP	Disagree	Ingleside Cogeneration, LP believes that this definition is still too vague to make a determination of whether a system meets the threshold of a BES Cyber System and can be assigned a "No-Impact" rating. This is in stark contrast with the "bright line" delineation between High Impact systems and Medium Impact systems provided in Attachment II of CIP-010-1. The components of the definition in question are "restrict control and operation of the BES" and "affect situational awareness of the BES". Both seem to be Control Center concepts and could be interpreted to mean that any system supporting multiple generation or transmission facilities at multiple locations would automatically carry at least a "Low-Impact" rating. However, this does not speak to the associated generation or transmission facilities that may be "No-Impact" if a cyber intrusion cannot cause a Disturbance - a term which is very well defined in EOP-004-1. Ingleside's concern is that recent rulings by FERC concerning the definition of the BES

#	Organization	Yes or No	Question 1.b. Comment
			and the applicability of PRC-023-1 to facilities under 200 kV, indicate they are pushing a stricter level of adherence to Reliability Standards across the board. If this continues, Functional Entities with “No-Impact” systems once considered compliant with CIP-010-1, may be considered non-compliant at a future date. This could lead to the assessment of violations and fines, even though the Standard has not changed.
39.b	Emerson Process Management	Disagree	It could be more appropriate to state that the unavailable component(s) can not be recovered within 15 miuntes.
40.b	Bonneville Power Administration	Disagree	It is not clear that this definition limits the scope and applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems as indicated in Attachment I and Question #2 of this comment form. Situational Awareness is too broad and all the commas in the definition can lead to numerous interpretations of the sentence. Recommend changing the definition to the following: "One or more BES Cyber System Components which if rendered unavailable, degraded compromised, or misussed could, within 15 minutes: (1) cause a Disturbance to the BES; or (2) restrict real-time control and operation of the BES; that could cause a Disturbance in 15 minutes, or (3) affect situational awareness of the BES that would lead to a Disturbance required for real-time control of the BES. "What is real-time operations? To fully understand the definition of a BES Cyber System, the reader must pull out the NERC Glossary for the definition of Disturbance, BES, and ACE. Recommend an explicit definition that doesn't contain words from the NERC Glossary of Terms.NERC defines Disturbance as: 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system; or 3. The unexpected change to ACE (Area Control Error) that is caused by the sudden failure of generation or interruption of load.
41.b	CWLP Electric Transmission, Distribution and Operations Department	Disagree	It is unclear how the 15 minute time frame is to be construed for the purpose of defining a BES Cyber System. The 15 minute time frame appears arbitrary.

#	Organization	Yes or No	Question 1.b. Comment
42.b	FirstEnergy Corporation	Disagree	It is unclear if systems such as HP OpenView or a centralized logging system, which monitor alerts, are outside the scope of a BES Cyber System or if they are considered to affect situational awareness of a BES. As written, the definition could encourage entities to not install alerts so as not to have additional cyber systems. FE proposed change: "... or impact situational awareness that is deemed essential to the reliability of the BES". As an alternate, FE also supports EEI's suggested change to " ... materially disrupt situational awareness of the BES"The SDT should clarify how redundancy may impact the classification of BES Cyber Systems. For example, in a highly redundant architecture, there are many components whose loss would not impact or render essential systems as unavailable.The team should consider leveraging its work in developing the BES Cyber System and BES Cyber System Components to revise the existing Critical Cyber Asset.
43.b	Dairyland Power Cooperative	Disagree	It seems likely that a component could belong to multiple systems. How does this fit with the compliance regulations? Sentences are a little confusing with nested commas... It seems the intent is that 15 minutes applies to causing a disturbance, but it could be argued that it is ambiguous.
44.b	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
45.b	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
46.b	US Army Corps of Engineers, Omaha Distirc	Disagree	Need definitions of "restrict control and operation" and "affect situational awareness. These are very broad. If the intent of the standard is to create groups of cyber system

#	Organization	Yes or No	Question 1.b. Comment
			components and evaluate them based on their impact to system reliability why not state the definition in terms of the impacts. Suggest alternative wording - A Cyber System Component or logical grouping of Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, negatively impact one of the functions essential to the operation of the BES (Dynamic Response, Balancing Load and Generation, Controlling Frequency, Controlling Voltage, Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, other functions as needed).
47.b	Garland Power and Light	Disagree	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good definition and we would agree.
48.b	The United Illuminating Co	Disagree	Not clear if the rendering unavailable, degraded, compromised or misused applies to the Cyber System or to the individual components of the Cyber System.Suggest: BES Cyber System - Comprised of One or more BES Cyber System Components. If a BES Cyber System when rendered unavailable, degraded, compromised, or misused could, within 15 minutes of such act, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
49.b	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested alternative definition:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness

#	Organization	Yes or No	Question 1.b. Comment
			of the BES. In addition, the phrase “situational awareness of the BES” needs some more clarity to derive determine what is intended.
50.b	Public Service Enterprise Group companies	Disagree	Please clarify that the 15 minute threshold means that if the cyber component would not cause a disturbance in the BES, or restrict control and operation, or affect situational awareness, within 15 minutes, the aggregation of BES Cyber System Components is not deemed to be a BES Cyber System and thus out of scope of Version 4.
51.b	Hydro One	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. The SDT should consider 30 minutes instead of 15 as this time is consistent with requirements of EOP-001 and IRO-001.
52.b	ISO New England Inc	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. - Recommend “30 minutes” to align with EOP standards - Please provide background for where the 15 minute recommendation came from.
53.b	Northeast Power Coordinating Council	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of

#	Organization	Yes or No	Question 1.b. Comment
			the BES for the support of real-time operations.
54.b	Con Edison of New York	Disagree	Regarding the BES Cyber System definition, specifically the qualification criteria “within 15 minutes could impact BES operation”, it is not clear how an entity will determine / distinguish which BES Cyber Systems could impact operation within 15 minutes versus which will not. This may be more challenging than distinguishing which Cyber Assets are essential to operation or not, as we do for version 2 of the CIPs. Our understanding is that the purpose of including the 15 minute period is to limit the application of CIP-010 to BES Cyber Systems impacting real time operations. An alternate way to address BES Cyber Systems impacting real time operations would be to look to the existing NERC Reliability Standards. The following definition language is recommended: “The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within the time period established in the applicable Reliability Standard(s), or if no time period exists, within 15 minutes of the BES Cyber System failure.”The following are examples of Reliability Standard citations: Standard BAL-005-0.1b - Automatic Generation Control R6. ... If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator. Standard EOP-001-0 - Emergency Operations Planning R2. The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. ... The load reduction plan must be capable of being implemented within 30 minutes.
55.b	MWDSC	Disagree	Same general comments as for BES Cyber System Component. Also, "situational awareness" is redundant with the "monitoring and control" function as specified in Attachment 1 - see comment to Question 3 and suggested combination of terms. Disturbance reporting is required under EOP-004 - to avoid confusion or a conflict, definition needs a cross reference. Suggest changing last part of definition as follows:"... within 15 minutes, cause a Disturbance to the BES that requires a report pursuant to EOP-004, or affect the monitoring and control of the BES by a Transmission Operator,

#	Organization	Yes or No	Question 1.b. Comment
			Generator Operator, or Balancing Authority.
56.b	San Diego Gas and Electric Co.	Disagree	SDG&E is supportive of the "15 minute" criteria to help focus CIP-010 attention on real-time BES Cyber Systems. SDG&E recommends clarifying the categorization levels in conjunction with the 15 minute criteria, if the architecture or design includes the concept of redundant BES Systems (per Attachment I & II). Example: If a given BES System is potentially classified as a High BES System; but where an Entity has designed and operates a redundant BES System to enhance reliability of the BES Systems; and one which is in place to mitigate or reduce negative impacts to the BES, then the combined redundant system would not meet the criteria of a High BES System. Suggestions include incorporating a third classification category or filter which identifies potential High BES Systems which are treated separately, but have security controls applied.In the definition for a Component, the language states how a cyber system component "responds" to a BES condition or Disturbance or "enables" control and operation, but when talking about the System, a Component is spoken of in terms of a "causing" a disturbance, or "restricting" operation. Why is the piece of the whole (the component) "responding or enabling" yet when used in the context of "the whole" (the system) the piece is now labeled as "causing or restricting"? It is a bit confusing and redundant that a cyber system may also be a cyber system component. SDG&E is not certain what the value is with this level of granularity, and we are not certain that a "system component" definition is necessary. In addition, SDG&E suggests additional clarification on what "affect situational awareness of the BES" means.
57.b	Electricity Consumers Resource Council (ELCON)	Disagree	See comment on 1.a above.
58.b	Wolverine Power	Disagree	See comments listed for 1a
59.b	NextEra Energy Corporate Compliance	Disagree	See comments to 1.a. Furthermore, NextEra questions why there needs to be qualifiers like Disturbance. The industry understands which components need to be protected to safeguard Control Centers, Transmission and Generation. There would be a minimum

#	Organization	Yes or No	Question 1.b. Comment
			list developed that must be protected without qualifiers that could be misunderstood. In this regard, it is recommended that the following approach be adopted: BES Cyber System - A BES Cyber System Control Center, Transmission or Generation as defined in Section XX.
60.b	EEI	Disagree	See EEI's suggested wording in 1.a. Alternatively, EEI suggests: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
61.b	Tenaska	Disagree	Should only say: A grouping of one or more BES Cyber System Components. All other qualifiers should be in tables for Medium and High requirements. Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity.
62.b	Madison Gas and Electric Company	Disagree	Suggest replacing the phrase, "cause a Disturbance on the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" with "cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES." The definition of Disturbance when used in this context is overly broad, for it includes "a perturbation to the electric system" or "the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load." A perturbation to the electric system and a change is ACE are not qualified as to materiality. For example, a responsible entity's programmable device may be used in normal operation to curtail or interrupt relatively small amounts of load; such control of load (even simply for economic reasons) perturbs the electric system and affects ACE to some extent. Yet such effects are part of normal operation of the electric system. In addition, control and operation of the BES are always restricted to some extent; the concern is whether or not control and operation are degraded.

#	Organization	Yes or No	Question 1.b. Comment
			Likewise, the concern is whether or not situational awareness is degraded ("affect" could be in a way that is good or bad). New definition should read: One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES.
63.b	ReliabilityFirst Staff	Disagree	Suggest thefollowing definition: "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could impact realtime operation of the BES such as; cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
64.b	Allegheny Energy Supply	Disagree	Suggest: BES Cyber System - One or more BES Cyber System Components, performing one or more functions essential to the reliable operation of the BES, which if unable to perform its function, is misused, or operated by unauthorized personnel, could within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES that could lead to a BES Disturbance, or affect situational awareness of the BES that could lead to a BES disturbance.
65.b	Allegheny Power	Disagree	Suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
66.b	SCE&G	Disagree	The 15 minute timeframe should be eliminated. There are too many variables in determining whether a system will have a 15-minute impact.
67.b	APPA Task Force	Disagree	The APPA Task force disagrees with the current definition for similar reasons stated above in regard to 1a. We offer the following simpler definition: “One or more BES Cyber System Components connected via routable protocol, which if rendered unavailable, degraded, compromised, or misused could cause an Adverse Reliability

#	Organization	Yes or No	Question 1.b. Comment
			Impact to the BES, or restrict control and operation of the BES for 30 minutes."See comments to Question 2 for time considerations. If the drafting team does not use this version we at least request that adding "connected via routable protocol" be included in some manner in the definition that is used.
68.b	US Bureau of Reclamation	Disagree	The identification of a BES cyber system based on the 15 minute criteria established here could be difficult to ascertain by those entities that do not directly operate or control the BES. Most entities can determine if it could compromize their respective BES assets. Further, this definition, if it does not establish additional qualifying criteria, would generally establish all Components identified under part 1.a., as Cyber Systems. As an example, an isolated single function cyber-based protective relay would qualify as a BES Cyber System Component under 1.a., but it would also qualify under criteria identified here in 1.b., since it is one or more "components" which could cause a disturbance if compromised - irrespective of the fact that it is not tied to any other components. Was this the intent of the drafting team?
69.b	LADWP	Disagree	The relative nature of the 15 minute criteria. What is the definition of a "Disturbance"?
70.b	Manitoba Hydro	Disagree	The term "misuse" in this definition is inappropriate. The definition misuse n. Improper, unlawful, or incorrect use; misapplication. 1. To use incorrectly. 2. To mistreat or abuse. The misuse of an asset describes the type of human action leading an effect on an asset, while the other terms unavailable, degraded or compromise describe more appropriately the state of the asset. The term misuse might lead into the area where analysis of one asset might cause an effect on another asset which is part of the BES Cyber System Component - secondary effects. Rather than using this approach the drafting team should list the types cyber assets which need consideration. i.e. support systems, HVAC, security, etc.) There may be Cyber system components linked to monitoring and/or network control that may operate periodically that could affect BES with disturbances. If there are any Cyber components that are not continuously or periodically (within 15 minute intervals) monitored for operational status that could either create or incorrectly not mitigate a network disturbance when they are

#	Organization	Yes or No	Question 1.b. Comment
			unavailable, they would not fit into the proposed definition. The definition needs clarification to include reference to all normal modes of operation of the BES Cyber System. For example, a protective relay has normal modes of operation of trip and restrain to trip. The 15 minute “real-time” criterion applies to both the trip and restrain to trip modes of operation. If a digital relay which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes of its trip mode or within 15 minutes of its restrain to trip mode (within 15 minutes of any normal mode of operation), cause or fail to mitigate a Disturbance to the BES, or restrict control and operation of the BES, it is a BES Cyber System.
71.b	American Electric Power	Disagree	The terms "situational awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
72.b	Seattle City Light	Disagree	The terms BES condition or Disturbance need to be further defined and clarified.
73.b	LCEC	Disagree	The time frame reference of "Within 15 minutes" could cause a great deal of confusion in identifying BES Cyber Systems. What is the basis for 15 minutes? How will the 15 minute test be audited?
74.b	Ameren	Disagree	The words “A Responsible Entity’s” should be added before the words “BES Cyber System Components” to make it clear that this only includes BES Cyber Systems components under the control of the Responsible Entity and specifically excludes entities such as Verizon. The last sentence the term Disturbance is too encompassing. Consider revising for more exact situations. The flow of the definition is difficult to read.
75.b	Matrikon Inc.	Disagree	This definition calls out those cyber systems that affect the BES in some way. During the application of CIP-010-1 there will be the need to classify and label those cyber systems that do not have any impact on the BES. That is the value of keeping the definition “Cyber Asset”, because it does not care about the relationship to BES

#	Organization	Yes or No	Question 1.b. Comment
			reliability, only to define the types of electronic systems to be evaluated as part of CIP-010-1 R1. My suggestion is to provide a label/definition for those systems that have no affect on BES, and allow "cyber assets" to remain.My second challenge when trying to apply this definition is how a "component" becomes a "system". The security controls of CIP-011 will be applied to individual cyber assets, and evaluating their individual impact on the BES is of ultimate importance. The need to apply the Impact requirements of CIP-011 appropriately will be satisfied when cyber assets share the same boundary access point, and all will have to inherit/conform to the same, and uppermost security controls criteria.In our CIP-002 definitions, we have defined a "system" as a group of cyber assets performing similar and/or cooperative activities in order to support a function. A similar definition can be used to support BES Cyber System, and the difference from BES Cyber System Component.
76.b	Duke Energy	Disagree	This definition is too broad. The phrase "compromised, or misused" could render compliance an impossibility, since administrators must have access to, and could misuse their access. Also, the phrase "situational awareness" should be clarified to include only that awareness required by System Operators to perform their reliability-related functions. Suggested clarifying change as follows: "One or more BES Cyber System Components which if rendered unavailable or degraded, could, within 15 minutes,: cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES required by System Operators to perform their reliability-related functions." Also, It is not clear if there will be any guidance around how 15 minutes threshold should be measured to ensure that numbers of interpretations for this threshold are limited.
77.b	Midwest ISO	Disagree	We agree that the time frame should be limited to the present but question the use of 15 minutes. Real-Time is a term that is included in the NERC Glossary. Why not use this term?
78.b	Pepco Holdings, Inc. -	Disagree	We appreciate the desire of the SDT to narrow BES Cyber Systems to real-time operations and understand the purpose of including 15 minutes to make that

#	Organization	Yes or No	Question 1.b. Comment
	Affiliates		distinction. We are not sure what the appropriate time frame would be and/or if 15 minutes is the correct time. So a Digital Fault Recorder which is traditionally used for after the fact analysis would not fall within the 15 minute window while and EMS/SCADA system which provides alarms and allows control of the BES would fall within the 15 minute window. Would a system that is compromised with a Trojan months or years ago but no action has been taken yet to compromise the BES meet the 15 minute window. Another possible approach is to list the real-time systems that need to be in-scope or considered.Because there does not seem to be a clear distinction between a BES Cyber System and a BES Cyber System Component, it would seem like a BES Cyber System could qualify as a BES Cyber System Component
79.b	Alliant Energy	Disagree	We believe the definition should be revised to: "One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES."
80.b	Independent Electricity System Operator	Disagree	We do not agree with the 15-minute qualifier. Any BES cyber system components that if tampered with can cause a disturbance to the BES or restrict control and operation of the BES, etc. should fall into this category since some components may have an impact on the BES if tampered with by more than 15 minutes before real time. To qualify the components to be only those that affect real time operation, we suggest wording such as "for the current hour and next hour operations" at the end of the sentence. Further, the term "misused" can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
81.b	We Energies	Disagree	We Energies agrees with the EEI Suggested alternative definition with minor modifications: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or

#	Organization	Yes or No	Question 1.b. Comment
			materially disrupt situational awareness of the BES.
82.b	MRO's NERC Standards Review Subcommittee	Disagree	We feel “affect situational awareness of the BES” should be removed, as this is already covered under “operation of the BES”. As written, situational awareness is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for operation of the BES. We also feel “misused” should be removed, as this is already covered under “compromised”.As currently worded, we also believe the intent of the 15 minute time frame is ambiguous. We would propose incorporating what we believe to be the drafting team’s true intent directly in to the definition, along with our other suggestions, as follows: One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES.
83.b	IRC Standards Review Committee	Disagree	We question the technical basis for a 15 minute time frame applied to any component that may cause a “Disturbance” to the BES. Without careful understanding of how the failure of the component could impact the BES 15 minutes may be too long or too short a time frame to allow recovery of the component or enable a mitigation solution. Further, we disagree that the disabling or degradation of any BES Cyber System Component would cause a “Disturbance” that is of significance to the integrity of the interconnected BES. To qualify the components to be only those that affect real-time operation reliability, we suggest wording such as “for the current hour and next hour operations” at the end of the sentence.The term “misused” can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
84.b	Southern Company	Disagree	We recommend the following definition: A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.

#	Organization	Yes or No	Question 1.b. Comment
85.b	Covanta Energy	Disagree	Without a clear understanding of why '15 minutes' is the defined measure, it is difficult to support the definition.
86.b	Verizon Business	Agree	The “15 minute” criterion should be expanded in writing by the drafting team to provide a better sense of when the time starts. This could be done in an associated guideline or “Frequently Asked Question”

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Summary Consideration:

Many entities expressed concerns that the proposed definition of Control Center was too broad and could include various types of facilities not commonly considered control centers. Others questioned whether a Control Center should be defined as a collection of systems versus a physical facility housing such systems. Many entities indicated that the definition should be restricted to the functions of Reliability Coordinator, Balancing Authority, or Transmission Operator. Some expressed concerns about including situational awareness in the definition.

The SDT has modified the definition of Control Center to clarify that it is one or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more functions that support System Operators in the real-time operation of the BES. In consideration of the possible configurations where multiple locations may host such systems, the SDT used 'one or more' facilities. The SDT declined to limit the definition to of Control Center to facilities operated by RCs, BAs, or TOPs, since there are Control Centers operated by TOs and GOs/GOPs as well that must be protected.

The revised definition of **Control Center** is as follows:

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- *Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,*

- *Inter-utility exchange of BES reliability or operability data,*
- *Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,*
- *Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,*
- *Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES*
- *Coordination of BES restoration activities.*

#	Organization	Yes or No	Question 1.c. Comment
1.c	BCTC		BCTC recommends the following aspects of this definition be revisited:Â Recommend the first bullet point be broken into three:ï,§ Supervisory Controlï,§ AGCï,§ Automatic Load SheddingÂ Recommend that the functions be categorized as “mandatory” for defining a facility as a control centre. These would include:ï,§ Supervisory controlï,§ BES and system status monitoringï,§ Alarm monitoringï,§ Coordination of BES restoration activitiesÂ To be considered a control centre the facility should have “two or more” of the functions listedÂ Remove “or” and replace with “and”Â For BES restoration a Utility may have workstations at an alternate site that by our everyday definition is not considered a control centre (i.e. alternate office building); how would these be classified within this definition? One of the questions we struggled with when looking as this definition was how to define a facility based on the number of RTUs present within them (i.e. one versus many) ... any advice?
2.c	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group		With no metrics defining anything upfront, it is possible to include applicability to very small entities. Control of two or more BES generation or Transmission Facilities with a combined historical demand of less than 500 MW should not be included in this definition. At some point, a defining line needs to be established to effectively define the bounds of the BES “castle” where defense of BES reliability is cost effective. Adding undue BES reliability compliance burdens on smaller DP/LSEs will ultimately add no BES reliability, and will hurt local distribution reliability efforts. If 500 MW is too large, then a conservative value can be agreed to and later revised as engineering studies become

#	Organization	Yes or No	Question 1.c. Comment
			available to justify a larger value.If that cell phone from 1.a. receives alarms from two or more locations and is used to make real time decisions it becomes a Control Center although it performs no control function and is not a center. Suggest that a Control Center be defined as a fixed server location.From the workshop, we realize that the lines separating the Component from the System and from the Center were intended to be flexible and up to the entity to consider system designs. The standard, however, does not read that way. We are concerned that based on the written standard the REs will not allow flexibility or even lines. All BES cyber devices, including every BES alarm displaying cell phone will be cast into all three buckets.
3.c	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
4.c	Southern California Edison Company	Agree with proposed definition	SCE requests clarification on systems and components that: (1) facilitate inter-utility exchange; and (2) devices that enable system status monitoring. Would devices such as email systems used for messaging and IP telephony systems in facilities be considered a "control center" or a BES Cyber System? The drafting team should issue guidelines on systems that directly perform BES reliability functions and systems/devices that are used by human operators for feedback prior to the manipulation of cyber components that directly impact the BES. It would also be beneficial for telecommunications equipment, which support a BES Critical Cyber system, be applicable only to COM-001 R2. If the intent of the drafting team is to limit the scope of cyber security controls to systems where real time BES impact is caused by direct human supervisory control over devices and systems, it should be clearly stated as such.
5.c	FEUS	Agree with proposed definition	What would it be considered if it only performed one function for a single BES facility at a single location? It would not be a control center.

#	Organization	Yes or No	Question 1.c. Comment
6.c	Minnesota Power	Agree with proposed definition	While Minnesota Power generally agrees with the proposed definition, it recommends that “(i.e., two or more)” be removed from the definition.
7.c	National Grid	Disagree with proposed definition	1. A control center is usually considered as a physical place with operators using various tools like EMS. The definition implies that a control center is a cyber asset. Isn't the Control Center much more than that? Maybe SDT is trying to define a "Control Center Cyber Asset". If so then SDT should use the term Control Center Cyber Asset. 2. National Grid seeks clarification on "Reliability" or Operability Data" since they can be subject to interpretation. 3. In bullet 3, the asset management piece should not be included. Also, if bullet 3 is indicating statuses like breaker status, then it is not required since it is covered in the preceding bullet. If not, then this should be better defined. 4. In bullet 4, there is no need to include "restoration function" as this is included in "operation" 5. In bullet 5, operators "coordinate" the BES restoration activities and not the cyber systems.
8.c	Progress Energy (non-Nuclear)	Disagree with proposed definition	1. From the definition, the ECC, DCC and the back-up control facilities would definitely be included. A substation that has a LAN connecting several cyber components would not be included. 2. Is a single generating facility the same as a single generating plant? Is a single generating plant a generating unit or a collection of generating units at 1 physical plant site? Clarify that a generating station control room is not a control center. 3. We need to be careful with definition of supervisory control as one possible interpretation of what the control room operator does is supervise the distributed control platforms that make up the plant control system. 4. These systems are independent only controlling one at a time. The key word here is “multiple”. Control rooms at some generation plants house multiple DCS systems. But, by design, each DCS controls its respective unit independently and are considered separate entities. I do not think this example would qualify as a Control Center. We can agree with this concept if they are talking about large regional control like the PJM interconnect or an ECC which it sounds like and NOT plant level Control Rooms. 5. A Control Center would operate

#	Organization	Yes or No	Question 1.c. Comment
			multiple generating Units with one control system.
9.c	Consultant	Disagree with proposed definition	1. The definition should identify that the "set of one or more BES Cyber Systems capable of performing..." are at a single location. If there are multiple locations where this capability exists then each location should be identified as a Control Center. 2. As stated, the definition creates a Control Center at every location where the capability "exists", whether this is a normal operation for each of those locations or is an emergency capability of each of those locations. If that is not the intent of the definition, then the distinction between normal and emergency (backup, off-normal) operations should be included in the definiton.
10.c	Progress Energy - Nuclear Generation	Disagree with proposed definition	A control center at a nuclear facility is different than this definition. I do not belive it is intended to apply to nuclear generation facilities, but rather the energy control centers that supervise bulk power loading functions.
11.c	Dairyland Power Cooperative	Disagree with proposed definition	A control center sound intuitively like a type of facility, but here is used as a term for a system(s) affecting multiple facilities. This will be confusing terminology.
12.c	Indeck Energy Services, Inc	Disagree with proposed definition	A control system that monitors through read-only access should not be categorized as a Control Center under CIP-010. A load aggregator is not identified as a potential Control Center.
13.c	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: The term “multiple locations” should be clarified to “multiple geographically distinct locations” to preclude confusion with a single facility with multiple generating units from being inappropriately identified as a control center.

#	Organization	Yes or No	Question 1.c. Comment
14.c	Alliant Energy	Disagree with proposed definition	Alliant Energy agrees with the EEI comments.
15.c	Pacific Gas & Electric Company	Disagree with proposed definition	Appears that under this definition of Control Center, several BES Cyber Systems or Components would be considered Control Centers such as:Distributed EMS or SCADA front-end processors Transfer Trip Protection Systems located at a specific substation control house that control other subs and/or generationSpecial Protection Schemes that control devices at multiple substations.Don't disagree on the importance of the items above to BES, just that defining them as a Control Center likely will lead to confusion.
16.c	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
17.c	Ameren	Disagree with proposed definition	Clarify the definition to explain if it covers Power Plant control rooms, or if this is limited to transmission dispatching. Please clarify if “locations” refers to physical or electrical locations. Does “generation plants” refer to a Power Plant or generation “Facility” as defined by NERC; there use of plant vs. Facility is inconsistent. The definition appears to automatically cover all plant control rooms for any generator that see’s or controls the switchyard, is this the intent? In the third bullet, the term “and asset management” needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition.The definition of Control Center should only include those facilities where NERC certified operators are required for its operation.
18.c	CenterPoint Energy	Disagree with	Disagree - Control Center is a common industry term that often refers to a physical location. It should not be redefined under the CIP standards and should be deleted.

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	However, if the SDT feels a strong need to include this definition CenterPoint Energy suggest the following: A set of one multiple (i.e. two or more) BES Cyber Systems, located together at the same physical location, capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.
19.c	Tenaska	Disagree with proposed definition	Display and Inter-utility should be left out. Just display of will not hurt the reliability of the BES (PI data). Loss of inter-utility data need to have an N-11 type requirement with it. The loss of some percentage of data is tolerated in normal operation every day. The EMS/SCADA accounts for bad data. Consider using the definitions for Reliability Coordinator and Balancing Authority for clarity.
20.c	E.ON U.S.	Disagree with proposed definition	E.ON U.S. does not believe that the "display of BES reliability or operability data for the support of real-time operations" alone should qualify a locale as a control center. For example, view only information is often made available to plant operators Does "Alarm Monitoring" in the Control Center definition include sending alarms to remote ends of a transmission line from a substation? For example, carrier check-back and breaker failures. In addition how is transfer trip being addressed.?
21.c	Southern Company	Disagree with proposed	EOP-008, which is focused on control centers and control center functionality, does not contain or need a definition of the term. This implies that the CIP standards may not require a definition, either, and that any definition which is constructed must be done in light of the contents of EOP-008.If a definition is needed, we recommend the following

#	Organization	Yes or No	Question 1.c. Comment
		definition	definition:A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple locations.If, for some reason, the existing definition must be modified, the following factors should be taken into consideration:Definition of Control Center - its our understanding that the Control Center definition is to be used to scope requirements based on 'environmental' factors and to differentiate it from generating plants and substations (field locations). So Control Center 'environment' is a 'data center' environment consisting of mostly traditional servers and workstations, Generation environment was a campus, plant type environment, and Transmission is an environment with unmanned field locations and mostly purpose built devices. These environments are then used to scope requirements appropriately based on the types of devices and the physical environment prevalent in that situation. The current definition of control center will pull in devices and systems from all the above environments and loses what we considered was the reason the environments were created and defined.For bullet 2...This clause pulls in far more facilities than are either intended or generally thought of as control centers. Things that would qualify: o An unattended remote data acquisition node o A standalone ICCP server feeding data to neighboring utilities o An RTU receiving data from multiple generating unitsThe definition should be modified to require multiple functions for a facility to qualify as a Control Center, and the second bullet, which includes many facilities which are not actually Control Centers and which does not add any additional facilities which should be considered as Control Centers, should be removed.In general, and in particular on bullet 4, processing is not a function of a control center; it's a function of the underlying cyber systems. The actual alarm monitoring, for example, is the key piece, and the wording about "processing" should be removed.For bullet 5...The fluid nature of disaster recovery makes this one worrisome. A makeshift command center set up in the wake of a natural disaster would qualify, even if all they had were laptops with no external network connection, creating some difficult access tracking issues. In general, the inclusion of BES restoration, if necessary, will need to be bounded carefully - one solution would be include the phrase "BES restoration specific to situational awareness".In addition, there are concerns about

#	Organization	Yes or No	Question 1.c. Comment
			small hydro units which can send control signals to other small hydro units being classified as control center locations.
22.c	Oncor Electric Delivery LLC	Disagree with proposed definition	Exclude “display” of data. Inclusion would allow an auditor to assess that the simple display of Responsive Reserve in an office constitutes a “control center”.
23.c	Southwestern Power Administration	Disagree with proposed definition	For the purpose of this standard it would be clearer if the definition would just identify what NERC functions are performed in the control center environment. This will also lessen the chance for confusion going forward with non-CIP reliability standards usage of the term “Control Center”. BES Control Center - A site where personnel can perform one or more of the following functions:Reliability CoordinatorBalancing AuthorityTransmission Operator
24.c	USACE HQ	Disagree with proposed definition	Given that Control Center is based on the definition of BES Cyber System Components and BES Cyber System, which I disagree with both, I must also disagree with this one.
25.c	Edison Mission Marketing and Trading	Disagree with proposed definition	I don't agree that status and alarm monitoring has anything to do with relaibility
26.c	San Diego Gas and Electric Co.	Disagree with proposed definition	If an asset to be evaluated for Control Center status is only one BES Cyber System, it does not seem to meet the definition of “a set”. Therefore, SDG&E suggests that the first sentence of the definition should be changed to read “One or more BES Cyber Systems capable of ...”Is a control center appropriately defined as one or more “BES Cyber Systems capable of performing...”, or would is it more appropriately defined as “A location where one or more BES Cyber Systems are monitored for proper performance

#	Organization	Yes or No	Question 1.c. Comment
			of one or more of the following functions (i.e., two or more)..."Why is control of two or more facilities required for this definition? How does a backup control center factor into this definition? In the past, the "two or more facilities" piece was part of the differentiation between a control room and a control center, but we don't see a definition of "control room" in this draft.
27.c	Dominion Resources Services, Inc.	Disagree with proposed definition	It is not clear whether the control center is the aggregate of the BES Cyber Systems or the physical space containing them. There is ambiguity as to whether the last phrase (at multiple...) belongs to the set of BES Cyber Systems or to the multiple facilities. Other definitions are of the form that "if it does this" then it is "this". It should be clarified that the presence of one or more of these functions does not make it a Control Center. For example, using a conference room or field office to direct BES restoration activities during an emergency does not make that conference room or field office a Control Center. The term should be limited to only those physical spaces used by a Balancing Authority, Reliability Coordinator and/or Transmission Operator in the performance of real-time functions, since these are the 3 entities charged with overall reliability functions for the BES. Dominion proposes the following definition of a Control Center: Control Center - The space where a Balancing Authority, Reliability Coordinator and/or Transmission Operator uses one or more BES Cyber Systems to perform one or more of the following functions for two or more geographically dispersed BES Generation or Transmission Facilities: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.

#	Organization	Yes or No	Question 1.c. Comment
28.c	Emerson Process Management	Disagree with proposed definition	It is very unclear how this term could be interpred for typical power generation plants. Very rarely, multiple generation facilities at different locations will be controlled under one physical control center. Control systems and control rooms are mostly located at the same place with the generation units.So, the term of Control Center in this standard may be totally inapplicable to BES generation facilities or entities.
29.c	Liberty Electric Power, LLC	Disagree with proposed definition	Many generation plants are not part of the current definition of BES. This standard is not the correct place to redefine BES, and any language which does so will force "No" votes on the standard, regardless of the merits of the rest of the document.
30.c	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested modification to “Alarm monitoring” below:BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
31.c	Public Service Enterprise Group companies	Disagree with proposed definition	Mostly agree with the definition. However, the applicability of the first qualifier “(i.e., two or more)” is not clear. Does the qualifier apply to only “BES generation Facilities” or to “BES generation Facilities or Transmission Facilities”? Please clarify the language.
32.c	Regulatory Compliance	Disagree with proposed definition	Please clarify - for any control room at a generating facility that can remotely operate another site, whether or not it would be classified as a control center.
33.c	MWDSC	Disagree with proposed definition	Proposed definition conflicts with industry understanding and potentially with other standards. Attachment II assumes a Control Center is not just a collection of BES Cyber Systems gathering data, but rather a 24/7 facility staffed with certified power operators who take appropriate actions. Someone has to make decisions using the information being sent over cyber systems. Suggest changing definition as follows:"Control Center -

#	Organization	Yes or No	Question 1.c. Comment
			A facility staffed by a Transmission Operator, Generator Operator, or Balancing Authority who makes decisions based on information received from a set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations.
34.c	Con Edison of New York	Disagree with proposed definition	Regarding the definition of Control Center, as written, it appears that any facility can be deemed a Control Center. If a Transmission, Generation or other facility has a BES Cyber System that controls more than 1 generation or transmission facility it would be a Control Center. If so, this may be conflicting when addressing CIP-011-1 requirements that distinguish between Control Center and other facilities. This may also cause a transmission station that is connected to a generating station to be a Control Center if the station has an RTU cyber asset (with or maybe without an HMI) that can trip all station breakers (impacting the transmission station) and thereby trip the generator (impacting the generating station).
35.c	Wolverine Power	Disagree with proposed definition	See comments listed for 1.a
36.c	EEI	Disagree with proposed definition	See EEI's suggested wording in 1.a. Alternatively, EEI suggests:A modification to "Alarm monitoring":BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
37.c	WECC	Disagree with proposed definition	Seems to define the control center to try and exclude control rooms that only affect local facilities. Suggest rewriting to scope all bulleted functions performed inside a single location and EXCLUDING locations that only affect location facility operation.Based on the previously defined term "BES Cyber Systems" it is redundant to characterize a Control Center as a "set of one or more."The following rewrite is

#	Organization	Yes or No	Question 1.c. Comment
			proposed;Control Center - A facility used to implement a BES Cyber System(s) to perform one or more of the following functions for BES Generation Facilities, BES Transmission Facilities, and/or Distribution Facilities located at two or more locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.Distribution is included in this suggested rewrite based on its inclusion in the Applicability List as “Distribution Provider.”
38.c	Madison Gas and Electric Company	Disagree with proposed definition	Suggest removing the comma after "Transmission Facilities." With the comma, the subsequent phrase, "at multiple (i.e., two or more) locations," could be interpreted to apply to "one or more BES Cyber Systems" rather than BES Generation or Transmission Facilities.The term "location" is ambiguous in the context of the definition. For example, multiple generators at the same generating plant are placed in multiple locations (unless they impossibly occupy the same physical space). The intent of the qualification "at multiple locations" seems to be to exclude generating plant control systems, yet the definition could be read to potentially include generating plant control systems as Control Centers. Recommend modifying the definition to provide more specificity.Similar to the definition of BES Cyber System, the definition of Control Center does not provide criteria for aggregating BES Cyber Systems to define the "set of one or more BES Cyber Systems" that comprise a Control Center.New definition should read:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

#	Organization	Yes or No	Question 1.c. Comment
39.c	Entergy	Disagree with proposed definition	Suggest: A) Changing definition to speak specifically to "Functions" in Attachment I; and delete "for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations." B) Delete all bullets and rely on list of Functions as sole qualifiers. C) Note: close scrutiny of this definition is needed relative to EOP-008 (Project 2006-04: Backup Facilities; nearing final ballot) to avoid conclusion.
40.c	Green Country Energy	Disagree with proposed definition	Suggested definition:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions at two or more BES generation Facilities, or Transmission Facilities at two or more locations:
41.c	Allegheny Power	Disagree with proposed definition	Suggested modification to "Alarm monitoring" o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
42.c	Allegheny Energy Supply	Disagree with proposed definition	Suggested modification to "Alarm monitoring"- BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
43.c	Constellation Power Source Generation	Disagree with proposed definition	The "Acquisition, aggregation, processing..." function that a Generation Management System (GMS) or a marketing system would fall under scope of a "control center" though it would make more sense (in reliability terms) for it to be just a BES cyber system. A clarifying statement is needed to exclude marketing and GMS systems from this control center definition. The definition of control center is too broad in only requiring performance of one of the functions to meet the definition. A control center is commonly understood to be a location, not a system, where at least 4 of the 5 functions are performed, if not all 5 functions. This definition eliminated the concept of a control center as a defined space with operating systems and instead identifies a control center

#	Organization	Yes or No	Question 1.c. Comment
			as cyber systems which pull in work spaces that should not be in scope.
44.c	APPA Task Force	Disagree with proposed definition	The APPA Task force is concerned that under the proposed definition, a substation control room could be considered a "Control Center." Therefore, we offer the following clarification for your consideration:"A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator."
45.c	Xcel Energy	Disagree with proposed definition	The definition needs to clarify that it applies to interconnected control systems. For example, two independent control systems with no interdependency that operate generation units at separate locations should not be defined as a control center.
46.c	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjust generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level with in established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these type of Control Center functions.Remove asset management from function 3.

#	Organization	Yes or No	Question 1.c. Comment
			Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.
47.c	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	The definition of... "capable of performing one or more..." should be changed to "capable of performing four or more..."The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems, which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjusts generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level within established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these types of Control Center functions.Remove asset management from function 3. Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers

#	Organization	Yes or No	Question 1.c. Comment
			are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.Typically, BES restoration processes are coordinated with manual processes, and are not Cyber System related.
48.c	Platte River Power Authority	Disagree with proposed definition	The function"BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES)," doesn't clearly represent the real-time nature of the function. "System" is already included in BES. Suggested revision:BES real-time status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
49.c	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	The last two bullet points should be removed. The first is redundant and the last muddies the concept of control center. Restoration activities could be coordinated from a bucket truck or a temporary command center. These functions are actually human interactions not cyber systems.
50.c	US Bureau of Reclamation	Disagree with proposed definition	The term "BES asset" is not defined. The requirement should either propose a definition or the language in the requirement should be modified to refer to "BES Facilities" both of which are defined in the NERC Glossary of Terms.
51.c	LCEC	Disagree with proposed definition	The term "locations" needs to be defined. Should the human/machine interface be considered in defining a control center? Ensure that control rooms are not considered as control centers per this definition.
52.c	Southwest Power Pool Regional Entity	Disagree with	The use of "multiple (i.e., two or more)" twice in the same sentence is confusing. Consider changing the definition to read "A set of one or more BES Cyber Systems

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	capable of performing one or more of the following functions for multiple (i.e., two or more) geographically disperse BES generation Facilities or Transmission Facilities:"
53.c	Hydro One	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.Based on the control centre proposed definition all hub sites would be deemed within the definition of control centers. We would like the clarification if the auxiliary systems (High pressure air systems, cable temperature monitoring, QFW sag monitoring, DC inverters, PLCs, substations WANs, teleprotections, synchrophasors etc.) would be considered as BES Cyber System Components. As proposed, this definition would have massive implications to Hydro One in terms of implementation, capital cost, OM&A expenses etc.
54.c	Northeast Power Coordinating Council	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.
55.c	Bonneville Power Administration	Disagree with proposed definition	Third bullet should make it more clear that only real-time management (control and operation) is relevant. The example is for real time control; changing "e.g." to "i.e" would be sufficient. In addition, the way the definition is written it is possible that a substation could end up being identified as a Control Center. The definition needs to be clear that these are facilities whose prime purpose is to be control centers, not just substations that happen to have information covering other substations, or even possibly the ability to exercise some control over another substation.
56.c	Exelon Corporation	Disagree with proposed	This definition does not align with the commonly understood definition of control center and could be interpreted to apply to multiple unmanned locations housing servers.

#	Organization	Yes or No	Question 1.c. Comment
		definition	
57.c	NextEra Energy Corporate Compliance	Disagree with proposed definition	This definition needs to be more specific. NextEra suggest removing "capable" in the first line and removing or better defining "coordination" and "restore BES activities." NextEra also recommends defining control center as having the "Primary function."NextEra also suggests being clear on whether remote Control Centers are included, and, if so, CIP-011 needs to be very clear on any differences in the protection of remote control centers versus primary control centers. NextEra will be providing additional comments in the future.
58.c	Reliability & Compliance Group	Disagree with proposed definition	This definition seems to include control room as a Control Center. Does this mean a control room can be considered as a control center? Normally a Control Center requires having real time operation functions. The way it is stated above if you meet one of the last two functions, it is qualifies as a control center
59.c	Duke Energy	Disagree with proposed definition	This definition should be revised to clarify that a Control Center only includes facilities required to be staffed by NERC-certified operators. The revised definition should explicitly clarify that the term Control Center does not include the control room for a multiple generating unit site. Also, the use of the capitalized term "Facilities" continually causes confusion during audits, because, as the term is defined, even a single generating unit site could contain multiple "Facilities" (e.g. a line, a generator, a shunt compensator, transformer, etc.)Also, the phrase "capable of" is open to interpretation, and should be replaced with the phrase "operationally responsible for". Also, the phrase "for the support of" in the second bullet is open to interpretation, and should be replaced with the phrase "essential to".
60.c	Old Dominion Electric Cooperative	Disagree with proposed definition	This seems to widen the definition of control center to the point of being overreaching.

#	Organization	Yes or No	Question 1.c. Comment
61.c	Pepco Holdings, Inc. - Affiliates	Disagree with proposed definition	We agree with EEI's comments. Do transmission facilities include substations or does it reference just the transmission line components?
62.c	FirstEnergy Corporation	Disagree with proposed definition	We are unclear why 'control center' is being redefined as a logical set of cyber systems rather than a physical site which accommodates the functions traditionally identified with control centers. This definition appears to align with legacy architectures, where the control center serves as a communications hub and data center, thus creating a single point of failure. Modern architectures that employ best practices for reliability, redundancy, and diversity do not employ that structure. Since this is a significant departure from the commonly understood definition of 'control center', it is unclear how this definition will impact compliance to the newly proposed standards.
63.c	GTC & GSOC	Disagree with proposed definition	We do not agree with this definition. We believe that it will capture a large number of systems that are not part of what is commonly understood to be a control center. For example, an RTU acting as a data concentrator acquires data from multiple locations and supports real-time operations, but is not itself a control center. In addition, the term "BES assets" is an artifact of the version 1, 2, and 3 CIP standards and should either be replaced or clarified. More basically, though, we question the need for this definition. Its primary function appears to be as a scoping criterion for CIP-011 in the same manner that generation [sic] Facility and Transmission Facility are. However, the SDT did not feel the need to define either of those terms. We recommend that this definition may be better suited for a guidance document.
64.c	We Energies	Disagree with proposed definition	We Energies agrees with EEI Suggested modification to "Alarm monitoring" with minor modifications: o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or Suggested modification to "Acquisition" bullet o Acquisition, aggregation, processing, inter-utility exchange or display of BES reliability or operability data for the support of real-time BES operations.

#	Organization	Yes or No	Question 1.c. Comment
65.c	Independent Electricity System Operator	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster”.
66.c	IRC Standards Review Committee	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster” or “BES Control System”.
67.c	Midwest ISO	Disagree with proposed definition	What is really being described is a control system and not a control center. A control center implies physical attributes that are not described in this definition. We suggest to modify the definition to control system rather than control center.
68.c	Florida Municipal Power Agency	Disagree with proposed definition	With this definition, a substation control room can be a “Control Center”. A Control Center has other characteristics associated with it that make it a control center, i.e., “centralized operation”, the reverse of the term. FMPA suggests a simpler definition:”A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator.”

2. **The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

While there was general agreement with scoping the applicability of the standards to "real-time" systems, many entities questioned the source of 15 minutes as the scoping time. Some commenters expressed concerns about the auditability of this qualification in defining the scope of applicability.

In selecting the 15-minutewindow, the SDT reviewed various reliability standards and identified two widely used time horizons: 30 minutes and 15 minutes. The intent of the SDT is to include those systems that impact "real-time" operation of the BES. The SDT used a 15-minute window to qualify the "real-time" nature of the impact and felt that a 30-minute window would include those systems that might not be considered as "real-time".

The proposed definition of a **BES Cyber System** has been revised as follows:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 2 Comment
2.1	USACE HQ		I disagree with the scope and disagree with expanding the scope. The use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit
2.2	Arizona Public Service Company		The 15-minute criteria specified as part of the definition of a BES Cyber System may both lead to confusion and/or act as a loophole to exclude BES Cyber System Components from further consideration. Confusion may be caused by likely differing interpretations of "restrict control and operation of the BES, or affect situational awareness of the BES". Without more specific definitions, each Entity may utilize different criteria for determining whether control and operation has been 'restricted' or whether situational awareness has been 'affected'. Such potential ambiguity may also allow Entities to utilize

#	Organization	Yes or No	Question 2 Comment
			excess discretion in this determination in order to 'exclude' Cyber System Components from categorization. A suggestion would be to attempt to avoid such vague terms if a timeline is specified in the definition at all, or to avoid a timeline in the definition and add time windows to the Impact Categorizations. Examples of terminology changes include using the term 'impede' rather than 'restrict' (as some restriction may be tolerable, but impede strengthens the concept being conveyed) or using the phrase 'impact operational decision making' rather than 'affect situational awareness' (as such a phrase might be less likely to be misinterpreted outside of Power Operations expertise).
2.3	Nuclear Energy Institute	Agree with scope	A recommended change to BES Cyber System Component has been proposed to clarify that the intent is to protect real-time operations. NEI recommends examples of systems that would fall in and outside this scope.
2.4	US Army Corps of Engineers, Omaha Distirc	Agree with scope	Agree with limiting scope to real-time systems with an operational time horizon of 15 minutes. However the wording of the definition needs to be strengthened because the intended meaning of the definition as "real-time" systems with an operational time horizon of 15 minutes" was not clear until.
2.5	Entergy	Agree with scope	Agree with scope limitation to "real-time operations." Suggest: Rule 706 be carefully reviewed to assure this is not countervailing to FERC directives; their directives suggest a broader scope of applicability.
2.6	Allegheny Power	Agree with scope	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.7	EEI	Agree with	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be

#	Organization	Yes or No	Question 2 Comment
		scope	appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.8	MWDSC	Agree with scope	Also need to identify who makes the real-time operational decisions, i.e., Transmission or Generator Operator or Balancing Authority. See suggested changes in comments to question 1.b.
2.9	City Utilities of Springfield, Missouri	Agree with scope	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
2.10	Dominion Resources Services, Inc.	Agree with scope	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for the real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES.
2.11	Southwest Power Pool Regional Entity	Agree with scope	Entities today eliminate assets from the Critical Asset list because they assume a mitigation to a voltage instability or thermal overload is available and will always be successful. Consider modifying the definition to read "...could, if not mitigated within 15 minutes,..."
2.12	Southwestern Power Administration	Agree with scope	Fifteen minutes seems to be a reasonable operational horizon, but should the language be modified in such a way to allow for an operational time horizon of approximately 15 minutes in order to discourage "clock watching" by entities and/or auditors to reach a conclusion of either fourteen or sixteen minutes.
2.13	Platte River Power Authority	Agree with scope	I agree so long as the BES Cyber System definition is updated to more clearly explain the horizon. For example:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within an

#	Organization	Yes or No	Question 2 Comment
			operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
2.14	MidAmerican Energy Company	Agree with scope	MidAmerican Energy agrees with EEI's affirmation below:Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.15	Progress Energy (non-Nuclear)	Agree with scope	See comment for question 1b.
2.16	APPA Task Force	Agree with scope	The APPA Task force agrees with the proposed definition, but offers the following suggestions:It seems that the 15 minute horizon is arbitrary. We suggest aligning the time to an already determined time limit in the standards. For instance, TOP-004-2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an “unknown operating state”, which seems to be a good metric to use since loss of situational awareness at a Control Center results in an “unknown operating state”, which seems to correspond with the longest time frame of Attachment I to CIP-010. We understand that other commenters are submitting alternative language. We can support alternative options if they are based on existing NERC defined terms or already determined time limits.
2.17	Bonneville Power Administration	Agree with scope	The definition clearly ties the scope of the standard to real-time control. The time limit clearly separates real-time from long-term. The choice of 15 minutes versus some other duration is not as important as limiting the duration.While we agree with the scope, we don't believe the definition of BES Cyber System makes it clear that the scope is limited to real-time operation systems. The definition of BES Cyber System doesn't include the words real-time. For CIP-002, BPA identifies only control center systems used for real-

#	Organization	Yes or No	Question 2 Comment
			time controls as Critical Cyber Assets. This scope is consistent with what BPA does now for control center cyber systems.
2.18	Southern California Edison Company	Agree with scope	The drafting team should provide justification on the use of a 15 minute window for a BES cyber system to cause a Disturbance. Is the drafting team suggesting registered entities simulate disturbance events in 15 minute increments as a criterion in engineering studies to assess device capability that may be the justification for an impact based assessment methodology? If so, the drafting team needs to clarify this.SCE suggests removal of the 15 minute qualifier if no clear operational justification exists for the choice of such timeframe. While a three year timeframe for engineering studies is an acceptable, the constraints necessary for inclusion within the study, to look for specific disturbance conditions, may be difficult to implement.
2.19	Midwest ISO	Agree with scope	We agree in general. However, we do not necessarily agree with 15 minutes. Please see our response to Question 1.b.
2.20	Pepco Holdings, Inc. - Affiliates	Agree with scope	We agree with EEI's comments regarding the intended scope (i.e. limit to systems that impact the real-time real-time operations of the BES) and suggestions. Please also reference response to 1b.
2.21	We Energies	Agree with scope	We Energies agrees with EEI comments. Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.22	GTC & GSOC	Agree with scope	We understand the intent of the 15 minute aspect of the defined scope, but believe it will be difficult to implement and audit. Otherwise, we recommend the revised definition in 1b

#	Organization	Yes or No	Question 2 Comment
2.23	Duke Energy	Agree with scope	With the clarifications we've made above, we agree with the scope of applicability.
2.24	ISO New England Inc	Disagree with scope	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
2.25	ReliabilityFirst Staff	Disagree with scope	Assuming the 15 minutes identified here is the same 15 minutes used in question 1.b above, we believe the scope should be 5 minutes.
2.26	Tenaska	Disagree with scope	Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity. The Operational Time Horizon should be based on the potential severity of the event as well as the availability of other systems that can provide the same functionality.
2.27	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with scope	Comments to Questions 1.a and 1.b apply here also.
2.28	ERCOT ISO	Disagree with scope	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
2.29	CenterPoint Energy	Disagree with scope	Disagree - CenterPoint Energy is concerned with the definition as stated above in response to 1.b. In addition, the SDT has offered no basis for the 15 minute time horizon.

#	Organization	Yes or No	Question 2 Comment
2.30	E.ON U.S.	Disagree with scope	E.ON U.S. seeks clarification of whether the 15 minutes captures the intent of the 'Restoration of BES" function identified in Attachment 1 of CIP-010
2.31	Exelon Corporation	Disagree with scope	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..." The 15 minute timeframe is inconsistent with other standard language. Specifically, TOP-004-2 R.4. has a 30 minute response requirement.
2.32	LCEC	Disagree with scope	I am concerned that a time based definition will lead to confusion and create a difficult situation from an audit perspective. I agree that the standard should exclude "situational awareness" related functions that are not real-time in nature and do not provide the primary operational monitoring or control function of the BES.
2.33	Matrikon Inc.	Disagree with scope	I am trying to determine where to insert this operational time horizon into the evaluation criteria. Due to the room for interpretation, I don't yet support or reject the use of 15-minutes, or an appropriate duration. Fundamentally, there is no clear definition or instruction on how this can be used as criteria for determining Impact Level of cyber systems.I worry there is room for different interpretations, putting an entity trying to comply with the new CIP-01x standard at a competitive disadvantage to another entity that takes a different approach. I foresee 2-3 places where the time horizon could be inserted into a Responsible Entity's interpretation of BES Cyber Systems, I am hoping a tighter definition will address this issue.First Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2.2. Do they now evaluate the impact rating against the time horizon? Let us assume the Cyber System has High Impact. But if there is no effect in 15 minutes, does that mean: 2a. I automatically assign a Medium impact Rating? 2b. Or, I now evaluate it against the Medium impact criteria?3. If it continues to have no impact in 15 minutes to the Medium criteria, then is it a Low Impact BES Cyber System?Second

#	Organization	Yes or No	Question 2 Comment
			Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2. 1a. Let's now assume that the rating of High/Medium/Low is assigned to each BES Cyber Component and cannot be changed.2. Do they now go through the complete list of Cyber Systems looking for those which could affect any reliability function within 15 minutes? 2a. This may bring in other support systems like HVAC, UPS, CEMS opacity readings for generation, water supply and others that are not explicitly named in Attachment 1.Third Interpretation Scenario:1. An event has occurred at the facility that some action needs to be taken. There is the capability to notify the authority, and shutdown/bypass safely within 5-10 minutes.2. If the Responsibility Entity has the ability to exceed 15-minutes before taking action, then is this no longer an impact to the BES, and subsequently falls to the bottom and become Low Impact. 2a. For example, coal handling is down but we have some coal left on the conveyor, and the boiler is still hot so we have time to respond. 2b. For example, water supply is dropping but do not have to take action within 15 minutes. 2c. For example, vibration or emissions data is high, but we don't have to take action, within 15 minutes.Please provide additional information and guidance on how the 15-minute time horizon is to be applied to systems.
2.34	CWLP Electric Transmission, Distribution and Operations Department	Disagree with scope	It is unclear how the 15 minute time frame is to be applied.
2.35	Emerson Process Management	Disagree with scope	It really depends on how we view this issue. If I understand this intent correctly, the current language is trying to state that the BES reliability will be suffered if the BES cyber system is unavailable for more than 15 minutes. In another word, if the BES cyber system is failed for more than 15 minutes and the BES is not suffered, this system will be not categorized as BES Cyber System. This definition is very difficult in interpretation for power generation. If a plant has a 2000MW generation capacity and its water treatment cyber system is failed, the plant itself can sustain for a while, but not too long. After this grace period, the unit(s) will be shut down. The 2000MW will be lost. Does this affect

#	Organization	Yes or No	Question 2 Comment
			BES reliability? This is the confusion.
2.36	Florida Municipal Power Agency	Disagree with scope	It seems that the 15 minutes is arbitrary. FMPA suggests aligning the time to an already determined time limit in the standards. For instance, TOP 004 2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an "unknown operating state", which seems to be a good metric to use since loss of situational awareness at a Control Center results in an "unknown operating state", which seems to correspond with the longest time frame of Attachment I to CIP-010.
2.37	Seattle City Light	Disagree with scope	It will be difficult to quantify the impact of systems within a window of time - this would be a qualitative assessment which invites a tremendous amount of subjectivity.
2.38	Garland Power and Light	Disagree with scope	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good scope and we would agree
2.39	Kansas City Power & Light	Disagree with scope	No. Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber

#	Organization	Yes or No	Question 2 Comment
			System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study.
2.40	Covanta Energy	Disagree with scope	Not clear as to why 15 minutes is the optimal number... would like more basis information prior to supporting.
2.41	IRC Standards Review Committee	Disagree with scope	Please see our comments under Q1b
2.42	Independent Electricity System Operator	Disagree with scope	Please see our comments under Q1b.
2.43	Public Service Enterprise Group companies	Disagree with scope	PSEG agrees that cyber protections should be mandated only for real-time operations systems.
2.44	National Grid	Disagree with scope	Real time operation of the system typically implies SCADA. If protection systems are part of the real time operations then as stated in 1b, the 15 minute time horizon may not be adequate. 15 minute time limitation also does not appear realistic. The vulnerability can exist beyond this timeline and can be equally catastrophic.
2.45	Electricity Consumers Resource Council (ELCON)	Disagree with scope	See comment on 1.a above.
2.46	NextEra Energy Corporate Compliance	Disagree with scope	See comments to 1a. NextEra believes if this approach is maintained despite these concerns, then this section needs clarity regarding 15 minute time horizon regarding recoverability. As written, the definition encompasses and overlaps normal operations

#	Organization	Yes or No	Question 2 Comment
			systems and recovery timeframes and does not address impacts to the BES beyond normal reliability operations.
2.47	Manitoba Hydro	Disagree with scope	See comments to Question 1.6
2.48	BCTC	Disagree with scope	See previous response
2.49	Network & Security Technologies Inc	Disagree with scope	See response to 1.b., previous
2.50	Puget Sound Energy	Disagree with scope	See response to question 1b. While it seems realistic, it is unclear how to prove something is within the 15 minute timeframe or not and unclear how this could be tested during an audit that something should have been included or not included. Some examples would be beneficial. Also PSE agrees with the scope of the definition, but is concerned with the vagueness of two of the terms used in the definition: “restrict” and “affect”. PSE agrees with the definitive language of “cause a Disturbance”, as that is a measurable level of compliance. The current standard has too many vague terms that are left open for interpretation.
2.51	WECC	Disagree with scope	Suggest SDT re-evaluate if reliability coordination systems such as Coordinated Outages, Historian, or Next Day Studies should be excluded from scope of these standards.Also, see response to 1c
2.52	Indeck Energy Services, Inc	Disagree with scope	The 15 minute time horizon needs to exclude events that the BES normally resolves within 15 minutes. Many events could take place in significantly less time. Normal operations work within the 10 minute horizon for measurements such as controlling

#	Organization	Yes or No	Question 2 Comment
			ACE. Not everything that happens within 15 minutes necessarily affects BES ALR. A single 15 minute time horizon appears to cast the net too widely. The time horizon needs to be specified for each of the Functions in Attachment I.
2.53	FirstEnergy Corporation	Disagree with scope	The 15 minute time limit causes confusion on how the definition will be applied in practice, since in most cases the loss of a component creates a probabilistic risk and not a certain risk.FE suggest that the SDT avoid the use of the 15 minute reference and consider incorporating the existing NERC glossary terms of "Real-time" and "Real-time Assessment". We offer the following definition for BES Cyber System:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a BES Disturbance or impact the Real-time Assessment capability, Real-time control and operation, or materially impact situational awareness of the BES.Situation awareness is somewhat vague and may mean different things to different people. The team should consider taking the description of situational awareness as shown in Attachment I - "Functions Essential to Reliable Operation of the Bulk Electric System" and making it a NERC Glossary of Terms definition.
2.54	LADWP	Disagree with scope	The 15 minute window is relative. The industry needs to define what is an acceptable time horizon.
2.55	Dairyland Power Cooperative	Disagree with scope	The 15-minute rule seems arbitrary and one dimensional. How does the availability of using a system for control relate to this time frame? I'm having trouble relating this to for instance a telemetry/control function. It would be possible that long periods of down time could pass without impact to the BES system... but under certain conditions it would be critical to have the monitoring and control functions.
2.56	Constellation Energy Commodities Group Inc.	Disagree with	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting

#	Organization	Yes or No	Question 2 Comment
		scope	team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events that immediately impact the system; the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.57	Constellation Energy Control and Dispatch, LLC	Disagree with scope	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events the immediately impact the system, the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.58	San Diego Gas and Electric Co.	Disagree with scope	The phrase "real-time" doesn't have a definitive industry-wide connotation, although for collecting field data it usually means seconds instead of minutes. In general, SDG&E supports the inclusion of real-time operations systems being in-scope, but we support a shorter operational time horizon (such as 5 minutes) to make the definition more immediate, with more high value BES Cyber assets being part of the scope.
2.59	Minnesota Power	Disagree with scope	The scope of applicability and operational time horizon of 15 minutes appears arbitrary and Minnesota Power is unsure as to how the Standards Drafting Team envisions that a Registered Entity will be able to show and document (i.e., prove for audit purposes) that a particular Cyber System will or will not have an effect on the BES in a certain time period. If the intent is "real-time operations," then state that and drop "within 15 minutes."
2.60	Consultant	Disagree with	The scope statement should clarify the inclusion or exclusion (or alternative treatment) of backup systems, development systems and environments, quality assurance systems and environments, testing systems and environments.As stated the only systems that

#	Organization	Yes or No	Question 2 Comment
		scope	appear to be "in scope" are live production systems.
2.61	US Bureau of Reclamation	Disagree with scope	This requirement puts a premium on the definition of what the BES is. There are components of the power system that are not "BES" and therefore do not qualify under these Standards. This issue needs to be further addressed. Further, the term "operational time horizon" needs further definition. Is this 15 minute criterium to be applied under normal operation conditions, or only those that COULD be experienced if the Cyber System were to be compromised?
2.62	Ameren	Disagree with scope	We disagree with the scope; the 15 minutes should only apply if the disturbance is not recoverable.
2.63	Southern Company	Disagree with scope	While we understand the intent of the 15-minute scope, we feel that the inclusion of this factor causes too much vagueness in the interpretation of the definition. We recommend that the focus be limited to real-time operations only.
2.64	Verizon Business	Agree	The “15 minute” criterion needs to be expanded – perhaps in an associated guideline or “Frequently Asked Question”

3. **Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns on the broad implication associated with the phrase "execute or enable…". Entities generally agreed with the assignment of compliance responsibility to owners, but many others expressed concerns for jointly owned facilities or facilities that may be operated by other than owners. There were many concerns expressed about the Functions and their description and definition. Others expressed concerns about the differences between systems and their components.

CIP-010-1 Requirement R1 has been replaced by CIP-002-5, which reads:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems*. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

Additional guidance for jointly owned facilities has been provided in the Application Guidelines section of the standard. The reliability functions have been redefined as Reliability Operating Services to avoid any confusion with the use of the term Functions as used in the Functional model.

#	Organization	Yes or No	Question 3 Comment
3.2	WECC		Agree with the concept however, "...to execute or enable..." or "...which execute and/or enable." "to" can be construed as passive. It is redundant to utilize the phrasing "...to identify BES Cyber Systems for the application of security requirements."The following rewrite is proposed;R1. Each Responsible Entity shall identify and document each BES Cyber System(s) that it owns, which execute and/or enable one or more functions defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES. (Violation Risk Factor: High)
3.3	Entergy	Agree	Agree that applicability should be strictly focused on "owned" assets.

#	Organization	Yes or No	Question 3 Comment
3.4	US Army Corps of Engineers, Omaha Distirc	Agree	Agree with R1 requirement - Find the measures for R1 - R3 troublesome. Measures are stated in terms of number of BES cyber systems. It is conceivable that plant SCADA systems could be considered a single system or a group of a few systems. How is a missed component handled? Is it another system or is a component. It appears like the violation measures are being handled as a count of BES cyber system components not BES cyber systems. Feel the measures should be revisited with the low number of systems likely to be identified in mind. Seems odd that any additional system is a sever violation if you have identified fewer than 6 systems.
3.5	Florida Municipal Power Agency	Agree	Although FMPA agrees with the requirements, FMPA suggests that naming Attachment I "Functions ...." will add confusion with the "Functional Model". FMPA suggests renaming Attachment I to "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in Question 6.
3.6	Garland Power and Light	Agree	Definitely agree with the words "it owns"
3.7	SCE&G	Agree	Guidelines should be provided to assist entities in determining how BES Cyber System Components should be grouped into BES Cyber Systems. Can a single component reside in two cyber systems?
3.8	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
3.9	Reliability & Compliance Group	Agree	Is the assumption that the initial list needs to contain both BES and non-BES Cyber Systems? It would be better if the standard was even more proscriptive here.
3.10	Con Edison of New York	Agree	Please note comments to question 6. It may be easier if the DT reference functions as detailed by FERC-approved NERC Reliability Standards. The definitions in Attachment I will ultimately lead to many requests for interpretation. R1 requires identification and documentation of BES Cyber Systems. There is no requirement to identify BES Cyber

#	Organization	Yes or No	Question 3 Comment
			System Components within CIP-010. However, CIP-011-1 R23 requires that you develop an inventory of these Components. Should this be a CIP-010 requirement? Then CIP-011 can expand on the Change Management Controls.
3.11	San Diego Gas and Electric Co.	Agree	SDG&E agrees with the wording in R1, but has additional comments and requests for clarification. Specifically, we request clarification regarding the "situational awareness" reference in Attachment I. In our case, as many other entities, we use Remote Terminal Units to gather data from BES substations and present that data to the operators to improve their Situational Awareness. Loss of a single RTU vs. loss of multiple RTUs affects the presentation of this data to operators to varying degrees (with associated effects on monitoring the BES), but the Standards don't address quantitative issues such as this.In a similar vein, SDG&E also requests clarification regarding the term "inter-entity real-time coordination and communication" in Attachment I. For example, are inter-entity telephone systems in-scope or is this referring to electronic data exchange between entities such as ICCP data links?Probably SDG&E's largest concern with CIP-010-1 R1 is the sheer amount of effort and resources it will take to build the lists of BES Cyber Systems and the impact categorizations. While there are some loose parallels with the current CIP-002 Standard, we won't be able to re-use the bulk of the work already done in our Risk-Based Assessment to identify Critical Cyber Assets. SDG&E's opinion is that CIP-010 doesn't leverage as much of CIP-002 as we'd like to see. We'd like to take advantage of what already has been produced to become Compliant with the existing Standards, and we see these new draft Standards as going in a new direction with many of the requirements. We would feel better about it if the new Standards were bringing substantial additional reliability and security to the BES, but that is not apparent.
3.12	Minnesota Power	Agree	With the previously stated recommendations regarding the definition of BES Cyber System (see Question 1.b.) and the changes indicated below, Minnesota Power generally agrees with the proposed Requirement R1. "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns which execute or enable one or more functions defined in CIP-010 - 1 Attachment I, Functions Essential to the Reliable

#	Organization	Yes or No	Question 3 Comment
			Operation of the BES, for the purpose of applying the security requirements."
3.13	BCTC	Disagree	- Recommend removal of the “Inter-Entity Real-Time Coordination and Communication” (Attachment 1) point as this is covered under the COM domain
3.14	Bonneville Power Administration	Disagree	"...that it owns to execute or enable..." is somewhat unclear. It appears the intent is the equivalent of "that it owns that is able to execute or enable...". As it is written, it can give the impression that the purpose of owning the system is to execute or enable the functions. That is too narrow. Another possible interpretation is that the "to execute or enable..." refers to the objective of the requirement. If that is so, then please break the objective out separately:"Objective: To execute or enable...Requirement: Each Responsible Entity..."Many of the other requirements include "to..." at the end of the requirement. These are clearly objective statements. They should be broken out separately, into an "Objective" and "Requirement", as stated above. The last phrase in Requirement 1 is “for the application of security requirements.” In Requirement 2 the last phrase is “for the application of Cyber Security requirements . . . .” Are these two phrases supposed to have the same meaning? If so, shouldn’t they use identical words? If not, what does “for the application of security requirements” mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: “for the application of the Requirements contained in Standard CIP-011-1.”
3.15	Consultant	Disagree	1. I think the standards should provide some distinction between ownership responsibility and operations responsibility, or provide a mechanism to identify the responsibility for the requirements based on each specific situation. (Technical Feasibility Exception for owner versus operator responsibility?) This may include split responsibility for different aspects of the requirements. (This comment probably applies to more than just this requirement in both CIP-010 and CIP-011.)2. Wording is confusing regarding systems for application of security requirements. Suggest ending the requirement statement after "...Reliable Operation of the BES."3. Suggest using the complete title of

#	Organization	Yes or No	Question 3 Comment
			Attachment I: "Bulk Electric System" not "BES".4. In all locations in both CIP-010 and CIP-011 suggest removing references to specific revisions (e.g. CIP-010-1). This requires all standards to be changed for a change in any one standard. The documentation of which revision was used at the time of implementation should be included in the Responsible Entity's documentation or compliance.
3.16	Dairyland Power Cooperative	Disagree	A Responsible Entity should be responsible for any systems used for their operation regardless of ownership. Basing responsibility based on the ownership of a system creates a big loophole. It is possible an interfacing utility or service provider could be involved. Basing responsibility on the ownership of the facility containing the systems make more sense.
3.17	Duke Energy	Disagree	Additional clarification is needed on the process for identifying and categorizing BES Cyber Systems. Requirement R2 should really come first, and require that Responsible Entities identify their BES Cyber Systems that meet the criteria in Attachment II (i.e., that can affect operations for the listed facilities/functions). Requirement R1 should come second, and require documentation of the functions affected for each BES Cyber system identified. Attachment I is not needed as part of the standard, but should be included in a guidance document.Much more clarification is needed to Attachment I. As described, the functions are far too broad. Specific language issues: o Monitoring & Control - Activities, actions and conditions that provide both monitoring and control of BES elements. o Situational Awareness - too broad as stated. Should be limited to situational awareness of the BES required by System Operators to perform their reliability-related functions o Inter-Entity Real-Time Coordination and Communication - too broad as stated; would seem to possibly include telephone lines
3.18	Arizona Public Service Company	Disagree	Additional verbiage needs to be included in order to clearly delineate which entity is responsible for an asset/system when it is jointly owned. Is it the majority owner? The operator? Where is the line?”

#	Organization	Yes or No	Question 3 Comment
3.19	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Again, no defining metrics. Small DP/LSEs will unnecessarily be required to comply with no BES reliability return.
3.20	IRC Standards Review Committee	Disagree	At the NERC CIP workshop in May 2010, there were so many examples brought forth where it could not be determined with exactness which components are part of a BES Cyber System or not because of the flexibility built into the requirements. "It depends" was often the response from the panels. So although the intent of CIP-010 is to provide more concrete guidance for registered entities to define BES Cyber Systems, in practice it may introduce just as many new questions about applicability as it may solve. It would be better to develop a performance based approach to define BES Cyber Systems rather than use bright line definitions to identify BES Cyber Systems. The proposed definitions of High and Medium include criteria that describe facilities, by KV level, MW size etc. But these are really proxies for an underlying intent of trying to describe a certain level of operational performance. For example, higher KV levels are assumed to reflect greater impacts on neighbors. And higher MW levels of generation are assumed to reflect greater risk of disturbance to load. Rather than use these proxies, the ratings High and Medium should instead employ descriptors related to a desired level of performance, for example, "...a loss of a facility that does not cause a IROL violation two systems away." Such an approach in defining the BES Cyber System would better focus the CIP-011 requirements and compliance efforts of both NERC and the registered entity on only those components that truly have a significant impact on the interconnected BES and not include facilities and components that although meet a bright line definition, really have minimal impact on the BES because of its particular location or configuration.
3.21	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
3.22	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall

#	Organization	Yes or No	Question 3 Comment
			document each identified BES Cyber Systems that it owns which support the functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES, for the application of security requirements."
3.23	LCEC	Disagree	Concerned with the word "owns". Recommend "owns or operates" or a statement referencing operational responsibility.With the current definition of BES Cyber System Components including "one or more" devices, a lot of guidance will be needed to determine what constitutes a system versus a number of components. Most of the standards currently reference the system versus the component which could leave a gap in applicability. Is it assumed that all components must be a system or part of a system? Modifying the BES Cyber System Component definition to exclude "one or more" will help but entities will still need clarification on the grouping of components to form systems. An implementation guideline will help address this.
3.24	Constellation Power Source Generation	Disagree	Constellation believes that this requirement is too broad in terms of auditability. The proposed verbiage of CIP-010 is flexible in terms of how to define cyber systems, but is it implying that a methodology is needed to identify cyber systems? Or is it implying that each Responsible Entity define cyber systems as they see fit, without an explanation? For a company such as Constellation, which owns a fleet of diverse generation facilities, this flexibility will cause each plant to have its own unique methodology for developing cyber systems, which vastly increases the procedural burden of this standard when compared to the current version of CIP-002. A suggestion would be to clarify this requirement in a guidance by stating whether or not a methodology is needed to define cyber systems, and if not, what type of evidence would be suggested for showing that a cyber system has been identified correctly.
3.25	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy does not agree with the direction of the SDT and believes it is pre-mature to discard the current CIP requirements with a completely new philosophy. Most entities are in the compliance phase of implementation of the current CIP requirements and have yet to be audited. To have a fundamental shift in approach before the current requirements have been evaluated as to effectiveness and

#	Organization	Yes or No	Question 3 Comment
			compliance is unwarranted. In addition, CenterPoint Energy does not agree with the expansion of the CIP requirements to facilities that do not have a high impact on the reliable operation of the Bulk Electric System. CIP-010-1 and CIP-011-1 would apply some cyber security requirements to facilities and systems that the draft Standard would identify as having a medium to low impact to the reliable operation of the Bulk Electric System. While CenterPoint Energy agrees that some set of minimal security criteria should be used to protect facilities from malicious behavior, vandalism, or simply the curious, CenterPoint Energy believes these efforts are more accurately characterized as Good Business Practice and as such should not be auditable under mandatory reliability standards. Stated another way; those facilities and systems that have been identified as medium to low impact, using the draft standard methodology, by the nature of having little or no impact to reliable operation of the Bulk Electric System, should not be protected under auditable, mandatory, requirements.
3.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 1 Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints: (Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope

#	Organization	Yes or No	Question 3 Comment
			for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES equipment required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment . Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.
3.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 1Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints:

#	Organization	Yes or No	Question 3 Comment
			(Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & Control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES Cyber System or Components required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to

#	Organization	Yes or No	Question 3 Comment
			directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Define the term Situation Awareness and how it applies to BES Cyber System or components required for system restoration.
3.28	Dominion Resources Services, Inc.	Disagree	Dominion agrees with R1, but is concerned with the functions listed in Attachment 1. Please see Dominion's response to Question 6.
3.29	E.ON U.S.	Disagree	E ON U.S. notes the absence of any study to assess whether identifying and categorizing all BES Cyber Systems as required by R.1 provides for material enhancement of BES reliability relative to the current Critical Asset identification methodologies allowed under CIP-002. E ON U.S. is also not aware of any effort to objectively quantify the costs that will result from R.1. Given the likely significant costs to consumers it would behoove the SDT and NERC to make an effort to understand the costs and incremental improvement to BES reliability associated with the sweeping changes proposed in CIP-010, R.1.The proposal does not allow for "no impact" assessments to be determined through engineering evaluation or other approved methods. E ON U.S. believes it would be an improvement to include language similar to that in existing CIP-002 R1.2.
3.30	EEI	Disagree	EEI generally agrees with R1, however, all owners of jointly owned facilities may not be responsible for protecting the BES Cyber Systems. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1. As a result, the drafting team should clarify what is meant by "owns" (i.e. how should GOs and GOPs collectively assess BES Cyber Systems).
3.31	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, "BES Cyber Systems that the entity owns, operates, or is otherwise

#	Organization	Yes or No	Question 3 Comment
			responsible for. . .”
3.32	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
3.33	USACE HQ	Disagree	I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of essential function without any support of why they are essential. Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. To create a list of functions and stating that they are essential without having done some type of study looking into what are really essential functions supporting the BES are only limits the protection of each asset to what a small group of people think is critical without taking into consideration the individual circumstances each asset brings to the table. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish the “functions essential to the reliable operation of the BES”.
3.34	Pepco Holdings, Inc. - Affiliates	Disagree	In general we agree with R1 when there is only one owner of a BES Cyber System. However we also agree with EEI’s comments that owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are

#	Organization	Yes or No	Question 3 Comment
			Transmission Lines and/or Substations that are owned by multiple parties but one party is responsible for the operation and maintenance. Suggest considering adding language to R1 to cover joint owned facilities (e.g. In cases of joint owned BES Cyber Systems, the assigned Responsible Entity or Entities shall...).
3.35	Southern California Edison Company	Disagree	It is not clear how this requirement differs from CIP-002, R3. While the description of CIP-011 states the intent to retire CIP-003 through CIP-009, CIP-002 would still be in place. It is also not clear how these CIP-010-1 and CIP-002 would work together.
3.36	SPS Consulting Group Inc.	Disagree	It is unclear how the list of Essential Functions in Attachment 1 correlates to the categorization in Attachment II, which does not mention essential functions. I believe that Attachment I can be deleted and that Attachment II is fully sufficient for the categorization exercise. The stated purpose of Attachment I to define the scope of the CIP standards is unnecessary because the CIP standards do not apply to functions, they apply to registered entities, which are quite clearly stated.
3.37	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
3.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's recommendation to change owner to the owner-operator that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The owner-operator that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.39	Michigan Public Power Agency	Disagree	MPPA is one of many organization that are co-owners of facilities that do not maintain operational control of the facility. MPPA suggests that the word "owns" in "...Systems that it owns to execute..." be changed to "operates."
3.40	Tenaska	Disagree	No R1 should be to identify BES assets that cyber systems are a part of. Consider

#	Organization	Yes or No	Question 3 Comment
			replacing attachment 1 with better definitions in the body of the standard.
3.41	Progress Energy (non-Nuclear)	Disagree	One major issue is that we do not have a clear definition of the BES. How do we define the BES? Is it all lines over 100kV excluding transmission feeders? It appears that some reliability groups are presently trying to define the BES clearly. If the BES includes >100kV import/tie lines, nuclear off-site power path, cranking path, quite a few T/T substations with microprocessor relays on lines could be put in scope of identification. These might be excluded or classified low impact if no communication is provided. Will power line carrier, transfer trip, etc. be in scope? This could turn into a very large list to develop and maintain.
3.42	Allegheny Energy Supply	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.43	Allegheny Power	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.44	PacifiCorp	Disagree	PacifiCorp agrees with EEI's recommendation to change owner to entity that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is should be identified as responsible for the requirements identified by CIP-010-1.
3.45	Regulatory Compliance	Disagree	Please clarify - Attachment I - The function identified for Inter-entity Real-time Coordination and Communication: Is the coodination between the Responsible Entities' associated System operators or between BAs? Also what specific equipment is brought

#	Organization	Yes or No	Question 3 Comment
			into scope? Is it only for data communcation or voice communication as well?
3.46	Puget Sound Energy	Disagree	Puget Sound Energy feels that, without clarity (as commented in question 2 above), the scope of BES Cyber Systems can not be uniformly agreed upon and, as such, defendable metrics to prove compliance will not be able to be establish. For example, corporate email can be used to provide efficient communications between operators of the BES. The loss of corporate email, which in no way could cause a disturbance to the BES (and is physically and logically separated from all BES Cyber Systems), could "restrict" or "affect" the real-time operations of the BES through degradation in efficient communications. As well in order to prove compliance the unintended consequence of this requirement is a massive work effort to evaluate all the BES Cyber Systems in order to then establish or demonstrate which enable or execute essential functions.
3.47	Alliant Energy	Disagree	R1 is ambiguous when referring to "Joint-Owned Units", and we believe that the word "owns" should be replaced with "owns and operates." In a joint-owned facility, the operator typically has responsibility for compliance with NERC standards.
3.48	Wolverine Power	Disagree	See comments listed for 1.a
3.49	NextEra Energy Corporate Compliance	Disagree	See comments to 1a. In addition, NextEra believes if the introduction of "functions" is another area that could lead to misunderstanding. If left, we recommend it only be for "informational purposes" and not controlling. As stated above, the specific list of components in BES Cyber Systems of Control Centers, Generators and Transmission should be what is controlling and protected. Also, as the drafting team will see throughout these comments, language that can be misunderstood will be proposed to be changed. The drafters often spoke of their intent, and while this term is widely used by the industry and it always means well, it is not a compliance/regulatory term the serves the industry, NERC or FERC well. The intent of the drafting team is not recognized as record evidence, nor is it controlling in an audit or before NERC or FERC. Thus, preambles should be clear. For example, "Purpose: To provide clear understanding of what BES Cyber System Components must be protected consistent with CIP-011-

#	Organization	Yes or No	Question 3 Comment
			1.”Similarly, NextEra is not supportive of using technical guidance papers to supplement the Standards. NextEra believes the Standards are what NextEra will need to comply with and the guidance papers, unless approved by FERC, are not controlling from a compliance perspective. Moreover, guidance papers tend to be loosely written and subject to being misunderstood. NextEra would rather see the specifics in the Standards.
3.50	MWDSC	Disagree	Situational Awareness is a new term that will be confused with Monitoring and Control function in Attachment I. The term "Control and Operation" was changed from prior draft to "Monitoring and Control". Shouldn't situational awareness be performed by the same operator? Suggest deleting Situational Awareness and revising the Monitoring and Control function as follows:"Activities, actions and conditions that provide monitoring and control of BES elements, including the assessment of current, expected, and anticipated state of the BES.
3.51	Matrikon Inc.	Disagree	Still open for interpretation, in its most simple form the only action words are “execute” or “enable” that correspond the cyber system to each of the functions. Please provide further definition or guidance on its application.
3.52	Southwest Power Pool Regional Entity	Disagree	The ability of the entity to group its cyber assets into cyber systems as it sees fit potentially offers an opportunity to game the system by dissecting legitimate cyber systems into smaller groups of components with less span of control and thus lower impact. There needs to be some sort of sufficiency criteria to ensure proper logical grouping. Additionally, a concern to the auditor is the ability to ascertain that the entity has identified all of the pertinent cyber systems and that all of the necessary cyber system components have been accounted for. Lastly, consider modifying the phrase “...that it owns to execute or enable...” to read “...that it owns to execute, enable, or support...”
3.53	APPA Task Force	Disagree	The APPA Task force disagrees with the proposed requirement but we offer the following suggestions:We suggest that naming Attachment I “Functions ....” will create

#	Organization	Yes or No	Question 3 Comment
			confusion with the "Functional Model". We suggest renaming Attachment I "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in response to Question 6. There are many different business models in our industry, and "ownership" may not mean "owns and operates." Therefore we would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has any control of the BES Cyber Systems installed, and/or the related day-to-day compliance with NERC standards.
3.54	Nuclear Energy Institute	Disagree	The current CIP-002 provides a risk-informed approach to the identification of assets critical to the reliability of the bulk-power system. The current practice is for a generator owner/operator to coordinate with the local transmission owner/operator to determine if the generator is critical to maintaining the reliable operation of the Bulk-Power system.The proposed CIP-010-1 eliminates this risk-informed approach, and would require all generators of any size to be required to comply with the CIP Standards even if the BES would not be adversely affected by the loss of the generating facility.NEI believes that the proposed methodology in CIP-010-1 is contrary to the intent of section 215 of the Federal Power Act (FPA) (16 U.S.C. 824o) which is to prevent instability, uncontrolled separation, or cascading failures as the result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.In order for CIP-010-1, R1 to be acceptable, reliance on an analysis by the transmission system owner/operator must be performed to determine if the generator operator/owner facilities are critical to the reliability of the bulk-power system.
3.55	GTC & GSOC	Disagree	The definition unnecessarily restates detail that should be in the definition of BES Cyber Systems. We recommend it be simplified to state the following "Each Responsible Entity shall identify and document each of its BES Cyber Systems in order to apply Cyber security requirements."

#	Organization	Yes or No	Question 3 Comment
3.56	FirstEnergy Corporation	Disagree	The definitional terms for Control Center, BES Cyber System and BES Cyber System Components in conjunction with the Requirement R2 "Impact Categorization (Attachment II)" should provide sufficient direction to the "programmable devices" that are within in scope and require protection under the proposed CIP standard. The R1 requirement places an unwarranted compliance documentation burden on the industry with questionable reliability payback. FE suggests that R1 and its corresponding Attachment I can be eliminated from the standard.Secondly, the requirement describes two unique actions - identify and document - BES Cyber Systems. "Documenting" the identified BES Cyber Systems is actually evidence of compliance that should be left to the Measures and not explicitly stated in the requirement. Failure to identify a BES Cyber System poses a real reliability risk to the BES, however, identifying and protecting a BES Cyber System but only neglecting to include it in a documented report is an administrative task with no reliability risk.
3.57	USACE - Omaha Anchor	Disagree	The owner may be a distant owner - I feel it should be operators - or the owner in conjunction with the operator.
3.58	Detroit Edison	Disagree	The phrase "to identify BES Cyber Systems for the application of security requirements" at the end of R1 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R1 to: Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES.
3.59	Indeck Energy Services, Inc	Disagree	The R1 requirement ignores the risk based assessment methodology that is required by FERC-see Order 706. [suggested replacement language] "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions, defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES, and perform a risk assessment according to its risk based assessment methodology of the impact on the reliability of the BES to identify a BES Cyber Systems for the application of security requirements."

#	Organization	Yes or No	Question 3 Comment
3.60	US Bureau of Reclamation	Disagree	The unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Whether the changes are made to the Attachment or within this requirement is immaterial. The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The title of Attachment to is incorrect in the requirement.
3.61	Platte River Power Authority	Disagree	There can be some confusion regarding who is responsible for implementing and demonstrating compliance with the CIP standards under certain circumstances (e.g. joint ownership). It would be helpful if there was a mechanism to identify the “Responsible Entity” responsible for implementing and demonstrating compliance for various Assets. The “Responsible Entity” designation could also include operators and could vary based on standard\requirement. For example:The designated Responsible entity is the owner unless specified otherwise.For Assets where an owner is not the designated Responsible Entity:- The owner must document an agreement with the designated Responsible Entity including the Asset(s) and requirements the designated Responsible Entity is responsible for.- The designation must be to a NERC Registered Entity.- The designation must be reviewed and reaffirmed annually
3.62	Manitoba Hydro	Disagree	This is satisfactory if identifying the cyber system with a reasonably short descriptive overall functional summary is sufficient. It is unsatisfactory if each and every single component of the cyber system must be described in some detail. Since some of the requirements in CIP-011 are at the BES Cyber System Component level, the need to identify the components should be explicitly required in the standard. Requirement R1 is unclear as drafted. It is not clear if the phrase “to execute or enable one or more functions...” describes the purpose of identifying BES Cyber Systems, or if it describes a

#	Organization	Yes or No	Question 3 Comment
			necessary characteristic of the BES Cyber Systems. Note that in Measure M1, "to" is replaced with "that", creating an inconsistency between Requirement R1 and Measure M1. Measure M1 is not a complete sentence. What needs to be documented?.
3.63	Southwestern Power Administration	Disagree	Though identification of BES Cyber Systems may be beneficial, adding prescriptive categories such as those included in Attachment I only add another layer of administrative "check-listing" for compliance purposes and do not actually have a positive effect on reliability. If Attachment I is intended as guidance in understanding the functions essential to reliable operation of the BES, it would be more appropriately included in a guidance document.
3.64	Midwest ISO	Disagree	We do not believe that it is necessary to document what function its BES Cyber Systems perform in attachment I. We believe that it is only necessary to test them against the criteria established in Attachment II. Developing inventory lists of what BES Cyber Systems performs what functions in Attachment I would increase the risk of a coordinate attacks should the information get into the wrong hands.
3.65	We Energies	Disagree	We Energies agrees with EEI comments. Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.66	Madison Gas and Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards. Attachment 1 requires clarification.Balancing Load and Generation, Controlling Frequency (Real Power) and Controlling Voltage (Reactive Power) are Functions Essential to Reliability Operation of

#	Organization	Yes or No	Question 3 Comment
			the Bulk Electric System but do not contain the modifier of BES as in Monitoring and Control does. Is it implied that the listed functions are only those functions Essential to Reliability Operation of the Bulk Electric System? Please clarify.
3.67	MRO's NERC Standards Review Subcommittee	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.68	The Empire District Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.69	Alberta Electric System Operator	Disagree	We find the current wording somewhat confusing. Consider rewording the sentence. As a suggestion, "...that it owns that executes or enables one of..."
3.70	Oncor Electric Delivery LLC	Disagree	We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems. Is the relaying scheme at a single substation a "system" and all the individual relays are "components", or is the primary and backup relays for a single line terminal, bus, or transformer the "system" and the individual primary/backup relay is a "component". This is basic to the implementation of this standard and needs to more fully defined.

4. **Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

The majority of the concerns raised in the comments were related to Appendix 2, the criteria used for categorization.

Specific concerns about categorization are addressed in the responses to Q7 and in the criteria which were approved by industry for Version 4 of CIP-002.

In CIP-002-5, this requirement has been consolidated with Requirement R1 of the previously posted CIP-010-1, to create CIP-002-5 Requirement R1 as follows:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*.

#	Organization	Yes or No	Question 4 Comment
4.1	WECC	Agree	Agree with the comment but it is unnecessary to utilize the phrasing "...for the application of Cyber Security requirements commensurate with the potential impact on the BES." The following rewrite is proposed;R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System(s) identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1. (Violation Risk Factor: High)
4.2	LCEC	Agree	Agree with the intent of the requirement but need to clarify the content of the attachment.

#	Organization	Yes or No	Question 4 Comment
4.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
4.4	FirstEnergy Corporation	Agree	FE supports R2 and the Impact Categorization achieved through Attachment II. Attachment II provides much needed clarity, compliance certainty but most importantly a consistent application of the critical infrastructure required to be secured within the context of the proposed CIP requirements.Suggested improvements to Attachment II are provided in our Question 7 response.As described in Question 3 above FE believes that R1 and Attachment I are not needed within the standard and that terminology for Control Center, BES Cyber System and BES Cyber System Components is sufficient. Therefore, conforming changes would be needed in R2 for a removal of R1/Attachment I. For example, "Each Responsible Entity shall document an impact categorization of its BES Cyber Systems consistent with CIP-010 Attachment ...."Requirement R2 and its corresponding Attachment II provides no guidance on whether digital relays colocated at a Transmission Facility need to be treated as individual BES Cyber Systems. FE recommends that the team clarify that a responsible entity could generically reference "Digital Relay Protection System" as a BES Cyber System located at a particular Transmission Facility (substation). There should be no need to identify/document each individual digital relay as a separate and unique BES Cyber System. Rather, the digital relay would be viewed as BES Cyber System Component of the Transmission Facility protection system. This will simplify compliance documentation, particularly for devices that may be associated with a Low Impact categorization.
4.5	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
4.6	NextEra Energy Corporate Compliance	Agree	In general, NextEra is supportive of the high, medium and low impact approach. However, in response to question 7, NextEra addresses concerns of the low impact approach.

#	Organization	Yes or No	Question 4 Comment
4.7	Minnesota Power	Agree	In order to increase clarity, Minnesota Power recommends the following changes to the language of Requirement R2: "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II, Impact Categorization of BES Cyber Systems. Each BES Cyber System's impact category will require the application of specific Cyber Security requirements commensurate with their potential impact on the BES."Minnesota Power believes that if a Registered Entity can support the exclusion of specific criteria identified in Attachment II with study data, then the Registered Entity should be allowed to exclude such criteria from further analysis.
4.8	Puget Sound Energy	Agree	Puget Sound Energy agrees with the language in R2, provided the language in attachment II is addressed (comments provided in question 7).
4.9	Con Edison of New York	Agree	See comments on question 7.
4.10	Platte River Power Authority	Agree	Suggest Revising:Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems for the application of Cyber Security requirements commensurate with the potential impact on the BES.
4.11	Reliability & Compliance Group	Agree	The categorization seems pretty straight forward however, it appears that you will be now excluding lots of "BES Cyber Systems" that were identified as CCA's originally and now will be just medium impact BES cyber systems.
4.12	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	The Requirement is sound in and of its self.
4.13	Bonneville Power	Agree	There need to be definitions of "High", "Medium", and "Low" impact. Attachment II describes how to determine whether a system meets the criteria for one of the impacts,

#	Organization	Yes or No	Question 4 Comment
	Administration		but doesn't give an overall explanation of what they mean. The CIP-002-4 draft included level definitions and that was a good idea. That level of detailed definition is not required; that detail is in Attachment II. But, a general impact level definition is needed, for example:"High: Loss of availability of the system leads to an unacceptable risk to the BES. Medium: Loss of availability of the system has a direct impact on the BES.Low: Anything else"These definitions will be used in answering the various questions about the tables.The objective of this requirement ("to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.In Requirement 2 the last phrase is "for the application of Cyber Security requirements . . . ." The last phrase in Requirement 1 is "for the application of security requirements." Are these two phrases supposed to have the same meaning? If so, shouldn't they use identical words? If not, what does "for the application of Cyber Security requirements . . . ." mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: "For the application of the Requirements contained in Standard CIP-011-1 . . . ."
4.14	Western Area Power Administration	Agree	Why is Cyber Security capitalized?
4.15	Independent Electricity System Operator	Disagree	(i) Medium impact categorization is based on an arbitrary generator nameplate rating of 1000 MVA, or voltage level of 200 kV and number of lines, with no regard to actual impact. The same is true of Special Protection Systems. Thresholds should be determined according to studies or other criteria determined by the Reliability Coordinator. As currently drafted, these criteria would significantly reduce the MW currently identified as 'Critical Assets' and protected within our Reliability Coordinator

#	Organization	Yes or No	Question 4 Comment
			area. (ii) The 3 impact levels (H, M, L) create additional layers of management complexity to implement and maintain security processes and monitor compliance, with no commensurate improvement to reliability. Based on the proposed applicability of CIP 11 for H,M & L categories, it seems likely that the number of BES assets afforded the maximum level of protection will decrease from the current standards.
4.16	E.ON U.S.	Disagree	: CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 "High Impact Ratings" of the categorization of the BES Cyber Systems. E ON U.S. proposes that the Standard include only Control Centers and Backup Control Centers in the High Impact Rating category; all other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category.
4.17	BCTC	Disagree	Â Recommend sample BES Cyber Systems be provided for each impact categorization to help guide UtilitiesÂ (Attachment 2) Cost should not be a consideration as the focus is the reliable operation of the BES(Attachment 2) the impact categorizations are good for directing Utilities on how to categorize their BES Cyber Systems ... nice job!
4.18	USACE HQ	Disagree	As same as for question 3, I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of thresholds to assign risk levels to assets. Again, Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish real threshold levels to assing risk to the different assets and/or systems in the community.

#	Organization	Yes or No	Question 4 Comment
4.19	Entergy	Disagree	Asset categorization in Attachment II may be valid for any number of purposes, but cyber security is not one of them. Size does not matter in terms of potential adverse impact to the BES as a functioning whole from cyber threats. Connectivity and network navigability are what matter in terms of the ability to adversely affect the bulk electric system through cyber means. Size matters for grid engineering and nominal-state operational grid management, physical security attacks (e.g. terrorist attack), and destruction by weather conditions (e.g. tornado). The cyber attack surface salient to integrity of the BES as a functioning system is primarily where routable protocols (e.g., TCP/IP) are used to connect operating sites, e.g., substations to control centers, regardless of size. The correlation between asset size and potential risk to the functioning BES as a whole is a misapplication of an electrical engineering frame of reference to what is fundamentally a networked-computing security engineering problem. The current approach brings great numbers of asset sites in-scope for required application of cyber defense countermeasures where the threat does not warrant it, e.g., substations of any size that are only connected back to a control/data center using legacy serial communications lines. If the paradigm of size-based impact categorization is to remain in the final Standard, specific requirements also should be established for each different type of network connectivity employed between sites, i.e., routed, legacy serial, dial-up, wired/wireless LAN, etc. One size fits all requirements such as that currently drafted will require overkill in far too many instances relative to genuine threat. As written, the standards are binary in terms of applicability across the spectrum of size-based impact categories, resulting in unnecessary requirements for some asset sites, generally medium impact sites with serial line communications only. This approach is not supported by any evidence in the administrative record. By bringing a large number of low-risk asset sites (i.e., substations using legacy serial communication lines only) into the scope of the requirements, they are imposing significant costs which do not address the real risks. Conversely, too little emphasis in the Requirements is placed upon “low impact” sites where routable protocols are used, which present a clear and present danger for which heightened security measures are certainly warranted.

#	Organization	Yes or No	Question 4 Comment
4.20	Madison Gas and Electric Company	Disagree	Attachment 2 requires clarification. Criteria Number 1.3, per the NERC Glossary, Wide Area is: The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits. Please give and state the reference of “must run” and how entities should interpret what “must run” is. Must run is a market issue, and could be designated as must run but for only a week. Criteria Number 1.11, is the intent that the automatic aggregate load shedding be under a common control system as is stated in the current CIP 002 Standard? If that is the case, adding a comment to clarify the criteria would provide clarity as in criteria 1.2 "(if using a shared BES Cyber System)"?
4.21	IRC Standards Review Committee	Disagree	Attachment II - Impact Categorization of BES Cyber Systems does not recognize that there is another dimension of risk or impact that must be considered. The availability of alternative tools that provide the same functionality should be considered when categorizing these components (e.g. a High Impact BES Cyber System with a viable substitute could reduce it to a Medium Impact).
4.22	Garland Power and Light	Disagree	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line.General CommentNeed to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
4.23	Southern California Edison	Disagree	Attachment II defines the amount of generation under control as the rated capacity of

#	Organization	Yes or No	Question 4 Comment
	Company		the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000, respectively. This would place the system in a "low impact rating" according to the attachment. The Attachment II should be modified to account for only the capacity that can be controlled by the system.In addition, Attachment II designates as a high impact rating, "Each BES Cyber System that can affect operations for Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan." This should be clarified to show only BES Cyber Systems will be utilized during the period of time that the resource is providing actual Blackstart service. In SCE's case, if a Blackstart unit is on GMS during normal operating conditions, this should not make it a high impact rating in and of itself. If GMS will be used in the Blackstart plan to restore the system, then it should be included.
4.24	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall document categorization of each BES Cyber System identified in Requirement R1. Categorization must address the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems."
4.25	Tenaska	Disagree	Dependent on R1
4.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.1. As drafted BES Cyber Systems associated with generating facilities that have a Contingency Reserve obligation lower than their net Real Power capability would be forced to be in the High Impact Rating even though they may be only capable of producing 600 MW. I do not believe the drafting team is intending to capture generators at this capability level. I recommend

#	Organization	Yes or No	Question 4 Comment
			having a specific net real power generation threshold that could result in frequency decay to underfrequency load shedding levels and elimination of the term Contingency Reserve to ensure that a larger threshold is captured.Attachment 2, 1.8 1.8 Transmission Facilities and Generation Facilities are capitalized terms in parts of the draft but not defined terms in the NERC Glossary. Based on their use in the standard a definition should be established. For example, the debate on whether operation of generator interconnection facilities qualifies the operator for transmission operator status may lead to confusion as to who is responsible to categorize Transmission Facilities under this standard.Atachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in the Eastern Interconnection, X MWs in the Western Interconnection or X MWs in the Texas and Quebec Interconnections. The Interconnection megawatt thresholds should be treated seperatly and not combined.
4.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in a balancing authorities' interconnection. The Balancing Authority megawatt thresholds should be treated separately and not combined.Request clarification and definition for the term Generation Aggregation and shared BES Cyber System.
4.28	Exelon Corporation	Disagree	Exelon does not agree with all of the specific criteria in Attachment II. Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment or supporting documentation. One result of a deterministic criteria, in terms of a lost MW threshold and assuming all generators employing a common cyber system are lost "in combination" is that detailed studies of cyber impact on equipment are avoided. That is, it is no longer necessary to identify specifically which

#	Organization	Yes or No	Question 4 Comment
			critical assets are affected. With the change in paradigm, a simple identification that a cyber system is common to multiple generators will result in a determination of "High Impact".
4.29	Allegheny Energy Supply	Disagree	Generally agree with intent, however there should be a "None" category in addition to High, Medium, and Low. For example there are likely Cyber Systems on very small generators connected to low voltage transmission that could not have any adverse impact on the BES.
4.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
4.31	American Municipal Power	Disagree	I disagree with the structure of CIP-010, but I agree with the intent. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
4.32	Progress Energy - Nuclear Generation	Disagree	If a plant system at a nuclear facility is in scope for NERC CIP Standards, additional categorization is not needed.
4.33	Public Service Enterprise Group companies	Disagree	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6 requires that only the "primary cranking path" transmission facilities need to be categorized with a "High Impact Rating". Statement 1.6 implies that some Blackstart

#	Organization	Yes or No	Question 4 Comment
			Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
4.34	National Grid	Disagree	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue.
4.35	Luminant	Disagree	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ... This should be reinstated.
4.36	Matrikon Inc.	Disagree	My suggestion is that the term “system” is replaced with “component”, as that is how the security controls of CIP-011 will be applied (to individual cyber components). A typical control system is built of multiple components, and some are more important than others (eg. operator stations versus controllers). As a whole, they work together to control generation or transmission, and identifying impact of each component will help with the application of CIP-011-1.
4.37	Seattle City Light	Disagree	NERC should first assess the effectiveness of the existing standards before proposing replacements. The current Requirements haven’t yet had the chance to undergo a full assessment for effectiveness. The impact of adopting CIP Requirements was tremendous and forced utilities to develop and implement new operational processes at a great expense. The first round of CIP Spot Checks is just now underway and is providing the first validation point for interpretations of the standards (and our first

#	Organization	Yes or No	Question 4 Comment
			round of significant penalties.) Utilities are now at a pivotal point in maturing their CIP compliance programs. Drastically changing the requirements now is a common reaction to newly introduced regulatory compliance frameworks and NERC should learn from the mistakes of other regulatory bodies that now have mature compliance frameworks (i.e., PCI, HIPAA, SOX.) Opportunities to further mature and improve the effectiveness of our CIP compliance programs will not happen if the proposed methodology is adopted in the near future. The cost and resource expense will shift to adapting to the new standards which carries a significant opportunity cost from a risk perspective.
4.38	Duke Energy	Disagree	R1 and R2 should be reordered and reworded (see comment on Question #3 above). Also, the quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System instability, separation, or cascading failures.
4.39	San Diego Gas and Electric Co.	Disagree	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have “BES outage” implications but not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole. Do the HIGH or MEDIUM impact categorizations consider redundancy and functionally equivalent back-ups? SDG&E recommends that this be taken into account during the categorization process.SDGE is concerned about the sheer number of assets that will be tagged “High impact” with the definitions presented in Attachment II, leading to a much larger compliance workload by entities with these new CIP Standards. Will all of these efforts bring significant additional

#	Organization	Yes or No	Question 4 Comment
			reliability to the BES?In paragraph 1.14, SDG&E has a concern about the last portion of the last sentence that reads "functionality that remotely controls a BES Cyber System with a High Impact Rating." That verbiage has the capability of causing many additional assets to fall in-scope that do not necessarily need to be. Suggest striking those words out of 1.14 since there are other protections in place within other requirements to protect the BES Cyber Systems with a High Impact rating.
4.40	Wolverine Power	Disagree	See comments listed for 1.a
4.41	Manitoba Hydro	Disagree	See comments to Question 3.
4.42	Indeck Energy Services, Inc	Disagree	The Impact Characterization of BES Cyber Systems is arbitrary and overly simplistic. It groups all facilities, regardless of the functions from Attachment I that they may or may not be able to perform and the significance of that type of facility to providing that function, in three arbitrary categories, LOW, MEDIUM and HIGH. The LOW category sweeps too broad a stroke. For generators, it arbitrarily includes, as a minimum, all generators less than 1,000 MW, regardless of type or capability to provide any or all of the functions from Attachment I. For example, one 150 MW generator providing "Controlling Voltage (Reactive Power)" has much less, probably a de minimis level, of support compared to a 999 MW generator. Wind generators are intermittent and non-dispatchable and, unlike dispatchable generators which are almost all running at high loads at high load times, when Controlling Voltage is a problem, are unlikely to be running near full load at those times. The categorization needs to be much more specific to the facility being categorized under CIP-010 and the function to be performed. Although the CIP-010 and CIP-011 are already voluminous, in order to positively affect BES ALR, they need to be restructured to reflect the complexity of the BES and not arbitrarily set LOW, MEDIUM and HIGH categories. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, for each of the functions in Attachment I.

#	Organization	Yes or No	Question 4 Comment
4.43	PacifiCorp	Disagree	The initial wording “Each BES Cyber System that can affect operations for” should be clarified or additional clarification added to some of the following items. For example the wording above, together with the wording associated with 1.8 give fairly good guidance, but the wording applied to items 1.4 and 1.5 are not as clear. The wording “affect operations” can have many meanings ranging from minor operational issues to total loss of the facility. The phrase “singularlity or in combination” in Item 1.1 of Attachment II seems to be attempting to incorporate multiple units of an integrated plant, but the parenthetical does not effectively convey that concept. While item 1.1 ties back to the Contingency Reserve and the Reserve Sharing Group, it does not provide definitive guidance regarding which Facilities are meant to be incorporated into the requirement since this value is not easy to obtain and may by definition change year to year. Also, item 1.3 seems to be an “either/or” catch-all related to item 1.1, but there is no indication of who determines which units are “must-run” units. It is unclear how A BES Cyber System, if rendered unavailable, degraded, compromised, or misused, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES could fall into anything other than High or Medium impacts.
4.44	US Bureau of Reclamation	Disagree	The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The remaining parts of sentence should be deleted.
4.45	Detroit Edison	Disagree	The phrase “to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES” at the end of R2 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R2 to:Each Responsible Entity shall categorize and document such categorization of each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of

#	Organization	Yes or No	Question 4 Comment
			BES Cyber Systems.
4.46	Progress Energy (non-Nuclear)	Disagree	This is a good approach to apply protection based on an impact level vs. an all or nothing approach. The trigger levels (MW, MVar, etc) need to be reassessed - are these realistic / practical? This requirement is going to involve extensive effort and coordination between work groups. The DSCADA master that could control all T/D substation capacitor banks would be included. The term misused shows up a couple more times in Attachment II. It would appear that 1.11 includes the T/D Substation under frequency relaying. This is installed in almost every T/D substation which would require some level of access control.What is a generation facility versus a unit?Do we need to identify each cyber component of the BES Cyber System or just the (sub)system itself? Our interpretation of R1, R2, & R3 is that the requirements are driving us to identify Cyber subsystems. If we design small Cyber subsystem architectures we could get to Low impact categorization for each defined subsystems?Are the requirements aimed at subsystem level or overall system? An example would be to design a simple cycle Cyber system (Siemens T3000) architecture for combustion turbines alone and a second Cyber system (Ovation) for the balance of plant. We can make these independent systems at the process level and thereby minimize their respective impacts on the BES. Is that NERC's intent?
4.47	Southwestern Power Administration	Disagree	This requirement seems to be an excellent candidate for performance/results-based criteria rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity.
4.48	MWDSC	Disagree	Unclear how much supporting documentation or explanation is required to demonstrate how your system applies or doesn't apply to each of the subcategories. For example, would a table with "yes", "no", or "not applicable" and certified by a SME be sufficient?
4.49	Turlock Irrigation District	Disagree	We agree with the principle of the Requirement, however, we disagree with some of the

#	Organization	Yes or No	Question 4 Comment
			High Impact Rating criteria in Attachment II, as explained in question 7 below.
4.50	Midwest ISO	Disagree	We do not believe the drafting team has developed a justification for moving away from the Critical Asset concept. We understand that the regulators have a concern about the level of Critical Assets identified but that could mean the criteria simply needs to be more stringent for selecting Critical Assets. If the categorization approach is maintained, at a minimum, a no or negligible impact category should be adopted. There are BES Cyber Systems that simply cannot have an impact on reliability and therefore the CIP standards should not apply to them.
4.51	Ameren	Disagree	We generally agree with the criteria used to identify "High" impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as "Medium" impact, but should be classified as "Low" impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as "Low" impact, as they likely have little impact on the BES.
4.52	Verizon Business	Disagree	In Attachment II, Item 1.1 regarding Generation Facilities, references to "Contingency Reserve" or "Reserve Sharing Group" should be removed. Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW, should be included as a High Impact Rating. Referring to the "Contingency Reserve" is confusing and could result in the incorrect or inconsistent declaration of a generation asset as a High or Medium impact.

5. **Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:**

   3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

   3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

   3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

   Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many entities expressed concerns about the requirement to review the categorization following a planned change. Others expressed concerns again on the emphasis on ownership, but asked for the addition of "or operates".

In response to these comments, the requirement has been restructured, separating changes to the BES and categorization, and periodic reviews and approvals. More specificity has been added in the requirements as to when the categorization has to be updated upon a change. The SDT continues to believe that owners should be responsible for compliance and that the responsibility to operators should be the subject of agreements between the owners and operators.

#	Organization	Yes or No	Question 5 Comment
5.1	Progress Energy (non-Nuclear)		Agree that there needs to be a periodic review set cycle as well as a process to assess the impact for current projects. One concern could be how we deal with multi-phase projects that may extend over years.3.2 should not require that the whole identification and categorization process be redone for any 'planned changed'. Suggest changing the wording to 'review the identification and categorization of its affected BES Cyber Systems as a results of any planned change to the portion of the BES that it owns.'
5.2	MWDSC		Although R3 generally appears reasonable, cannot comment on specified times until all the requirements are finalized.

#	Organization	Yes or No	Question 5 Comment
5.3	National Rural Electric Cooperative Association (NRECA)		In R 3.3, please provide an explanation on "when applicable" -- explain this so that both the auditor and a registered entity can understand the "when applicable" circumstances.In R 3.3, what is meant by "such change" -- is it referring to actions related to R 3.1 and 3.2? If yes, ensure the standard is clear about this in order to minimize confusion about what is required.
5.4	Arizona Public Service Company		Potential confusion may exist without guidance or criteria that indicate how, specifically, a BES Cyber System Component should be identified. This is a problem of specificity in uniquely identifying a Component versus generically categorizing types of Components. This also relates to CIP-011 R23 and the inventory. Some potential options for specificity include manufacturer, model, serial number, assigned name or unique identifier, and location (logical and/or physical). Concerns with inventory management and uniquely identifying include how to better determine if a Cyber System Component has been modified or replaced with a different one, etc.
5.5	FEUS	Agree	3.2 is not clear when the entity is required to review the identification and categorization as a result of a planned change. 3.3 require documentation to be updated relative of changes from R1 and R2 within 45 calendar days. The drafting team should consider clarification for 3.2 either prior to implementation/completion of the planned change or within xx days.
5.6	Constellation Energy Commodities Group Inc.	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes. Also recommend adding provisions for re-evaluating new systems prior to going live.
5.7	Constellation Energy Control and Dispatch, LLC	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes.
5.8	WECC	Agree	Agree with the general requirements, but for clarity and auditability the following rewrite is suggested.R3 Perform a documented review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and

#	Organization	Yes or No	Question 5 Comment
			categorization. R4 Perform a documented review the identification and categorization of its BES Cyber Systems as a result of any planned or unplanned change to the portion of the BES that it owns.R5 Update or reaffirm the documentation specified in Requirements R1 and R2 within 45 calendar days from the completion of reviews as required by R3 and R4.Also suggest that the SDT consider requiring documentation be updated PRIOR to completion of the change.
5.9	Florida Municipal Power Agency	Agree	Although FMPA agrees with the intent of this requirement, we believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap for significant changes to BES Cyber Systems. In addition, ownership of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations and it would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator to operate the BES within its operational scope. FMPA recommends deleting 3.3 and replacing 3.2 with the following:"3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in service date of such change."Such language would result in the need to plan ahead of time and ensure the documentation is developed, but not necessary implemented until the in- service date of the new equipment.FMPA also recommends adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:"3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in service date of such change."
5.10	Minnesota Power	Agree	Minnesota Power recommends the following wording change to increase the clarity of Part 3.2, "...as a result of any planned and implemented change..."
5.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam	Agree	Need to clarify what is required for temporary situations, such as a normal open closed to allow maintenance. The closing of the open would be a "planned change," but only

#	Organization	Yes or No	Question 5 Comment
	Group		temporary. The Change in status of a BES Cyber System would be a wasted compliance effort for only a short duration.
5.12	US Army Corps of Engineers, Omaha Distirc	Disagree	"planned change" in 3.2 needs to be qualified. Suggest changing to "planned change likely to alter the impact of the associated BES cyber systems." Changes to BES Cyber Systems that could change their impact on the BES should also be considered.
5.13	Covanta Energy	Disagree	3.1 - If no changes have been made to any BES Cyber Systems, would suggest changing review period from 36 months to 60 months.... need to reduce administrative activities to allow more focus on reliability based activities.
5.14	Duke Energy	Disagree	3.1 is part of change control. Do we still need this review? Also, 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change.
5.15	Southwest Power Pool Regional Entity	Disagree	3.2 assumes that the BES Cyber System owner is also the owner of the BES assets being changed. This is not always the case. There are, for example, numerous instances where the Balancing Authority, Transmission Operator, and / or Generation Operator is not the Transmission and / or Generation Owner. Some sort of mandatory coordination is required to avoid this important requirement from falling through the cracks. 3.3 only requires a documentation update to be completed upon a change to the BES. This requirement should be modified to also require a documentation update upon a change to the BES Cyber System configuration, including adjustments to the list of components and supporting networks.
5.16	LCEC	Disagree	3.2 Change "owns" to "owns or operates". "Any planned change" may not be signficant enough to justify a full review.
5.17	Hydro One	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should

#	Organization	Yes or No	Question 5 Comment
			be considered.
5.18	Northeast Power Coordinating Council	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should be considered.
5.19	BCTC	Disagree	Â Preference would be to retain the current process of an annual review BES Cyber Systems and impact categorizationsÂ Please consider that if a change occurs that results in a BES Cyber System’s impact categorization increasing (i.e. from medium to high) the resulting effort to bring this system into compliance could be substantial (i.e. 6 to 12 months); how are these types of scenarios covered under Version 4?
5.20	USACE - Omaha Anchor	Disagree	A) 3.2 - any planned changes to the “cyber-system” portion of the BES that it owns. Otherwise you would be continually reviewing the plansB) 3.1 - would prefer to strike 3.2 and change 3.1 to 12 months.
5.21	Ameren	Disagree	Ameren feels that 45 days is too short and is also an uneven boundary that is hard to track. We would recommend changing it to a more even boundary such as bi-monthly (60 days) or quarterly (90 days). In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved and implies a perfectly complied with Configuration Change Management Program. Suggest adding “or as a result of the periodic review” at the end of R3.3.
5.22	E.ON U.S.	Disagree	CIP-010-1, R3.2 creates arguments that parties must constantly assess and re-assess their Impact Ratings of facilities. This is particularly true given that changes to the BES occur on a daily basis. Parties should be permitted expressly to engage in an annual assessment and a reassessment should only be required for “any major planned change to the portion of the BES that it owns prior to implementation of such plan.”CIP-010-1, R3.3 should read, “Update, when applicable, the documentation specified in

#	Organization	Yes or No	Question 5 Comment
			Requirements R1 and R2 within 45 calendar days of the completion of such major changes to the BES."
5.23	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
5.24	PacifiCorp	Disagree	Comments: The term "Any any planned change" used in 3.2 is terribly open-endedshould be more specific to avoid including small planned changes that have a de minimis impact on the identification and categorization of BES Cyber Systems. There must be some operationally prudent, de-minimus changes that can be made without triggering the 45 day change reviewIn addition, PacifiCorp suggests the following:. Change Modify item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.25	Black Hills Corporation	Disagree	Define "change" in terms of those alterations to BES Cyber Systems which may modify the functional identification or an impact categorization. There are numerous minor changes which clearly will not change either Attachment I or II assignments and would not need to be tracked. If they are not tracked, an entity will not be able to prove compliance.
5.26	Exelon Corporation	Disagree	Exelon is concerned that this Requirement implies that each BES Cyber System Component will need to be classified as High, Medium or Low Impact. If this is the case, this will result in a major change management initiative with field personnel and add unnecessary administrative burden and expense with no resulting benefit to the reliability of the BES. Given that concern, Exelon suggest that Requirement 3.2 be modified to read "review the identification and categorization of its applicable BES Cyber Systems as a result of any planned change to the portion of the BES that it owns." Exelon has several concerns as to how this Requirement would be audited. As written, Requirement 3.2 could be interpreted to mean that ANY change to the BES, whether it impacted a BES Cyber System or not, would necessitate a 45 day review and documentation. Furthermore, what is the definition of "planned"? Exelon is concerned

#	Organization	Yes or No	Question 5 Comment
			that like-for-like emergent equipment replacements would likewise necessitate a 45 day review and documentation.
5.27	Dominion Resources Services, Inc.	Disagree	Extending the window for periodic validation of the identification and categorization of BES Cyber Systems is an improvement given the additional requirement to review the impact of planned changes. The current language implies that all identified and categorized BES Cyber Systems must be reviewed each time a change occurs to any single system, although the intent is only to determine the impact of the change. How that determination is made should be at the discretion of the Responsible Entity. The wording for R3.2 should be changed to more accurately represent the intent as follows:"...determine whether planned changes to the portion of the BES it owns, requires the identification of additional BES Cyber Systems or changes or impacts the categorization of any existing BES Cyber System."
5.28	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of these requirements, 3.2 ". . . of any planned change to the portion of the BES that it owns or operates", 3.3 "Update within 45 calendar days, the documentation specified in Requirements R1 and R2 when the review required in 3.1 or 3.2 indicates a change."
5.29	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.2, we believe the word "planned" should be replaced with "incorporated". Otherwise, an entity could end up identifying and categorizing BES Cyber Systems that never actually end up getting installed.
5.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
5.31	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will

#	Organization	Yes or No	Question 5 Comment
			be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
5.32	Constellation Power Source Generation	Disagree	It seems the intent of R3.2 and R3.3 is to review and document any changes to a BES Cyber System that an entity owns, but instead it states "a change to the BES." An ownership change of a generation facility, or the change of an electromechanical overcurrent relay to a microprocessor overcurrent relay would change a BES Cyber System, but that doesn't change the BES. These requirements need to be rewritten to state BES Cyber Systems in place of BES.
5.33	Green Country Energy	Disagree	It would be nice to add a bit more definition to the timeframe. 3.1 within 36 months of last completed identification... 3.3 within 45 days of approved completion of such change...
5.34	Luminant	Disagree	Item 3.2 is unclear and very broad. Any planned change to the BES that it owns could simply be the changeout of an oil pump or boiler tubes. Luminant proposes two possible fixes. First, limit the review to changes that impact the BES Cyber Systems, or impact the High, Medium or Low rating. Even this is problematic in execution and enforcement. S
5.35	MidAmerican Energy Company	Disagree	Item 3.3 is not clear what does "update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES." mean. Change item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.36	National Grid	Disagree	National Grid recommends a local definition of "planned change". Also, clarify if planned change refers to an "approved" change. There are scenarios when planned changes are

#	Organization	Yes or No	Question 5 Comment
			not approved by Senior Management for various reasons. Should the planned change still be “reviewed”? What about “unplanned changes”?
5.37	NextEra Energy Corporate Compliance	Disagree	NextEra suggests combining 3.2 & 3.3 as follows:3.2 For any planned change that results in a BES cyber system re-categorization (low, medium, high) the documentation specified in R1 & R2 will be updated within 45 days of the completion of such change.NextEra also suggest eliminating or specifically defining what constitutes a change that needs to be documented, such as a hardware modification, or change to network connectivity.
5.38	Progress Energy - Nuclear Generation	Disagree	Nuclear facilities are required by multiple the Code of Federal Regulation (CFR)requirements to maintain configuration control of components. Plant systems and components subject to Cyber Security regulation, either by FERC/NERC or other regulatory agencies are maintained under configuration control due to the CFR programs. Revisiting the classification of assets is not needed to enhance configuration control as on-going design control and configuration management processes are applied to meet the legal requirements implemented by CFR.
5.39	The United Illuminating Co	Disagree	Proposed R3.3 uses the term “such change to the BES” is not clear. The use of the phrase leads to the belief it applies only to 3.2, Did the SDT intends R3.3 to apply to both R3.1 and R.32?Suggest rewording 3.3 to: Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of reviews required by R3.1 and R3.2.
5.40	Pacific Gas & Electric Company	Disagree	R 3.2 Understand the overall intent of 3.2, however "...any planned change to the portion of the BES..." essentially occurs on a daily basis so unclear on the overall feasibility of this requirement. Suggest 3.2 be more refined than "any planned change to the portion of the BES".
5.41	Reliability & Compliance Group	Disagree	R3.1 is unnecessary with a proscriptive program for identifying BES cyber systems. Therefore, you should only need to review the identification and categorization of your BES cyber systems if there is a planned change to the system or if there is a change to

#	Organization	Yes or No	Question 5 Comment
			the standard's definition of what is or is not a BES cyber system or system component.
5.42	American Electric Power	Disagree	R3.2 and R3.3 are triggered from changes to the BES. Depending upon what constitutes a change to the BES, there could be daily triggering events that would require the review and updates as stated in these two requirements. Will every BES Cyber System (including those not associated with the BES change) need to be reviewed and possibility updated for each and every change to the BES?Furthermore, it appears that it would be possible that a Responsible Entity could be in violation of R3 the Responsible Entity could also be in violation of R1 and/or R2 as well. It appears that R1 and R2 are one-time initial events and that R3 is the on-going requirement replacing those events; however, if that is the intent it is not clear in that regard.
5.43	Consultant	Disagree	R3.2 'any' planned change is probably too broad. Should include addition or removal of BES assets, whether by construction, retirement, purchase, or sale of assets. Some qualification of the changes BES assets that would require review of the identification and categorization of a BES asset would be better. Possible wording "changes to cyber systems or physical protection cyber systems associated with BES assets...", which would appear to be consistent with R23 in CIP-011.Possible "unintended consequence" - requirement R3.2 as stated, and in the suggested changes, requires change control for all BES cyber assets regardless of impact categorization.
5.44	SCE&G	Disagree	R3.2 needs to be clarified regarding "any planned change to the portion of the BES that it owns". What constitutes a change? Is this a Transmission/Generation factility change, operational change, or a cyber systems change, or all three? This has the potential to be interpreted by auditors as needing to be reviewed anytime equipment is replaced.
5.45	Madison Gas and Electric Company	Disagree	R3.2 states " review the identification and categorization of BES Cyber Systems of any planned change to a portion of the BES that it owns". It is unclear how an entity will accomplish a review of a "planned" change. Recommend the "planned" be removed and supplement with "incorporated". R3.2 should read as:"review the identification and categorization of its BES Cyber Systems as a result of any incorporated change to the

#	Organization	Yes or No	Question 5 Comment
			portion of the BES that it owns".
5.46	ERCOT ISO	Disagree	R3.2: Consider: review and document the identification and categorization of its BES Cyber Systems as a result of any planned change to its BES Cyber Systems or BES Cyber System ComponentsR3.3: Recommend that the 45 days be changed to 30 days to align with the changes recommended under FERC Order 706 (i.e., section 651).
5.47	BGE	Disagree	Recommend adding provisions for re-evaluating new systems prior to going live.
5.48	ISO New England Inc	Disagree	Recommend that a local definition of "planned change" is needed. Suggest this definition excludes planned outages or maintenance. Possibly use "modification to Facilitiies" per FAC-009 as a starting point.
5.49	Detroit Edison	Disagree	Remove the "planned change" verbiage in R3.2. Consider changing R3 subrequirement 3.2 to:Each Responsible Entity shall: 3.2 Review the identification and categorization of its BES Cyber Systems as a result of any change to the portion of the BES that it owns that affects the classification of a BES Cyber System or causes the addition or removal of BES Cyber Systems
5.50	Nuclear Energy Institute	Disagree	Requirement 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change. Also, it would be helpful to clarify the term "change" to preclude the triggering of a review for something like a password change.Additionally, the phrase "adequate requirements" in the R3 introductory paragraph should be clarified to "adequate security requirements."
5.51	Southern California Edison Company	Disagree	SCE's concerns regarding Requirement 3.2 are three-fold: (1) Requirement 3.2 appears to require review of all BES cyber systems whenever any change in ownership of any portion of the BES occurs. SCE recommends the drafting team clarify that the review should only occur for systems that are impacted by the ownership change.(2) It is unclear whether Requirement 3.2 adds significant value to the reliability of BES because

#	Organization	Yes or No	Question 5 Comment
			planned changes may not be always approved or implemented as designed and actual changes made would, regardless, have to be documented by R3.3 within 45 calendar days.Finally, the drafting team should make the period after an unplanned change "time-bound" obligating RE's to develop plans to address compliance with CIP standards within a specific timeframe after which R3.2 would become applicable. This approach would be in agreement with the intent of Order 706 which places paramount importance on the reliability of the BES. It is also unclear from this requirement that the timeframe within which a system or component identified in R3 has to adhere to CIP-011. Such a timeframe should be clearly stated within the standard.
5.52	San Diego Gas and Electric Co.	Disagree	SDG&E doesn't necessarily have issues with the 36-month review requirement in R3.1. However, we do have a concern about the 45-day requirement in R3.3 due to the sheer number of BES Cyber Systems that could change. We suggest that this requirement be changed to 90 days so that entities will have adequate time to update appropriate documentation.
5.53	Network & Security Technologies Inc	Disagree	Suggest adding a requirement to review the identification and categorization of its BES Cyber Systems as a result of any planned changes to one or more of its BES Cyber Systems. "Planned changes" include but are not limited to hardware and/or software upgrades adding new functionality, addition of new BES Cyber Systems, retirement or redeployment of existing BES Cyber Systems.
5.54	Allegheny Energy Supply	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.55	Allegheny Power	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.56	Dynegy Inc.	Disagree	The 3.3 update should be extended to 6 months. This type of update could be detailed and require more than 45 days.

#	Organization	Yes or No	Question 5 Comment
5.57	APPA Task Force	Disagree	The APPA Task force agrees with some parts of the proposed requirement but we offer the following suggestions:We believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap that does not cover significant changes to BES Cyber Systems. In addition, “ownership” of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations. It would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator that it uses to operate the BES within its operational scope. We recommend deleting 3.3 and replacing 3.2 with the following:”3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in-service date of such change.”Such language would result in the need to plan ahead of time and ensure the documentation is developed, but that it need not be implemented until the in- service date of the new equipment.We also recommend adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:”3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in-service date of such change.”
5.58	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The change management requirements of CIP-011 necessitate lengthening the time to document completed changes to 60 days or more.
5.59	ReymannGroup, Inc.	Disagree	The dynamic and real-time nature of cyber security threats requires a minimum review cycle for identifying and classifying new or changing BES Cyber Systems to 12 months or less as determined by planned or unplanned changes to the BES. Therefore, we recommend revising 3.1 to a 12-month cycle and revising 3.2 to include planned and unplanned changes.

#	Organization	Yes or No	Question 5 Comment
5.60	Bonneville Power Administration	Disagree	The objective of this requirement (“To ensure the application of adequate requirements on its BES Cyber Systems") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence. The Requirement should not include the objective. That would clearly separate the objective from the action(s) that the Responsible Entity must take.3.2 doesn't define the magnitude of "planned change". As defined, it includes routine maintenance such as replacing conductors on a line. A better definition would be "...planned change to the architecture of the portion...". In any event, there must be some way for entities to determine which change triggers a review.
5.61	Manitoba Hydro	Disagree	The requirement needs to include a review of the categorization of the BES Cyber System as a result of a change in the BES Cyber System. Is the intent of Requirement 3.2 to review the identification and categorization of ALL its BES Cyber Systems as a result of ANY planned change to the portion of the BES that it owns? If so, this is excessive and should be limited to BES Cyber Systems impacted by the planned change. If the intent is to limit the review in Requirement 3.2 to the BES Cyber Systems impacted by the change, then the 36 month review in Requirement 3.1 could be continually reset, and an overall review never completed. The period for an overall review should be a fixed interval of every 36 months. Requirement 3.3 language is vague when referring to “such change”. If the intent is to update the documentation in when triggered by events in 3.1 and 3.2, then the language of 3.3 needs to be added to both 3.1 and 3.2. As a result, 3.3 can be deleted. Requirement R3.3 is incomplete or inconsistent as drafted. The first portion of Requirement R 3.3 refers to updating documentation specified in Requirements R1 and R2, which includes a 3 year review, yet the latter portion of Requirement 3.3 specifies that updating must be done within 45 days of a change. It is not clear when updates must be done after a three year review.
5.62	Alberta Electric System Operator	Disagree	The wording of R3.3 implies it is a sub-requirement of R3.2 because of the wording “such change.” Consider revising to “... within 45 calendar days of the completion of such review.”

#	Organization	Yes or No	Question 5 Comment
5.63	EEI	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change. The change has to be material to the classification criterion in Attachment 2 in order to trigger a review.As noted in EEI's response to Question 3, a Responsible Entity may not need to characterize all the BES Cyber Systems it owns (for example, jointly owned units). EEI suggests the following modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of material changes to the portion of the BES that it operates."
5.64	Southern Company	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change.R.3.2 requires the review of identification and categorization for planned changes. R3.3 requires an update of documentation related to these changes within 45 days of completion. The requirements of R3.2 would be difficult to audit and are better covered under R3.3.
5.65	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
5.66	Independent Electricity System Operator	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities. We suggest replacing this term with "the portion of the BES that it owns or operates".

#	Organization	Yes or No	Question 5 Comment
5.67	IRC Standards Review Committee	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities but do own Cyber Systems with which they operate the BES. We suggest to replace this term with "the BES Cyber Systems or the portion of the BES that it owns".
5.68	GTC & GSOC	Disagree	We are concerned with requiring an update of all BES Cyber System categorizations whenever planned changes are made to the BES. First, there is a gap here with respect to capturing the changes to the BES Cyber Systems themselves that may affect categorization. Also, this will likely create a complicated compliance tracking scenario for the entity who will be required to track a number of activities to ensure they are completed "within 12 months" of the categorization. We recommend replacing "within 36 months" in R3.1 with "annually" and completely removing both R3.2 & R3.3. This will allow the tracking of compliance activities to occur more on a programmatic basis rather than necessarily on a device by device basis.
5.69	Xcel Energy	Disagree	We believe 60 days is a more appropriate time to allow updating of document under Requirement 3.3. During certain times of the year, (i.e. end of year holidays and financial close out activities) 45 days can be challenging.
5.70	Alliant Energy	Disagree	We believe Article 3.1 is unnecessary and should be deleted. If an entity does an initial assessment and identifies and categorizes its BES Cyber Systems, the only time there would be a change to the listing is if the BES Cyber Systems were modified, which is covered in Articles 3.2 and 3.3. If the SDT determines that Article 3.1 is required, the timeframe should be revised to 60 months to correspond to other summary reviews required by NERC (ie; 5-year analysis of Black-Start capabilities).In Article 3.2 the word "planned" should be replaced with "installed" or "incorporated". There are many modifications planned that never get installed, so it is not reasonable to require all "planned" items to be included.In Article 3.3 the update period should be 90 days not 45, to allow the Registered Entity time to make the necessary changes. 45 days is not

#	Organization	Yes or No	Question 5 Comment
			adequate time to do the updates at the end of a project.
5.71	FirstEnergy Corporation	Disagree	We do not agree with the VRF of High assigned to this requirement and believe a Medium VRF is more appropriate. Violating R3 does not pose the same risk to the BES as violating R1 and R2.As written, 3.2 implies that every change to the BES would trigger a documented review of the cyber system list and becomes a burdensome compliance task. As a compromise we propose that you simplify R3 such that a review/update is required every 18 months.
5.72	We Energies	Disagree	We Energies agrees with EEI suggested modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates."
5.73	Midwest ISO	Disagree	We request that 3.3 be modified to 60 days rather than 45 days. We believe 45 days will be a challenge for most entities to meet as this effort will likely be incorporated into an entity's broader business continuity efforts.
5.74	Verizon Business	Agree	The requirement should provide guidance relating to when a utility needs to add a new BES system or component and what the timelines are for implementation of the CIP-010, R3 requirements.

6. **CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns that Attachment I is part of the standard and includes the use of many undefined terms. Others expressed concerns about the vagueness of many of the terms.

In response to these comments, the SDT has changed the definition of the Reliability Functions to **BES Reliability Operating Services**, and has included these terms in the Glossary. Some modifications have been made to more precisely define the context in many sub-definitions.

#	Organization	Yes or No	Question 6 Comment
6.1	Madison Gas and Electric Company		Recommend eliminating the word "conditions" used in the descriptions of the functions. It's not clear what "conditions" means in the context in which it is used in Attachment I. A function is a set of activities and actions to accomplish an objective or purpose. Such activities and actions may be automatic or manual or a combination of the two and certain tools and infrastructure may be inherently needed to fully execute the functions. In contrast, conditions are states that result from the execution of functions and/or the effects of external, sometimes uncontrollable, factors.Recommend Function section to read:CIP-010-1 - Attachment I Functions Essential to Reliable Operation of the Bulk Electric System The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes. Dynamic Response - Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES activity or action Balancing Load and Generation- Activities and actions for monitoring and controlling generation and load. Controlling Frequency (Real Power)- Activities and actions to control frequency within defined bounds. Controlling Voltage (Reactive Power) - Activities and actions to control voltage within defined bounds. Managing

#	Organization	Yes or No	Question 6 Comment
			Constraints- Activities and actions to maintain operation of BES elements within their design limits and constraints. Monitoring & Control - Activities and actions that provide monitoring and control of BES elements. Restoration of BES- Activities and actions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Situational Awareness - Activities and actions to assess the current, expected, and anticipated state of the BES. Inter-Entity Real-Time Coordination and Communication- Activities and actions for real-time coordination and communication between Responsible Entities' System Operators.
6.2	ISO New England Inc	No	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
6.3	Progress Energy (non-Nuclear)	No	A concern is that depending on how we identify the BES, the 'monitoring & control' function may be associated with many transmission lines that utilize microprocessor relays. Based on the definitions of BES Cyber System Component and the monitoring and control function, this could be interpreted as to being in consideration regardless of whether or not we connect communications to the relay.CIP-010-1 Attachment I - More guidance needed - There needs to be guidance on the definition of 'can have an effect on real-time operation of the BES within 15 minutes'. This leaves too much ambiguity in defining the Cyber Systems that could potentially be covered by the standards and at which level. It could even be interpreted to include systems which may even be beyond the control of the Responsible Entity. The definition needs to provide a bright line of distinction so that systems which have the highest potential of presenting a risk receive the greatest attention to enhanced security - rather than requiring finite resources to be spent filling notebooks with information about low risk Systems/Components.
6.4	Duke Energy	No	Attachment I should not be part of the standard, but should be in a guidance document.
6.5	Kansas City Power & Light	No	Do not agree with the "Inter-Entity Real-Time Coordination and Communication" as the description appears directed toward the devices and systems utilized for verbal communications between Regional Entities and the coordination that occurs as a result

#	Organization	Yes or No	Question 6 Comment
			of those interactions and is outside of the scope of cyber control systems that monitor and control the BES.
6.6	Con Edison of New York	No	One general comment is that CIP-010 should avoid using undefined terms, and use NERC Glossary Terms and cross-references to other Reliability Standards wherever possible.Attachment I is a list of "Functions Essential to Reliable Operation of the BES". The DT has attempted to re-define functions that are already documented in Standards. The definitions should be enhanced to reference the applicable Reliability Standards. o Dynamic Response: The only actions automatically triggered on BES elements are protection systems (see PRC Standards), UFLS systems (see PRC Standards), AGC systems (see BAL Standards), Special Protection Systems and AVR's (see VAR Standards). Everything else is manual operation. It is recommended that the term "Dynamic Response" be removed and replaced with "Automatic Response" and reference the applicable Standards. o "Balancing Load and Generation" and "Controlling Frequency (Real Power)" are the same action. This activity should reference the BAL standards which require BA's to balance generation and tie lines. o "Controlling Voltages (Reactive Power)": This function is addressed by VAR, TOP, and IRO Standards. o "Managing Constraints": If included, this action falls within BAL, INT and TOP standards which should be referenced. o "Monitoring and Control": The definition of the "BES Cyber System" is monitoring and control. Remove this and use the term in the introduction to Attachment I. o "Restoration of BES": This function is addressed by the EOP standards. o "Situational Awareness": Eliminate the "Situational Awareness" function, as this category is too broad and general. o "Inter-Entity Real Time Coordination and Communication": Reference the applicable FERC approved Standards.Also the phrase: "activities, actions, and conditions" at the start of each items is not clear. For example, is an alarm panel an activity, action or condition? Is an HMI computer an activity, action or condition?
6.7	Regulatory Compliance	No	Please see response to question 3.

#	Organization	Yes or No	Question 6 Comment
6.8	Southwestern Power Administration	No	Requiring Responsible Entities to utilize categories which are intended for guidance in identifying BES Cyber Systems, within the reliability standard; and then requiring Entities to be measured by having evidence that those Cyber Systems tie to the functions listed in Attachment I does not further the goal of maintaining reliability and adds complexity and confusion to the process. Attachment I should be converted to a guidance document.
6.9	San Diego Gas and Electric Co.	No	SDG&E would like to request clarification on a definition of the "situational awareness" function. It is too broad for us to effectively determine what assets might be in scope for this requirement. Similarly, we'd also like to request a definition of the term "BES element" in the Monitoring and Control section.SDG&E would also like to request clarification on the "Inter-Entity Real-Time Coordination and Communication" function. Is this meant to cover voice communication between entities or would it also cover electronic data communication between entities such as ICCP data links? We'd suggest that the ICCP links be specifically excluded because it doesn't fit the wording of "real-time coordination or communication between System Operators"
6.10	IRC Standards Review Committee	No	The descriptions for most of the functions in Attachment I are too vague that they cannot serve as a guideline for identifying which components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tempered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that

#	Organization	Yes or No	Question 6 Comment
			they perform one or more of the functions listed in Attachment I.
6.11	E.ON U.S.	No	The inclusion within the function "Situational Awareness" of current state of the BES creates an unnecessary overlap with the "Monitoring and Control" function. In addition, this inclusion appears to require tools such as a video wall fall within the scope of CIP standards despite it not being necessary to perform state estimation or operator monitoring of real-time events. E ON U.S. suggests the "Monitoring and Control" function explicitly include real-time monitoring of real-time or current state of the BES and "Situational Awareness" be limited to assessment of the expected and/or anticipated state of the BES. E ON U.S. also notes that in most cases "Restoration of BES" would be greater than 15 minutes The term "effect" in paragraph 1 of Attachment 1 should be defined.
6.12	Nuclear Energy Institute	No	The introductory paragraph should be revised to be more precise. First, "could" should be replaced with "would". Second, it is not clear what "within 15 minutes" constitutes. Leveraging the definition of BES Cyber System, an acceptable opening paragraph would be:The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that would have an effect on real-time operation of the BES within 15 minutes of the BES Cyber Systems that implement them being rendered unavailable, degraded, compromised, or misused.
6.13	Manitoba Hydro	No	The second sentence of Attachment I is unclear. Within 15 minutes of what? Is the reference to "real-time" necessary given the requirement to have an effect on the BES within 15 minutes?
6.14	Midwest ISO	No	We do not believe Attachment I is needed for anything more than a starting point for identifying BES Cyber Systems per Attachment II. Thus, it is not necessary to expand this any further.
6.15	PacifiCorp	Yes	- PacifiCorp agrees with EEI's suggested improvements for Attachment I below:The

#	Organization	Yes or No	Question 6 Comment
			"Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions to assess the current (real-time) state
6.16	Cogeneration Association of California and Energy Producers & Users Coalition	Yes	1. The first paragraph of Attachment 1 to CIP-010 states:". . . the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." This is a vague statement. Every device connected to the BES will have an effect on real-time operation but some device's effects will be negligible. Clarification is needed on how entities can determine if their assets have a material, non-negligible effect on real-time operation of the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.2. In Attachment 1 of CIP-010, Dynamic Response is defined as:"Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition." Examples or guidance on what is covered by Dynamic Response areneeded. For instance, would Automatic Generation Control be considered a Dynamic Response action?3. Attachment 1 of CIP-010 describes Controlling Frequency and Controlling Voltage as functions essential to reliable operation of the Bulk Electric System. Generators provide Real Power (Controlling Frequency) and Reactive Power (Controlling Voltage). However, we are aware of no disturbance to the BES due to loss of Real Power output or Reactive Power output from our generators. Further clarification is required regarding how impact on grid operations should be determined and measured when determining if a function is "essential" to reliable operation.
6.17	Florida Municipal Power Agency	Yes	Although FMPA agrees with the intent of Attachment I, we believe the definitions contained in the attachment can be significantly improved.As discussed in response to Question 3, FMPA recommends using the word "activities" (or other suitable synonym) for the word "function" to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, FMPA suggests:"Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated

#	Organization	Yes or No	Question 6 Comment
			state of the BES."FMPA has other recommended changes to help simplify and clarify the definition of terms used:"Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance." (Facilities and Elements do not perform any action, protection, control and cyber systems perform the action)Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and Load. (supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term "generation", and Load should be capitalized since it is in the Glossary)Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. (by definition, a BES Element is a Facility; hence, if this suggestion is not taken, then BES element ought to be eliminated from the bullet. Additionally, SOLs and IROLs ought to be discussed in this context and those terms subsume Facility design limits)Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. (the phrase "delivering electric power without external assistance" adds no value and is not supported by EOP-005).
6.18	Tenaska	Yes	As long as these functions are applied to High and maybe medium BES assets then the cyber system attached to them. Clarification to "monitoring" should be considered to limit applicability.
6.19	FirstEnergy Corporation	Yes	As stated in our response to Question 3 FE believes that adequate critical infrastructure protection and BES reliability can be accomplished without a need for burdensome compliance documentation of functions described in Attachment I. We encourage the team to carefully review its need and consider removing this aspect from the standard. Please see our response to Question 3 for more details.
6.20	Progress Energy - Nuclear Generation	Yes	Attachment 1 needs to clarify that nuclear generating stations defer to the principles of nuclear security first before consideration is given to the bulk electric system.

#	Organization	Yes or No	Question 6 Comment
6.21	Southern Company	Yes	Broad use of Situational Awareness and System Restoration in the BES functions list and definitions cause the scope of the standards to be overly broad, well beyond the point where there is any reliability benefit. Because there are very few programmable devices in any BES facility that do not have some relevance to one of the listed BES functions, the number of devices included in the standard compliance effort will mushroom unmanageably. The large majority of these newly-included devices pose no significant threat to the BES, but the effort of bringing them into compliance will both distract from the efforts to improve security and will reduce reliability by slowing emergency restoration response time.The function list and other parts of the standards should be modified so that only systems which are used directly in regional or larger Situational Awareness efforts or are relevant to the Entity's System Restoration Plan are included.In addition, the definition of "Restoration of the BES" is vague - does "a shutdown condition" refer to the BES being shut down or a BES component is shut down. The wording should be changed to clarify that it is the BES that is in a shutdown condition."have an effect on real-time operation" should be replaced by "have an adverse effect on real-time operation".
6.22	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
6.23	LCEC	Yes	Concerned about the 15 minute threshold.All functions should state: Activities, actions OR conditionsSituational awareness: What is the difference between expected and anticipated? This function could reference real-time system operations of the BES instead of the proposed BES Cyber System definition.
6.24	Southwest Power Pool Regional Entity	Yes	Consider modifying the opening statement to read "...can have an effect on real-time operation of the BES within 15 minutes if not mitigated. Clarify that the expectation is to assume the mitigation is not available or fails for the purposes of the BES Cyber System identification."

#	Organization	Yes or No	Question 6 Comment
6.25	Idaho Power Company	Yes	Controlling voltage needs to reference the voltage on the BES, not just voltage in general which could include distribution level. Situational awareness would seem to include a time window beyond the 15 minute criteria especially as it relates to anticipated state of the BES. Inter-entity Real-Time Coordination and Communication is very broad and pulls in communication systems that are required by other reliability standards to be redundant with plans in place to deal with loss of the primary communication channels. Unless all of the redundant systems are compromised, communication can still be accomplished between entities.
6.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Defining metrics is needed somewhere. For instance, requiring Low Impact compliance over Monitoring & Control of a 20 MW cumulative BES system would be outrageous. If real-time operation is interpreted by the auditor as isolation of a faulted line and Dispatch awareness that the line needs to be fixed, what reliability objective is obtained for the BES? Only local level of service is affected.Concerning “without external assistance” for Restoration of BES is not clear. A boundary is not defined so as to know what external help would be. Would this be the Balancing Authority boundary, or the Reliability Coordinator boundary?
6.27	ReliabilityFirst Staff	Yes	Definition of “BES Elements”, What does “external assistance” mean (restoration)?, Sit Awareness: what is “anticipated state”, does communication include functions such as phones or email?
6.28	Puget Sound Energy	Yes	Dynamic Response: This is a poor title, as dynamic response has a specific meaning in Electrical Engineering. The definition is too vague and could be interpreted to include a breaker operation due to a line fault, as this is a “response to a BES condition”. This definition would include the auto switching controls at nearly every distribution substation with a looped transmission line as a BES Cyber System.Controlling Frequency & Controlling Voltage: This definition would include Under Frequency Load Shedding (UFLS) and Under Voltage Load Shedding (UVLS) schemes, which in many cases only drop single distribution banks, effecting 15 MW of load, which has negligible impact on the

#	Organization	Yes or No	Question 6 Comment
			BES.Managing Constraints: This definition would include overcurrent relays, which may only trip a single 115 kV line that serves local load and has negligible impact on the BES.
6.29	EEI	Yes	EEI suggests that the term “Situation Awareness” be deleted because the term is vague and duplicative of the term “Monitoring & Control.” In the alternative, the “Situational Awareness” description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.
6.30	Exelon Corporation	Yes	Generation functions are not explicit in the Attachment I functions, but are embedded/inherent. As a generation owner/operator, Exelon could review the functions of Attachment I and conclude that generation is not a required function, a reasonable approach if considering loss of a single unit or station out of the entire BES. If adopting the proposed CIP-010 approach, we recommend explicit inclusion of generation as necessary to ensure the Adequate Level of Reliability of the BES.
6.31	The Empire District Electric Company	Yes	I disagree with keeping Attachment I in the standard. The conceptual discussion of functions only adds redundancy, complexity and confusion. The suggested changes to the definition of BES Cyber System and BES Control Center should be enough guidance to identify what is in scope. Therefore, I recommend that the SDT either eliminate Attachment I or convert it to a reference/guidance document supporting the standard
6.32	Consultant	Yes	I think the "15 minute" criteria needs additional clarification. As stated, "an effect on real-time operation of the BES within 15 minutes." is very broad. Suggest limiting to "adverse effect". Also could include some terminology about "adverse effect preventing or limiting the capability of BES assets to perform the listed functions."Suggest numbering the defined functions to allow easier cross-reference to this attachment.
6.33	Alliant Energy	Yes	In paragraph 1 the phrase “that can have an effect on real-time operation” needs to be

#	Organization	Yes or No	Question 6 Comment
			clarified. We believe it should be tied to and IROL, SOL, or degradation of the reliability of the BES. As written it is undefined and too ambiguous.In the item listed "Monitoring & Control" we do not believe monitoring should be included as listed it is too ambiguous and could be interpreted to include every meter, instrument transformer, etc, even if it is not needed for protection of the BES.
6.34	Luminant	Yes	Is it possible to have a real time impact (15 minute time horizon) related to Situational Awareness for Generation? If not it should be removed. At most it should be scoped to BA, RC,TOP and then only to a subset of data.The definitions in Attachment I are very broad. Could the SDT include examples or a reference document that provides more details for the functions in Attachment I?
6.35	Detroit Edison	Yes	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Definition of Adequate Level of Reliability located at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.
6.36	Reliability & Compliance Group	Yes	It needs to be more clearly defined what it means to have an effect on real-time operation of the BES. There are many things that can have an effect on the BES that occur even during normal operations. Recommend that the effect be defined as a reduction in the stability of the BES and that level of reduction needs to have a quantifiable measure.
6.37	US Army Corps of Engineers, Omaha Distirc	Yes	It seemes clear from the workshop that the committee intends for protective relay systems to be include for consideration. That was not clear prior to the workshop. They appear to fall under the category of Dynamic Response. Suggest strengthening the definition and include the term "protective relay."
6.38	US Bureau of Reclamation	Yes	It would be helpful to provide a example list of some of the elements which provide the related functions. Further, the unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the

#	Organization	Yes or No	Question 6 Comment
			size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Rather that attempt to define Restoration of the BES in the Attachment, would it be better to refer to other Standards?
6.39	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
6.40	MidAmerican Energy Company	Yes	MidAmerican Energy agrees with EEI's suggested improvements below:The "Situational Awareness" description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System.
6.41	Oncor Electric Delivery LLC	Yes	Need more clarity on the "15-minute" criteria. Is this ADVERSE effect? Is this RESTORATIVE effect?
6.42	USACE HQ	Yes	Please read answer to question 3.
6.43	BGE	Yes	Provide examples or definitions of actions, activities and automatically triggered.Add the words "to the BES" after "delivering electrical power" in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all

#	Organization	Yes or No	Question 6 Comment
			call system, 800 MHz devices used to communicate to field personnel and notifind)
6.44	SCE&G	Yes	Remove the 15 minute timeframe.
6.45	Southern California Edison Company	Yes	SCE's concerns with the proposed criteria are two-fold. First, it is unclear whether the term "effect" and "disturbance" refer to the same event. Thus, SCE asks the Standards Drafting Team to clarify. As the criterion is currently written, Attachment I states, "To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." However, the definition of BES cyber system in this standard states, "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES." If "effect" means "disturbance to the BES, restricted control and operation of the BES, or affecting situational awareness of the BES", then the definitions are consistent. This being said, it is not clear that these have the same meaning. An extreme definition of "effect real-time operation" could be virtually anything whether the impact on operations will be significant or not.Additionally, SCE recommends treating control and monitoring as separate functions. Systems that are only capable of monitoring BES elements should be treated differently from systems that are able to perform control functions. SCE suggests the drafting team add an additional function that is based on "actual device capability" rather than "how it has been implemented" by a particular registered entity. For instance, HMI's providing electronic output have a different real-time impact on BES reliability than HMI's designed as I/O devices. The task of reviewing data on a "view only" capable system resulting in human action on another system that could potentially cause BES reliability issues is a distinctly different function than the task of initiating actions. In this case, the monitoring system and the control system are both "real-time" but with very different BES impact potential.
6.46	Constellation Energy	Yes	See answer to Question 3.

#	Organization	Yes or No	Question 6 Comment
	Control and Dispatch, LLC		
6.47	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 3.Provide examples or definitions of “actions”, “activities” and “automatically triggered” as provided in Attachment I.Add the words “to the BES” after “delivering electrical power” in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all call system, 800 MHz devices used to communicate to field personnel and notifying).Please define the industry use for the term Generation Management System (“GMS”). We believe there are two categories of GMS, Regulated and non-Regulated Utilities since they could be use differently or have different functionality.
6.48	MWDSC	Yes	See comments for question 3 above.
6.49	Wolverine Power	Yes	See comments listed for 1.a
6.50	BCTC	Yes	See previous response 0n CIP-010-1-R1
6.51	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment 1 would work.
6.52	Constellation Power Source Generation	Yes	Some of the terms are ambiguous. What is meant by monitoring and control? As written, it is an AND statement, meaning that a BES Cyber System would have to do both monitoring AND control to be labeled a BES Cyber System. What about electronic metering at a plant? That provides monitoring, but not control. So is it excluded?Situational Awareness should be clarified. A suggestion would have the following statement attached to the current definition: “and cause an action without further analysis.” This would exclude metering that, if rendered unavailable, would not be detrimental to the BES as phone communication would be used in the event of metering errors.

#	Organization	Yes or No	Question 6 Comment
6.53	Platte River Power Authority	Yes	Suggest removing “Inter-Entity Real-Time Coordination and Communication” until there is a mechanism to define a single BES Cyber System that includes BES Cyber System Components from multiple Entities. The mechanism should include documentation of coordination with implementing the CIP standards for the BES Cyber System.
6.54	SPS Consulting Group Inc.	Yes	Suggestion number one is to get rid of the list, as previously stated. Failing that my other question is about Dynamic Response. I assume this refers to things like UFLS, UVLS and runbacks initiated by SPS. Also assume this does not include things like AGC, AVR, and governor response from generators since these actions are not triggered by a single element or control device, or a combination of devices, but rather are initiated by operating condition fluctuations. Is that true?
6.55	Dairyland Power Cooperative	Yes	Systems used to communicate between entities are not mentioned, yet many of these are critical to the operation of the BES. Imagine the impact to the BES of an ISO/RTO without ICCP communications. How can these systems be ignored?
6.56	Allegheny Energy Supply	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest that the definitions for "Dynamic Response" and "Balancing Load and Generation" be more specific.
6.57	Allegheny Power	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.

#	Organization	Yes or No	Question 6 Comment
6.58	APPA Task Force	Yes	The APPA Task force agrees with the intent of Attachment I. We believe, however, the definitions contained in the attachment can be substantially refined and improved.As discussed in response to Question 3, we recommend using the word “activities” (or other suitable synonym) for the word “function” to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, We suggest:Situational Awareness - Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated state of the BES.Other recommended changes to help simplify and clarify the definition of terms used:Facilities and Elements do not perform any action, protection, or control; rather cyber systems perform the action. Therefore we propose:Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance. Supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term “generation.” Therefore we propose:Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and load. SOLs and IROLs should be discussed in this context. If this suggestion is not taken, then “BES element” should be eliminated from the definition. Therefore we propose:Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. The phrase “delivering electric power without external assistance” is not supported by EOP-005 and should be removed from this definition. Therefore we propose:Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES and should therefore be removed from the Monitoring and Control function. Therefore we propose:Control - Activities, actions and conditions that provide control of BES elements.
6.59	Arizona Public Service Company	Yes	The APS review team had the following comment: The document heading is “Function Essential to Reliable Operation of the Bulk Electric System.” Typically restoration of BES

#	Organization	Yes or No	Question 6 Comment
			is a completely different activity than the normal or emergency operation of the BES. The document includes restoration which is typically not essential to the reliable operation of the BES. This is not a contradiction but the operation is being defined more broadly than typical. This broad function description can create ambiguity.
6.60	Independent Electricity System Operator	Yes	The descriptions for most of the functions are too vague that they cannot serve as a guideline to identifying those components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tampered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that they perform one or more of the functions listed in Attachment I.We suggest Attachment I be eliminated.
6.61	Entergy	Yes	The Functions as identified in Attachment I are far too general in nature and thereby leave too much latitude in interpretation in audit, i.e., creates a risk that if the Responsible Entity excludes a system(s) from scope and the auditor disagrees, this could be a very significant adverse finding. Entergy recommends that general Function descriptors be augmented with specific examples of applications that execute the stated functions 'essential to reliable operation of the BES', e.g., ACE, AGC, state estimator, etc., to help avoid as this dilemma to the extent foreseeable.
6.62	NextEra Energy Corporate Compliance	Yes	The standard should clarify those functions and provide examples specific to Generation, Transmission and Control Center Facilities. These clarifications, we believe, should be contained in the body of the standard as opposed to a reference attachment.

#	Organization	Yes or No	Question 6 Comment
			Attachments should be used to add specific examples or propose exclusions.With respect to the Inter-Entity real time coordination and communication function, the standard should specifically exclude voice communications systems due to the fact that they are covered under separate standards (i.e. COM Standards)
6.63	American Electric Power	Yes	The terms "Dynamic Response" appears to be a very broad function. Is it the intent that this would include all devices such as relays?The "monitoring" portion of function "Monitoring & Control" is too ambiguous. We would propose using the following: "Control - Activities, actions and conditions that provide control of BES elements."In addition, "Situational Awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
6.64	Dominion Resources Services, Inc.	Yes	There is overlap among the many functions listed. The list can be reduced to only Monitoring & Control with many of the others listed as examples of this function. As examples; Balancing Load and Generation and Controlling Frequency (Real Power) are essentially the same. Frequency is a direct result of the balance between supply (generation) and demand (load). It is redundant to list both, and doubly redundant since both are covered by Monitoring & Control. Monitoring & Control touches or covers most of the other listed functions. Any portion of Dynamic Response, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), and Managing Constraints not captured in the Monitoring & Control function should be identified and listed separately, but not those entire functions. Also, some of the definitions are too broad and encompass functions that are not required for the reliability of the BES.Facilities must have ratings per FAC-008 and must be operated within those ratings in other reliability standards. Please refer to “ratings” rather than “design limits and constraints.”Dominion requests that the functions be reduced to: Monitoring & Control - Activities, actions, or conditions that provide real-time operation and control to maintain BES elements within their ratings. Restoration of BES (as defined).Situational Awareness - Activities, actions, or conditions required by the BA, RC, or TOP for real-time operational decision-making associated with the BES.Inter-Entity Real-Time Coordination

#	Organization	Yes or No	Question 6 Comment
			and Communication (as defined).
6.65	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
6.66	We Energies	Yes	We Energies agrees with EEI comments. The "Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for to assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.We Energies agrees with EEI Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System. Additionally, We Energies does not understand the inclusion of "Real "Power" and "Reactive Power" in the context of the functions "Controlling Frequency" and "Controlling Voltage" respectively. It is suggested that these qualifiers be eliminated.
6.67	Bonneville Power Administration	Yes	We find the guidance on Attachment I confusing. The statement "The following operation functions are essential to real-time reliable Operation of the Bulk Electric System" makes the explicit statement that all the functions listed below are essential to real-time operation; and the second sentence doesn't do a good job of clarifying that it is only those BES Cyber Systems for which the loss of the functions listed below (Dynamic Response, Balancing Load and Generation, Situational Awareness, etc.) can have an effect on real-time operations of the BES within 15 minutes.For example, the loss of a cyber system used for situation awareness of lightning strikes would not have an effect on real-time control and operations of the BES within 15 minutes. As such, it is NOT a

#	Organization	Yes or No	Question 6 Comment
			BES Cyber System.It would be helpful if this statement in Attachment I and the definition of BES Cyber System were more consistent with each other."Situational Awareness" is too broad. Refer to comments in Question 1.b.
6.68	American Transmission Company	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.69	MRO's NERC Standards Review Subcommittee	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.70	WECC	Yes	While scoping the CIP standards to only cover functions within a 15-minute event time frame is appropriate for generation, transmission, and other operations it is not appropriate for Reliability Coordination functions such as situational awareness. There are many cases of critical systems to support a reliability coordination function that do not fall within a 15 minute time horizon such as next day studies, coordinated outages, and contingency planning. Suggest that the SDT redefine functions for situational awareness and communication between entities to not be restricted to a 15 minute time period.The opening paragraph again refers to a 15-minute time period to be used in the identification of BES Cyber Systems. It appears that an effort is being made to restrict applicability of this standard to real-time systems. Section 215 of the Federal Power Act does not include such a restriction; therefore, this should be removed from the standard. Any cyber system that could affect the reliability of the bulk electric system, regardless of timeframe, should be in-scope.Dynamic ResponseThe second sentence is poorly worded and does not appear to add anything. This language should be clear and concise.Restoration of BESThere are a significant number of restoration plans at the

#	Organization	Yes or No	Question 6 Comment
			Balancing Area and Transmission Operator level that hinge on external assistance. In many cases these areas play a significant role in delivering power across the transmission system during restoration, but do require external assistance. As drafted, the functional characterization for restoration of the BES, may fail to identify systems critical to system restoration and is seemingly inconsistent with Attachment II, specifically Item 1.6.
6.71	Ameren	Yes	Would change the second sentence defining the scope to read "To define the scope of applicability of CIP Standards, the below functions are relevant only if they can have an effect on real-time operation of the BES within 15 minutes.Would suggest to impose limits on the definitions for example Controlling Voltage (Reactive Power) is partially dependent on hydrogen pressure for hydrogen cooled generators. We would also suggest adding the word "grid" in front of voltage.Change the first sentence of Dynamic Response to read "Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to mitigate the impact to a BES condition". Is it the SDT intent to implement physical and cyber security of any tertiary systems for example, Controlling Frequency (Real Power) is also dependent upon coal mills providing enough fuel to the boiler, do these systems also need to be secured?The "Controlling Frequency" section needs some clarification. Governor controls on all generating units have built mechanisms whether mechnical or electronic that act to control or balance frequency during a disturbance. The current definition would lead to inclusion of all generating units regardless of any other factor. â€,The last section on communication needs to be clarified to explicitly address voice communication vs. data communication and the expectations of both.
6.72	Verizon Business	Yes	The criteria should include major systems needed for the essential operation of such systems as control centers. For example, Heating, Ventilation and Air Conditioning (HVAC) systems are essential to the operation of a control center. The failure of the HVAC could lead to shutdown of the control center within the 15 minute time frame.

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

The summary of responses to Question 7 was previously posted on the NERC website prior to the posting of Version 4 of the CIP-002 through CIP-009 standards.

#	Organization	Yes or No	Question 7 Comment
7.1	Platte River Power Authority		1.1 is confusing. Consider revising: For the preceding 12 months did the Generation Facility's net Real Power capability (rated net) exceeds the largest value of either the Contingency Reserve or the Reserve Sharing Group's total reserve sharing obligation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW. 2.7. "switching stations operated at 200kV or above" should read "switching stations operated between 200kV and 299kV"
7.2	National Rural Electric Cooperative Association (NRECA)		In 1.1, "must run" must be more clearly defined and there needs to be language to make clear how Generation Facilities are labeled "must run" -- i.e., who determines the "must run" status? In 1.5 and other places in this document, the term Transmission lines is used. What does "lines" mean? One wire? One three-phase circuit? One single phase of a three phase circuit? Please make this clear so there is no confusion for registered entities when determining High, Medium or Low. In 1.10, please provide an explanation of what "impact" and "local area" means in the phrase "have impact beyond the local area." Add language to 1.10 as needed to make

#	Organization	Yes or No	Question 7 Comment
			this more clear.
7.3	Emerson Process Management		It is only uncertain how the criteria of 2000MW and 1000MW were chosen for generation facilities.
7.4	Arizona Public Service Company		These criteria are closely related to the definition of a BES Cyber System and the feedback for question #2. If the intent is to categorize the majority of BES Cyber Systems into the Low, Medium and High Impact Categories, with the current timeline specified in the definition of a BES Cyber System, it may lead Entities to exclude from Impact Categorization (by the Definition) Cyber System Components that the drafting team did not intend. A preferred approach may be to eliminate the time windows from the definition, causing all BES Cyber Systems to be inventoried, and enhancing the Impact Categories with additional time window criteria. For example, a High category may be further refined by specifying an impact window of 0-15 minutes, a Medium of 16-240 minutes, a Low of 241-1440 minutes (24 hours), etc. Additionally, a further Impact Category of 'None' may be beneficial if the 15-minute time windows is removed from the definition. This would allow a floor to be utilized in the Impact Categorization of 'Low' so that it would not result in unintended consequences of including undesired BES Cyber System Components in a category with Standard applicability. Further comments regarding the (as-of-yet undefined) implementation schedule include concerns that a long implementation schedule or different implementation schedules for High, Medium and Low both raise the risk of confusion as well as the risk or FERC disapproval. An alternate method, in conjunction with the definition and Impact Category adjustments mentioned, of creating a phased implementation schedule, by time period (12 months, 24 months, 36 months, for example) would allow the applicable standards to increase over time for the lower categories. This would also allow for some Standards to be applied earlier than other Standards in the same Impact Category.
7.5	ISO New England Inc	No	"Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important

#	Organization	Yes or No	Question 7 Comment
			to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.6	Madison Gas and Electric Company	No	1.3 and 2.3 utilize the words “must run”. Must run is used in many markets whereby a GO may designate a unit to be online outside the need for reliable operations of the BES. Since “must run” is not defined, it is recommend that the SDT remove the term “must run”.
7.7	Progress Energy (non-Nuclear)	No	All T/D substation capacitor banks that provide system reactive support are controlled through a capacitor bank control program residing on the substation gateway device. However the DSCADA master may be included in 1.2 (more than 1000 MVAR). 2.4 will bring many T/T substations into consideration with the four or more lines >200kV. Also see comment 4. Attachment II defines "Each Cyber System that can affect operations for..." as it relates to Impact Rating on BES. For new combined cycle facilities which will include diverter dampers to allow simple cycle operation can we designate separate Cyber systems for simple cycle operation (approximately 70% of total plant output) and combined cycle operation (approximately 30% of total plant output). Potentially that would define each system as a "Low " impact versus a combined Medium to High. The plants are being designed to go from combined cycle to simple cycle operation in less than 15 minutes. We will need to know whether this designation is allowed and then design the cyber system(s) architectures appropriately.
7.8	Consultant	No	Attachment II - Section 1.1 & 1.2 To avoid confusion, suggest consistent wording in the parenthetical phrases following the words "singularly or in combination" in these sections.

#	Organization	Yes or No	Question 7 Comment
			Section 1.2 - Similar to section 1.1, should there be a 12 month component to the Reactive Power criteria in addition to the 1,000 MVAR. Section 1.3 & 2.3 - The term "pre-designated" doesn't make sense. A facility is not in the "must run" status unless it is "designated". Additionally, the statement has "must run" units both "designated" and "assigned", and semantically these are two different conditions. Section 1.3 & 2.3 - Further, the reliability "must run" status is an economic and contractual condition rather than a BES operational condition. It would seem that the plants that would be designated as reliability "must run" should have a BES operational or reliability criteria, independent of their "must run" status, which should be the criteria used to include or exclude these facilities. Section 1.6 - suggest including the title of EOP-005 in the statement as a complete reference citation. Section 1.9 - suggest including the title of NUC-001 in the statement as a complete reference citation. Section 1.10 - suggest clarifying which entity makes the determination that a RAS has "impact beyond the local area." - RAS Owner, RAS Operator, or appropriate regional entity. Section 1.11 (& throughout CIP-011) - BES Elements, BES elements, and elements are used throughout this standard. It is not clear if all are intended to be the glossary definition of 'Elements', or if 'BES elements' or 'BES Elements' are new definitions or incorrect application of the glossary term 'Elements'. Please clarify the usage. Sections 1.8, 1.13, 2.5 - These sections include the words "singularly or in combination" without a subsequent parenthetical qualifier. Suggest consistency with sections 1.1 & 1.2 as discussed above. Section 2.1 - See comments on sections 1.1 and 1.2 regarding consistency of parenthetical statement.

#	Organization	Yes or No	Question 7 Comment
			Section 1.1, 1.3, 1.4, 1.5, 1.7, 2.1, etc. - Multiple sections use the terms Generation Facilities or Transmission Facilities with capitalization that should indicate a defined term, either by this standard or in the current glossary. These terms are not defined in the current glossary. Suggest consistency of using defined terms throughout the standard. Section 2.1 - The criteria in this section are not parallel to the criteria in section 1.1 with a 'downsized' value. The term "most current and prior to most current rated" is not defined, or included in the glossary. Suggest clarifying this section, and defining or referencing the terminology.
7.9	E.ON U.S.	No	CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 “High Impact Ratings” of the categorization of the BES Cyber Systems. E ON U.S. proposes that only Control Centers and Backup Control Centers fall into the High Impact Rating category. All other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category. More generally, “reliable operation” of the interconnected BES is defined in Section 215(a)(4) as:” . . . operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.” Attachment II’s low impact category appears completely untethered to the statutory definition of reliable operation of the bulk power system. Attachment II also appears to introduce an ill-defined set of multiple contingencies or sequence of events that needs more definition and boundaries to be of any practical use and to provide a reasonable means for compliance cost quantification.
7.10	Kansas City Power & Light	No	Do not agree with several of the items listed in Attachment II.

#	Organization	Yes or No	Question 7 Comment
			Items 1.7 & 1.8 are too broad. There are any number of combinations of transmission facilities that can be removed from service such that the undesirable effect of exceeding an IROL limit or the loss or reduction of generation would occur. Recommend their removal as the remaining items left in Attachment II are sufficient to capture the HIGH impact areas. Item 1.10 regarding SPS is too broad. SPS systems are in place for a number of different reasons, including the protection of facilities from damage. The SPS that should be considered here are only the SPS that are intended to prevent cascading, uncontrolled separation, or instability. Item 1.14 is too broad and would include facilities that are unnecessary. Recommend tying Control Centers in where facilities are identified in 1.5. Recommend the following language for consideration: Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations for transmission facilities identified by 1.5.
7.11	FirstEnergy Corporation	No	FE suggests that item 1.5 be removed such that it is effectively reclassified as a medium impact and covered by item 2.4. Within the High Impact category, items 1.6, 1.7 and 1.8 appropriately cover those situations where Transmission Facilities should rise to a High Impact level. Consider removing item 1.9. This delves into a nuclear plant safety concern that is covered by the NUC-001 standard and not directly associated with BES reliability. If in item 1.1 a 2000MW level adequately depicts a High Impact generation facility hurdle then transmission facilities associated with a 900MW nuclear plant should not be deemed High Impact for BES reliability. In item 1.10 the term “local area” is vague and open to interpretation. Its suggested to simplify such that all SPS and RAS systems would be treated as High Impact. If the intent is to exclude SPS or RAS associated with limiting generation output under contingency loss of certain Transmission Facilities then consider a separate Medium Impact SPS or RAS describing those instances and rewrite 1.10 to say “Special Protection Schemes,

#	Organization	Yes or No	Question 7 Comment
			Remedial Action Schemes (RAS) or automated switching of BES elements not include in Section 2, item 2.x" However, the preference is to keep it simple and just treat all SPS and RAS items as High Impact. Suggest adding thresholds below which no measures need to be taken. The low impact rating as written could require significant effort for negligible security and reliability improvement.
7.12	National Grid	No	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue. National Grid recommends a tabular format similar to the tables in CIP-011-1 with various criteria listed under Low Impact, Medium Impact, and High Impact. This will help in understanding the key differences among the three categories efficiently."Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.13	American Electric Power	No	Overall we like the concept of these gradients, but need more time to fully ascertain the validity of the breakpoints. It is uncertain what engineering analysis drove these specific categorization levels. We assume that there could be a significant difference from region

#	Organization	Yes or No	Question 7 Comment
			to region, and the SDT should consider regional impacts for the categorization.
7.14	Regulatory Compliance	No	Qualifier should include capacity factors averaged over the last five years - otherwise it will require some large plants that are only on-line several days a year to remediate to the "High Impact" category
7.15	Manitoba Hydro	No	Regarding criterion 1.1, the phrase “with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW” is difficult to understand. For some utilities, the required reserve obligations could be a small value which would not compare very well to the proposed 2000 MW limit for utilities with NO reserve obligations (such as small utilities). A related minimum value for utilities with reserve obligations should be provided, or the greater value of the required reserve obligations and 2000 MW should be used .Regarding criteria 1.5 and 2.4, clarify the requirements through the appropriate use of colons, semi-colons and numbers. It is not clear as drafted whether phrase “with four or more transmission lines” applies to Texas and Quebec.
7.16	Seattle City Light	No	see prior comments
7.17	Indeck Energy Services, Inc	No	The system of 3 categories oversimplifies the BES. 1) The grouping of, for example, all generators of capacity less than 1,000 MW (except for special cases like Must Run units) as LOW needs to be further subdivided. The categorization ignores the Functions in Attachment I. Not all generators have the same impact on the BES ALR for all functions. Different types of generators have different effects on the BES ALR. This isn’t to say that all generators should not be categorized, but not all require the same LOW level of requirements. Choosing only 3 categories was highly arbitrary. The LOW category should be subdivided into 3 or more groups reflecting the relative impact on BES ALR that was used to differentiate the HIGH and MEDIUM groups. 2) Additionally, the standards ignore the fact that access to BES cyber facilities can be

#	Organization	Yes or No	Question 7 Comment
			controlled at either end of a communications path. If it is adequately controlled at one end, then controlling the other end or the middle is less important, if not unimportant. For example, an RTU at a small generator that is a window to the BES cyber facilities at the control center is a bigger risk for BES ALR at the control center than it is at the generator. Any effect on the generator may be insignificant, whereas, access to the control center could be critical. Applying controls at the control center takes away the need to control all of the insignificant RTU's, but not the ones affecting other parts of the BES. 3) Nowhere in the categorization process is the potential impact on BES ALR assessed by Function. Attachment II makes arbitrary categories that may be appropriate for the HIGH and MEDIUM categories, but has not been done for the remainder that are lumped in the LOW category. The concept of impact to the BES ALR is missing from the categorization process. The impact on the BES ALR of, for example a 999 MW generator versus a 499 MW generator versus a 299 MW generator are very different and different by Function as well. The impact on the BES ALR should be assessed for all facilities in the LOW category to differentiate them. All of the facilities should be categorized as to the impact on the BES ALR by function. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, with various combinations of facility types and functions from Attachment I.
7.18	Reliability & Compliance Group	No	These criteria do now however, exclude many systems that were previously identified as CCA's. However they also include many systems that registered entities eliminated using the RBAM.
7.19	BCTC	No	This looked very thorough. Great job!
7.20	Xcel Energy	No	While the draft provides guidance in Attachment II as to which BES elements are classified as High, Medium, and Low impact, no criteria is provided for why each element was assigned into the specific impact category. The decision to place each element into

#	Organization	Yes or No	Question 7 Comment
			a category is not based on any identified objective criteria. The SDT should publish the criteria used to place each item under the assigned category.
7.21	Independent Electricity System Operator	Yes	(1) We support explicitly including Restoration of BES as a critical function. However, in the proposed standard it is limited to blackstart generation and transmission subsystem cranking paths (impact level H, items 1.4 and 1.6 in Attachment II). The impact criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). With these criteria, in Ontario we would drop 6 generating stations (a total of over 3000 MW capacity) from a High impact (current Critical Assets) to a Low impact category. We suggest to add a requirement in the High category for generation essential to facilitate restoration as determined by the RC. (2) 1.3 “Generator pre-designated as must run”: In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: “Generation Facilities that have Wide Area reliability impacts when removed from service”. (3) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part “Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (4) 1.13: BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (5) 2.3: See our comments on 1.3. We do not see the need for this category. (6) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.22	IRC Standards Review Committee	Yes	(i) There are "bright-line" cutoffs for the range of violations for MW of generation (1.1, 2.1) and voltage levels (1.5, 2.4). Although these cutoffs are appropriate for most of the Interconnection(s), there may be local configurations that warrant that BES Cyber System to be rated other than what is defined with the "bright-line" cutoff. CIP-010-1 should either allow for a documented alternative rating or waivers be allowed to diverge from the cutoff limits. (ii) 1.3: "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (iii) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (iv) 1.13: A BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (v) 2.3: See our comments on 1.3. We do not see the need for this category. (vi) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.23	FEUS	Yes	*1.1; clarify 'if the Generation Facilities capability exceeds the largest value of the Contingency Reserve or reserve sharing obligations for the Reserve Sharing Group' the Contingency Reserve is also relative to the Reserve Sharing Group. *1.10: The drafting team should consider allowing for voltage differentiations for High and Medium SPS, RAS, or automated switching stations similar to that used in 1.5 and 1.14
7.24	Hydro One	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase. We strongly suggest that a fourth category of NO IMPACT is included as follows: No Impact contains all other documented BES Cyber Systems that have no affect on operation and are not categorized as having either High, Medium or Low Impact rating.
7.25	Northeast Power Coordinating Council	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid

#	Organization	Yes or No	Question 7 Comment
			operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.
7.26	Florida Municipal Power Agency	Yes	1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Net Winter Real Power capabilities of generators are to be used in determining the supply side of determining the mismatch. The greater of actual coincident peak load, or forecasted peak load for the next year, of the Reliability Coordinator is to be used for the demand side of the equation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, the supply-demand mismatch metric shall be equal to the largest loss of source plus 50% of the next largest loss of source for the Reliability Coordinator area."Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single

#	Organization	Yes or No	Question 7 Comment
			contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:"Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact" Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL."Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. FMPA suggests:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load Elements since those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the

#	Organization	Yes or No	Question 7 Comment
			distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. Black start and cranking paths should not be High Impact at all. High impact would be the system going black, a delay in restoring the system is a Medium Impact since the damage has already been done. Hence, 1.4 and 1.6 should be combined and made a Medium Impact. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 2.4, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 2.4, or functionality that remotely controls a BES Cyber System with a High Impact Rating."
7.27	Southwest Power Pool Regional Entity	Yes	1.1: The criteria to include as High only the generation that exceeds the Contingency Reserve or reserve sharing obligation effectively removes nearly all generation resources from this impact category. 1.3: "Wide Area reliability impacts" as defined by the NERC Glossary of Terms (April 20, 2010) may be far too broad. If the unit is designated as RMR, it should be High impact regardless of the wide area consideration. 1.10: Please define the term "local area." 1.12 and 1.13: The Reliability Coordinator, and in the instance of a consolidated Balancing Authority, the Balancing Authority functions afforded a High impact categorization are fed real-time operational data from smaller, lower impact BES Cyber Systems owned and operated by other entities. Because of the criticality of the Reliability Coordinator and Consolidated Balancing Authority's near total reliance upon external real-time data sources, those sources need to also be afforded a High impact category. In particular, these BES Cyber Systems would include the EMS/SCADA and ICCP subsystems found in an entity's control center. 2.1: The 1000 MW criteria defining a Medium Impact generation asset will likely place

#	Organization	Yes or No	Question 7 Comment
			most generation into a Low Impact category.
7.28	Oncor Electric Delivery LLC	Yes	1.10 needs to better define “local area” (eg. 3 busses) Need criteria for “Low” such that “None” is the lowest level of protection required. Also, there is a need to have categories for systems with no IP communication or dial-up only communications.
7.29	LCEC	Yes	2.4 Replace transmission facilities with “Substations and/or switching stations and two or more non-radial transmission lines”. or”Transmission Facilities with four or more non-radial transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.” 2.7 change to "non-radial" Transmission substations or switching stations or”Primary or Backup Control Centers that remotely control two or more Transmission substations or switching stations, each with four or more non-radial transmission lines, operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.”
7.30	Turlock Irrigation District	Yes	Attachement II criterion #1.4 states that BES Cyber Systems that can affect operations for Blackstart Resources in the Transmission Operator's restoration plan shall be categorized as High Impact. This should be changed to include only the Blackstart Resources in a region's Blackstart Capability Plan because Transmission Operator's restoration plans typically include Blackstart Resources that are not material to the restoration of the BES. Blackstart Resources that are material to the restoration of the BES are designated by each Regional Entity in accordance with NERC Standard EOP-007-0 titled "Establish, Maintain, and Document a Regional Blackstart Capability Plan". We suggest that the wording of criterion #1.4 be changed to "Generation Facilities designated as Blackstart Resources in the Regional Blackstart Capability Plan". Making this change would maintain consistency between the Standards and would also be consistent with the Purpose section of CIP-010-1 which states that the categorization of

#	Organization	Yes or No	Question 7 Comment
			BES Cyber Systems should be "commensurate with the adverse impact... on the reliability of the BES. Attachment II criterion #1.6 uses the term "primary Cranking Path". What is the meaning of the word "primary" as used in this context? We suggest that the wording be changed to "Facilities required to support Cranking Path(s) that are material to the restoration of the BES as used in a Transmission Operator's restoration plan per EOP-005".
7.31	Garland Power and Light	Yes	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line. General Comment Need to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
7.32	Powersouth Energy Cooperative	Yes	CIP-010 Attachment II 1.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered High Impact if singularly or in combination exceed 2,000 MW. It seems to be reasonable to apply the 2,000 MW limit to reserves as well with reserve requirements only greater than 2,000 MW being considered as High Impact. 1.4 Additional consideration should be given to categorizing blackstart units in all cases as High Impact. Some units, while identified in a TO’s restoration plan, are not part of

#	Organization	Yes or No	Question 7 Comment
			the Regional Entities Restoration Plan. Some generation that may be used in a restoration effort may be removed from the TO's restoration plan to avoid implementation of High Impact security requirements. Some "middle ground" should be found so that more units can remain available in a restoration plan without being subject to costly security requirements and subsequently an increase in exposure for a utility to be non-compliant. It is recognized that there must be a sufficient number of blackstart critical units that remain protected by High Impact status to ensure restoration following an event. 1.10 Is "local area" meant to be the Balancing area or can the entity define local area. 2.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered Medium Impact if singularly or in combination exceed 1,000 MW. It seems to be reasonable to apply the 1,000 MW limit to reserves as well with reserve requirements only greater than 1,000 MW being considered as Medium Impact. 3. Some consideration should be given to providing exclusions to exempt assets that in reality have no material impact.
7.33	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
7.34	MidAmerican Energy Company	Yes	Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load". Subsequently, CIP-010-1 Attachment II item 1.4 should be updated to only designate

#	Organization	Yes or No	Question 7 Comment
			Generation Facilities associated with the “Primary Cranking Path”. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical asset systems that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Four critical units at MEC would move to low. Simultaneous loss of the four MEC units would impact the reliability of the BES. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
7.35	PacifiCorp	Yes	Comments: Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. ALSO "Wide Area" impacts need to be clarified in Item 1.3 for "Must Run" units. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical assets that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.

#	Organization	Yes or No	Question 7 Comment
7.36	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Concerning generation facility capability, "rated net Real Power" can produce fictitious numbers that will never be attained. This should be the historical or commissioning test maximum net Real Power continuous output, whichever is greater. Wide Area is a very large area for WECC, as WECC is the RC. We are not sure if there are any generation facilities in WECC that have an impact on the whole of WECC. We are also not sure if generation being "pre-designated as reliability 'must run'" is a practice in all areas. It is possible that some units may be designated using other terminology or have detailed contracts. It may be better to remove the quotes and define Must Run Generation in the Glossary. Not all generation that is designated by the Transmission Operator's restoration plan as Blackstart is critical to the plan. It may be listed as a possible resource, but not a primary first choice. Further, much of the restoration plans are out of date and due for revision; requiring generation owners and operators to upgrade for CIP compliance only to have their plant removed in the new restoration plan in the next year or so would be wasteful. The purpose of a Blackstart resource in an old (pre-mandatory reliability standard compliance) restoration plan may be for local level of service resource for the TOP's local distribution area rather than a resource for BES reliability, i.e. the old plans to not coordinate well with each other. Last of all, should there not be a rating qualifier?
7.37	Detroit Edison	Yes	Criteria 1.3 and 2.3 should be removed for the following reasons: 1. The term "reliability must run" is not defined. 2. There is no generator that is so essential to reliability that it would need to run 100% of the time. 3. A generator could be required to run on a given day to serve load in an area that cannot be otherwise served due to a transmission constraint. This would be a temporary condition and should not warrant a high or medium classification.
7.38	Cogeneration Association of California and Energy Producers & Users	Yes	Criteria 2.4 should be clarified. The criteria states "Transmission Facilities with four or more transmission lines operated at 200kV or above..." Do two transmission lines, each with two circuits that can operate independently for a total of four circuits, count as two

#	Organization	Yes or No	Question 7 Comment
	Coalition		transmission lines or four transmission lines?
7.39	Exelon Corporation	Yes	Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment. A specific example is the 4 or more Transmission line requirement. The previous draft had a 3 or more Transmission line requirement, so what was the basis for the 3 or more and, moreover, what is the basis for now changing it to 4 or more? The technical basis for generation limits in Attachment II is not provided. That is, the basis for the 2000 MW and 1000 MW thresholds appear arbitrary. Combined losses of greater than these values have occurred without significant impact to the BES. No "reasonable bounds" are allowed. For example, if a common vendor provides a cyber product in multiple generating stations, it appears that the assumption is that this common product, no matter how local its impact, creates a common mode failure for all plants simultaneously, resulting in the determination before the fact that this product will be rated as High Impact. No allowance is made for geographical location. For example, if a common cyber system is used in several large generating stations in different regions of the country, their simultaneous loss may result in no significant impact to the BES. However the deterministic MWe thresholds and simple "in combination" wording will result in virtually all such cyber systems rated as high, deterring use of common vendors, standardization, and economies of scale. Although moving to a more deterministic approach can be seen as increasing consistency in application of the standard, it would appear that a deterministic approach will decrease the flexibility of operation now allowed and may in fact, reduce BES reliability. As a modification to the Attachment, Exelon suggests that the existing deterministic criteria could be used, unless an entity chooses to show by actual historical data or modeling that such losses do not result in significant impact on the BES. This performance-based criteria could be expanded to define high, medium, and low impacts on the BES in terms of stability, voltage swing, etc.

#	Organization	Yes or No	Question 7 Comment
7.40	American Transmission Company	Yes	For R1.4, we propose changing text from “designated as Blackstart Resources” to “designated as the primary Blackstart Resources” (similar to primary Cranking Path in 1.6). Add “restoration plan per EOP-005” (similar to 1.6). Note that Transmission Operators can only designate Blackstart Resources that have been volunteered to them by Generation Owners. All GO may choose not to volunteer any Blackstart Resources if they don’t want their associated cyber systems to be subject to this standard. For R1.10, we propose removing SPS from the criteria. SPSs cannot be approved by the Regional Entities unless they have been designed not to be critical to the BES (e.g., not critical if they operate when they should not or do not operate when they should).
7.41	SCE&G	Yes	How does the SDT see AGC coming into play in 1.1? Would every generator operated on AGC (if the aggregated total met the contigency reserve commitment) be considered high impact, or just the centralized AGC itself?" Must Run" units needs to be clarified. Who determines if a unit is "must run"? 1.4 This language needs to be clarified to identify resources designated as "Primary" Blackstart resources. 1.5 Transmission lines should be change to Transmission Lines to utilize the NERC Definition 1.8 Is this misusing/destroying one Transmission Facility at a time? SDT should consider defining "Transmission Facility" as a whole instead of utilizing separate NERC Definitions for "Transmission" and "Facility"
7.42	Entergy	Yes	If “size” of an electric facility remains the primary key differentiator for applicability of CIP requirements, which Entergy does not support, the following should be considered: 1. High Impact Rating (H)”Each BES Cyber System that can affect operations for: 1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power

#	Organization	Yes or No	Question 7 Comment
			capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities , singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW." Attachment II of CIP-010-1 qualifier 1.1 as stated above includes those generation facilities that have the capability to exceed the Contingency Reserve as High Impact to the BES. This is not truly indicative of the impact to the reliability to the BES. Entergy has multiple generation facilities with the capability to exceed the contingency reserve. However, their Service Hours (SH) are less than 900 hours and a Service Factor (SF) is less than 1.0, averaged over the past five years, where: - Definitions from GADS Data Reporting Instructions - January 2010- Service Hours - SH is the sum of all Unit Service Hours.- Period Hours - PH is the number of hours in the period being reported that the unit was in the active state.- Service Factor - SF = SH/PH x 100% Entergy proposes that a better representation for how much a generation plant runs, and therewith potential adverse impact on BES reliability, would be better determined by a measurement of the percent of SH, e.g., running at least 80% of the year; SH greater than 7008 hours per year, or, a SF of greater than 80% per year. Therefore, suggested alternative language for 1.1 is: "Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability), whose Service Factor (Service Factor = Service Hours per Year / Hours per Year X 100%) is equal or greater than 80% for a five year average." Additionally, extending this logic to the Medium Impact BES Cyber Systems, Entergy suggests replacement of language concerning Medium Impact Rating (M) 2.1 from: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real

#	Organization	Yes or No	Question 7 Comment
			Power capability of 1000 MW or more, not included in Section 1." To: "Generation Facilities, singularly or in combinations (if using a shared BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability) with equal to or greater than 70% for a five year average."
7.43	Edison Mission Marketing and Trading	Yes	If we are going to use the High, Medium, and Low and there is not going to be a does not apply category, then there should be an engineering analysis or study performed by the BA's, RC's or an independent firm and it should include which sites/generators are critical and which are not and why. Once completed then and only then do we begin categorizing them into whatever scale the Standard Drafting Team and the included entities agree upon. As it is stands now we not only have to include nominal size generators, but wind sites as well.
7.44	Puget Sound Energy	Yes	In 1.6, the restoration plan is linked to EOP-005, shouldn't the restoration plan mentioned in 1.4 be linked to EOP-005 as well? It appears that all BES Cyber Systems must fall into one of three categories. Are there any other criteria that would all for something not to be categorized as one of these three (i.e., such as non-dispatchable wind generation)? Also Blackstart should only classify as high those needed for primary region wide restoration since some (such as ours) are more secondary paths and there should be some minimum level of generation to be classified low. There is no need to classify as low a 20 MW hydro generator that does not impact BES reliability. We would recommend 300 MW.
7.45	Alliant Energy	Yes	In Article 1.3 we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.

#	Organization	Yes or No	Question 7 Comment
			Article 1.4 - By including "All Black-Start Units" the standard is utilizing a "one-size-fits-all" strategy that the industry has recognized does not work for everything, and is working to address. All Black-Start units do not carry the same importance and this should be recognized in the standard. This philosophy may be counter-productive to system reliability as one classification may reduce the number of Black Start units that would be made available to a TOP's restoration plan due to the high initial security cost and the future possible financial risk of strict compliance guidelines with penalties. There should be a recognized hierarchy for the Black-Start resources, similar to the High, Medium, and Low for BES Cyber Systems. This methodology would assure Black Start units could be categorized by attributes in general to support the BES during a blackstart event. Each Balancing Authority Area (BAA) could be required to have a minimum number of high priority Black Start units depending on the BAA size to support the area during a black out. Lower priority units would be used for stabilizing power at generating stations, local area islanded load and used as a backup plan if all other contingency plans would fail. Article 1.6 - This item should reflect the same categorizing as is recommended in the comment to Article 1.4 above. Article 2.1 - Please clarify "with aggregate higher of the most current and prior to most current rated net Real Power capability." We believe it would be clearer if stated as below: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System) with a rated Real Power capability of 1000 MW or more, not included in Section 1." Article 2.3 - we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.
7.46	Public Service Enterprise Group companies	Yes	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6

#	Organization	Yes or No	Question 7 Comment
			requires that only the “primary cranking path” transmission facilities need to be categorized with a “High Impact Rating”. Statement 1.6 implies that some Blackstart Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
7.47	ReliabilityFirst Staff	Yes	In Part 1.1, the referent for “largest value” does not seem to be appropriate. Suggest changing the wording to “average value.” In Part 1.4, a “Blackstart Resource” is only the first resource that starts in a system restoration. Suggest changing the wording to “Generation Facilities required to support the Cranking Path(s) identified in Part 1.6.” In Part 1.6, a “primary” Cranking Path is not required to be identified in an entity’s restoration plan by EOP-005. Suggest changing the wording to “Facilities required to support at least one Cranking Path.” In Part 1.10 “local area” should be defined. As we are not certain what is meant by this term, we have no suggested wording.
7.48	RRI Energy	Yes	Include or add a "No impact category" that is determined by the RC.
7.49	MRO's NERC Standards Review Subcommittee	Yes	Item 1.3 We believe this item may be problematic in nature, as the designation of reliability “must run” units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc. Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System.

#	Organization	Yes or No	Question 7 Comment
			Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or

#	Organization	Yes or No	Question 7 Comment
			simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher..." Item 1.6 We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14 We would recommend rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7 We would recommend rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions We would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility

#	Organization	Yes or No	Question 7 Comment
			with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
7.50	Minnesota Power	Yes	Item 1.4: Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. In theory, on a smaller scale, this appears to be a "one size fits all" approach, but in reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, Minnesota Power believes that there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, Minnesota Power believes it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just the fact that it has been included. For example, a 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, Minnesota Power proposes that the Standards Drafting Team allow Registered Entities to assess the relative importance of a Blackstart Resource based on the importance of the facilities it directly supports. Minnesota Power recommends rewording item 1.4 as follows utilizing the existing language of Item 1.8:

#	Organization	Yes or No	Question 7 Comment
			"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Minnesota Power believes this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14: Minnesota Power recommends rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7: Minnesota Power recommends rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, which are not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions: Minnesota Power recommends adding the following items under section 2, Medium Impact Rating, for consistency with the proposed Item 1.4:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

#	Organization	Yes or No	Question 7 Comment
7.51	The Empire District Electric Company	Yes	Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same "one size fits all" approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. A regional study performed by the regional entities would be an excellent approach to determine this. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item #1.4 as follows, leveraging the existing language of Item #1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Since item #1.6 is also related to system restoration, we would recommend rewording it as follows for consistency in approach: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as

#	Organization	Yes or No	Question 7 Comment
			described in Part 1.1 above." We would also recommend adding the following items under section 2, Medium Impact Rating: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply changing the High Impact criteria to mirror that of the Medium Impact (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher...".
7.52	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS), which address the current structure of Attachment II as proposed. However, LES believes a better overall approach would be applying

#	Organization	Yes or No	Question 7 Comment
			Engineering studies to truly determine a facility's impact on the Bulk Electric System. We realize an Engineering study is not as simple as a "bright line" based metric. Unfortunately, the Bulk Electric System is not a simple system - it is actually very complex. So in order to properly assess the importance of the various facilities that make it up, LES feels a complex Engineering study is required.
7.53	Luminant	Yes	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ...
7.54	Nuclear Energy Institute	Yes	Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW?
7.55	NextEra Energy Corporate Compliance	Yes	NextEra finds that a catch-all for Low impact is a fatal flaw. There should be some threshold that is justified for low. For example, a proper minimum criteria for LOW impact BES Cyber Systems could be:Cyber Systems that control BES level facilities that meet one of the following: 1) three or more transmission circuits operated at 100 kV or above not covered in Section 1 or 2, 2) two or more transmission circuits and two or more autotransformer with a secondary voltage 100kV or above,3) two or more transmission circuits and generation capacity at the site of greater than 1000MW Alternatively, a NO IMPACT category may be added which eliminates subjectivity in which BES Cyber components need to be reviewed. Single point buses representing looped load serving type stations cannot produce results worse than single contingency which must be operated to at all times. An additional item that should be specifically covered is the use of remote access for transmission and / or generation control locations and their applicability to the High, Medium, Low and/or No impact criteria.

#	Organization	Yes or No	Question 7 Comment
			The term "affect operations" can be subjective and can be open to interpretation. NextEra suggests changing the15 minute requirement to “in real time (instantaneous). For example, closed loop control, which does not allow time for human intervention.” NextEra also recommends adding the word “both” prior to monitor and control. NextEra would also like to know what does 1.1.1 of section D mean? This is unclear. A suggestion would be eliminating or providing a specific definition.
7.56	Pacific Gas & Electric Company	Yes	Not all blackstart resources should necessarily be considered high impact. Suggest revising 1.4 as follows: Generation Facilities designated as Blackstart Resources and explicitly listed as essential to the restoration of the BES in the Transmission Operator’s restoration plan.
7.57	Northeast Utilities	Yes	NU is concerned with some of the impact criteria in Attachment II related to generation facilities. To base impact on “bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows. Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause levels of impact to the BES.
7.58	Matrikon Inc.	Yes	Please describe how the 15-minute time horizon would fit into Attachment 2. Is the intent for the 15-minute horizon to provide a level of realism to determination of impact? To bring in more BES Cyber systems that could have indirect impact, or an escape clause if effects don’t occur within 15 minutes?
7.59	USACE HQ	Yes	Please read answer to question 4.

#	Organization	Yes or No	Question 7 Comment
7.60	BGE	Yes	Provide additional clarification of “automatic aggregate”. For instance, does automatic mean an application that is kicked off without human intervention or does automatic mean after an operator hits a button? Suggest adding the word “instantaneous” before load shedding to clarify. Additional clarification on 1.14 (What is meant by “functions”)
7.61	Southwestern Power Administration	Yes	Rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity, a better approach may be to include performance/results-based criteria in Attachment II. However, if the current approach is forwarded, I would suggest the following improvements: 1.4. Generation Facilities designated as Primary Blackstart Resources in the entity’s restoration plan. 1.7 Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.10 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that if destroyed, degraded, or misused, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.11. Delete. Is this not a Control Center issue? 1.12. Control Centers that perform the Reliability Coordinator functions. 1.13. Control Centers that perform the Balancing Authority functions for 4,000 MW or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections. 1.14. Control Centers that perform the Transmission Operator functions for a Facility

#	Organization	Yes or No	Question 7 Comment
			with a High Impact Rating. 2.4. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more System Operating Limits (SOLs) 2.7. Control Centers that perform the Transmission Operator for a Facility with a Medium Impact Rating, not included in Section 1. 2.8. Control Centers that perform the Balancing Authority functions for 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.
7.62	Southern California Edison Company	Yes	SCE believes Attachment II should be modified to account for only the capacity that can be controlled by qualifying systems. As currently written, Attachment II defines the amount of generation under control as the rated capacity of the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000 respectively. This would place the system in a "low impact rating" according to the attachment. For that reason, SCE believes that Attachment II should be modified to account for only the capacity that can be controlled by the system.
7.63	San Diego Gas and Electric Co.	Yes	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have "BES outage" or reliability implications but may not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole.

#	Organization	Yes or No	Question 7 Comment
7.64	Constellation Energy Control and Dispatch, LLC	Yes	See answer to Question 4.
7.65	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 4. Please clarify the intended treatment of a Generation Management System ("GMS"). Attachment II implies that capacity monitored by a GMS system would be aggregated to determine its impact categorization. However, to be consistent with the intention to protect connections that truly impact the BES net real power capability should only be aggregated within a balancing authority.
7.66	MWDSC	Yes	See comments for question 4 above.
7.67	Wolverine Power	Yes	See comments listed for 1.a
7.68	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment II would work.Also, for 1.1, either increase the net MW rating or add an annual capacity factor to a generating unit to account for old units at a site that no longer run because no longer economical. These types of facilities should not have to meet High category requirements if they no longer run. Also, for 1.3 add more detail. Explain pre-designated. Assigned by who? Explain Wide Area reliability impacts.
7.69	WECC	Yes	Similar to our previous comment, if Attachment 1 is expanded to include in scope reliability coordination functions critical to reliable operation of the BES outside of 15 minutes the impact levels need to be updated. While many functions of a Reliability Coordinator are critical and should be an high impact, not all functions of reliability coordination should be made high impact. For instance, Coordinated Outage systems while important to the reliability of the BES and should be in scope, should best be classified as a low-impact BES Cyber System. The considerations for identification and categorization has been elevated to a high level such that BES Cyber Systems and not individual devices are identified based on their specific functionality. It is suggested that if BES Cyber Systems are to be indentified and

#	Organization	Yes or No	Question 7 Comment
			categorized there be some inclusion and development of a process to granulate these systems down to their individual component level. Further, the quantitative qualification bar has been set to level that precludes most BES Cyber Systems from reaching identification as a high or even medium level of impact. Taking into account. If a BES Cyber System can impact reliability a baseline set of security controls should be established that creates tracking for all assets, accountability for access to these assets, and physical and electronic protection for these assets. Specific Line Item Comments(1.1) The standard, as drafted, seemingly excludes all generation but large dams, large mine-based coal plant and nuclear plants?(1.1) The developed sentence structure lends itself to multiple interpretations and will prove to be difficult to audit consistently. (1.1) Is the term aggregated defined as geographically co-located, common substation, common communication paths, etc?(1.6) What about redundant paths? There is no requirement to identify and document multiple paths. (1.6) A reference to EOP-008 would also be appropriate.
7.70	Con Edison of New York	Yes	Specific comments on the Categorization: The impact categories should be linked to the reliability Standard functions in Attachment I. Therefore, the High, Medium and Low ratings should reference specific Standards whenever possible. o 1.1: This requirement should be broken down into two requirements. One should refer to BAL-002 and reserves needed to be compliant. The second should be any generation facility with a common BES Cyber System greater than 2,000 MW. o 1.2: This should be linked to the function of “controlling voltages”. Two other concerns; first - shunt reactors and capacitors are not included and second - there needs to be a technical basis for a Reactive Power capability limit. o 1.3: Suggest moving to “Low” category since reliability must run equipment is frequently a local congestion or voltage control situation. This would not qualify for a “High” impact rating.

#	Organization	Yes or No	Question 7 Comment
			o 1.4: Black start resources should only be designated as a High Impact Rating if they are the only resource in the TOP's restoration plan. If the TOP has multiple restoration resources and procedures, the resources should be a Medium Impact Rating. Reference this to EOP standards. o 1.5: OK o 1.6: This item should be included in item 1.4 o 1.7: FACTS devices are used to control voltage and power flow. o 1.8: This should be included in requirement 1.1 o 1.9: OK o 1.10: Refer to PRC standards o 1.11: A basis for the 300 MW or greater UFLS system should be provided. o 1.12, 1.13, and 1.14 address Control Centers and should be aggregated into one requirement based on RC functions, BA functions, TOP functions and TO functions. In addition, there may be a conflict between a Control Centers with a "Low Impact Rating" and a single substation with a "High Impact Rating". The DT should consider addressing this conflict where the "BES Cyber Security Components" on one side of a device (e.g. breakers) is a "high impact" while the command signal will be a "low impact" device. General comment on criteria for categorization: Overall, the high, medium, and low levels do not properly meet the needs of the BES. The DT should be looking at what the system does and determining its ability to impact the BES rating rather then the impacted equipment. For example, SCADA systems should be High whether they are on the 138 kV or 345 kV. Wide scale damage can be done with access to the SCADA system, however only local issues can occur with access into a single non-networked microprocessor relay. Alarm panels and other microprocessor that do not have direct impact should also be at lower level. Items that set levels should be a medium level. Basis for criteria for categorization is needed:

#	Organization	Yes or No	Question 7 Comment
			Attachment II to CIP-010 contains a number of what appear to be administratively determined "bright lines." Please provide both the detailed rational supporting each "bright line" and a specific quantification of the reliability benefits resulting from its implementation. In responding to this question, please focus more on the technical, reliability-related rational and improvements for each "bright line" selected, rather than on the source of any particular number. Reference any white papers, studies, expert opinion, or other documentation relied upon and supporting the "bright lines" selected. For example, in Attachment II category High Impact for item 1.11, please explain why 300 MW was selected. We are not so much interested in any reference to a 300 MW EOP-004 DOE reporting requirement, as we are in the specific criticality of the 300 MW level to BES reliability, e.g., 300 MW represents a large (>10%) percent of area load, or in the case of inadvertent actuation would cause an uncontrolled system instability(ies) and cascading, or in the event of a failure-to-actuate would cause the Interconnection UFLS program not to return frequency to nominal within the program required time period. What if for a given entity 300 MWs is not a significant percentage of local load, or inadvertent actuation would not cause uncontrolled instability and cascading, or failure-to-actuate would not prevent the return of frequency to normal within the required time period? Why rate such aggregate automatic load shedding "High" rather than "Medium" or "Low?" Are there any Interconnection-wide studies which would support this 300MW "bright line" value? Please provide any reference(s).
7.71	Allegheny Energy Supply	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.

#	Organization	Yes or No	Question 7 Comment
7.72	Allegheny Power	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.

#	Organization	Yes or No	Question 7 Comment
7.73	EEI	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. As a result, the drafting team should consider whether to combine Items 1.4 and 1.6. Moreover, most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from providing additional protections for more valuable facilities. Moreover, this may create incentives for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. EEI suggests the following definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. In addition, the drafting team should modify the wording to only include units designated on a seasonal or annual basis. Regarding 1.7, EEI recommends striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does

#	Organization	Yes or No	Question 7 Comment
			not appear in the NERC Glossary of terms Suggest Adding: 1.15 Control Centers including Generation Control Centers. Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. EEI suggests that 1.11 in Attachment II be revised as follows:"BES Elements that perform automatic aggregate load shedding of 300 MW or more under a common control system."]
7.74	APPA Task Force	Yes	The APPA Task Force commends the drafting team on their work on CIP-010-1. We appreciate the team's consideration of our Task Force comments from the previous informal comment period. We feel it is especially important for entities to have the option of categorizing the impact level based on the Contingency Reserve or total of reserve sharing obligations as stated in 1.1. However, we are concerned with the "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc. These thresholds do not have a basis from industry experience and could be challenged by entities or regulators. We are concerned that having chosen these numbers without empirical data supporting them, the numbers can easily be changed without the supporting empirical data. It is our recommendation that these numbers be evaluated more closely. At a minimum, the thresholds should be quantified to show what percentage of generation and transmission facilities would be designated under each Impact Rating. Florida Municipal Power Association (FMPA) provided some suggested alternative calculation methods for the Impact Categorization of Attachment II. We provide them here for the drafting team's discussion in evaluating the bright line thresholds. FMPA Comments:

#	Organization	Yes or No	Question 7 Comment
			Categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: o High (has the potential to cause an Adverse Reliability Impact) o Medium (has the potential to require planned/controlled loss of load) o Low impact (has no potential to cause loss of load) Make changes to existing criteria: 1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: “Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is

#	Organization	Yes or No	Question 7 Comment
			greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is: ”Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area.” In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact.” Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL.” Radial Facilities serving only load should not be included in 1.5 or 2.4. The term “Facilities” in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. We suggest:

#	Organization	Yes or No	Question 7 Comment
			”1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator).” By using the term Facilities, which by definition is a “... single BES Element”, we also exclude radial serving only load since that those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV. In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 1.5, i.e.:”Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 1.5, or functionality that remotely controls a BES Cyber System with a High Impact Rating.” End of FMPA comments. The APPA Task Force also supports the proposal by the MRO-NERC Standards Review Subcommittee (MRO-NSRS) in their comments on Item 1.4 and 1.6 to assign the impact rating of blackstart units and cranking path relative to assigned impact rating of the generating facilities it directly supports. We feel that inclusion of all blackstart resources in the High Impact Rating will waste limited resources protecting facilities which are not in support of High Impact generation. MRO-NSRS proposal: High Impact:1.4 “Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.” 1.6 “Facilities required by the Transmission Operator’s restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated

#	Organization	Yes or No	Question 7 Comment
			capabilities as described in Part 1.1 above."Medium Impact:2.X "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." 2.X "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."
7.75	US Bureau of Reclamation	Yes	The criteria defined in this and several previous requirements are based around BES Cyber Systems, which under the definition of BES (per the WECC Glossary) does not include all power system assets. Therefore, there appears to be a category of Cyber Assets that do not presently require any protection measures (i.e., they might control a powerplant feeding a radial load or be associated with a system of less that 100kV. The classification "Low" will potentially include those systems which do not have an impact. It is counterintuitive to classify a system as low when it has No Impact. The Team should develop a description of "Low" similar to that which was provided for "High" and "Medium". Then the Drafting Team could issue a statement that systems not classified as "High", "Medium" , or "Low" would be classified as "No Impact".
7.76	Dominion Resources Services, Inc.	Yes	The criteria for categorization of Low Impact systems is too broad and uses the terminology "can affect" which the SDT has appropriately recognized is ambiguous. The following alternate wording is proposed:"All other BES Cyber Systems not categorized as having a High or Medium Impact rating that are required for the reliable operation of the BES."
7.77	Southern Company	Yes	The definition of "pre-designated as Reliability must run" in Attachment II, 1.3 is unclear and cannot be implemented with existing practices in some utilities. For utilities who designate units as must run on a day-ahead basis in some cases, a valuable practice, every unit in the fleet would have to be classified as high impact. The wording should be changed to only include units designated on a seasonal or annual basis. In addition, a

#	Organization	Yes or No	Question 7 Comment
			definition of “must run” should be provided or referenced from elsewhere in NERC documentation. The wording in 1.3 also creates a new requirement that all “must run” units be classified as to whether they have Wide Area impact, which is not currently required. Are there actually any “must run” units (or any units, for that matter) that have Wide Area impact? Because Blackstart Resources are included in Cranking Paths, 1.4 is redundant in light of 1.6 and should be removed. Alternatively, 1.4 should be limited to primary Blackstart Resources to match 1.6. In 1.4, consideration should be given to reducing the impact level for situations where multiple Blackstart Resources are available. Universally search for “effect” and replace with “adverse effect”. In 1.6, replace “support” with “is part of”.In 1.7, delete the phrase "including Flexible AC Transmission Systems (FACTS). This is redundant as it is referenced again in the following sentence.
7.78	Constellation Power Source Generation	Yes	The final sentence in 1.1 needs to be rewritten, as it’s extremely confusing. A suggestion would be to simply add the 2,000 MW bright-line at the end of the first sentence. It would read “Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve, total of reserve sharing obligations for the Reserve Sharing Group, or 2000 MW (if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established).” Is it the intent of the SDT for the MOD10 data to be the data used in this criteria? If so, that data changes seasonally, so a seasonal review would be needed, especially for units who are on the thresholds of the high/medium/low criteria. A suggestion would be to use nameplate data as that is a fixed rating that will not change. 1.4 and 1.6 should be

#	Organization	Yes or No	Question 7 Comment
			combined together, as they are referring to similar items. The combined High Impact Rating should read "Generation, Transmission, and other Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005." However, 1.4 and 1.6, either combined or separate, still penalize generation entities that own numerous black start facilities within a single Balancing Authority's footprint. Generation entities in the aforementioned situation have already invested a lot to ensure the reliability of the BES, but under CIP-010 they will be forced to invest even more. A suggestion would be for the TOP to designate a percentage of the black starts as High, and the rest as medium or low depending on their MW size. Another suggestion would be for the TOP to specifically designate certain black start units as high, and the rest are classified based on their MVA size, with the caveat that the TOP should not designate all black start units as high to avoid liability.
7.79	Dairyland Power Cooperative	Yes	The impact ranking for blackstart should be equivalent to the highest impact of all transmission and control center systems. If an entity has only low or medium impact systems other than blackstart, a high impact for blackstart is not appropriate. 1.2 and 2.2 specify 1000 MVAR and 500 MVAR, respectively for categorizing reactive power facilities. Since reactive power problems are localized in general, these numbers seem to be high. It is difficult to set global criteria on reactive power as it is network dependent. I would advise about 50% of the proposed level to be more conservative.
7.80	Duke Energy	Yes	The quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System

#	Organization	Yes or No	Question 7 Comment
			instability, separation, or cascading failures. Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW? o CIP10-1.4: We have many small sites (hydro's) listed in our Blackstart plan because they are available. They are not essential to our plan, but because they are available, we list them. Under this guidance, we would be required to include them as "High Impact", when in reality they are 'Low'. The wording should be revised to reflect that only those sites "REQUIRED" for Blackstart be secured under 1.4 o CIP10-1.6: We need a defined and clear understanding of what is intended in the use of the term "Cranking Path" as it relates to CIP and EOP-005. What is being sought under this requirement? The term is loosely defined in the glossary, and how it is interpreted by the industry may vary greatly from how it is intended by regulators. o Under our current understanding of the term, we would see minimal increase in sites added to our "High" list. However if we impose a severe interpretation, we could see an exponential increase to our 'High' list. o CIP10-1.7 & 2.5: The word 'Misuse' should be removed or very strictly defined. It is too vague to have meaning. o CIP10-1.11: Need a clear and functional definition of 'Element' for the industry to understand the intent of the requirement. Current glossary definition is poor at best. Also, revise 2.6. as follows: Transmission Facilities operated at 300 kV or higher, which have 2 or more 300kV or above lines, in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.
7.81	Bonneville Power Administration	Yes	The sixth line in 1.1 begins with the words "Generation Facilities." Generation Facilities is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability

#	Organization	Yes or No	Question 7 Comment
			Standards. Since this phrase is not used at the beginning of a sentence, it should be "generation Facilities." There is the same problem at the beginning of the second line in 1.2. That should also be changed to be "generation Facilities."The first line in 1.7 contains the phrase "Flexible AC Transmission Systems (FACTS)." That phrase is not defined in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Aren't all capitalized terms used in Standards supposed to be defined? Or does FACTS have a generally accepted definition in the industry? CIP-010-1 - Attachment II Impact Categorization of BES Cyber Systems High Impact Rating (H)Each BES Cyber System that can affect operations for:1.1. Generation Facilities, etc."can affect operations" does not relate to impact. We suggest it be reworded: "If the BES systems can change operation by the following amounts they will be in the HIGH CATEGORY: - Generation - 4,000 MW- trip or reduce output of "MUST RUN" generators to below their MUST RUN amount. - Transmission - de-energize at least 4 lines above 300 kV - MVAR support - change MVAR by 1,000 MVAR
7.82	US Army Corps of Engineers, Omaha Distirc	Yes	The word "affect" in the first sentence is somewhat ambiguious and does not fit the intent of all of the subsequent paragraphs(1.4 & 1.6) Paragraph 1.3 define wide area impacts. Paragraph 1.4 should be limited to BES Cyber Systems that are required to energize a Blackstart Resource listed in the TO's system restoration plan per the GO's written restoration plan. As written it appears to apply to any BES Cyber System that merely affects the Blackstart asset and that all BES at such a facility would be High Impact which could have a chilling effect on an entities willingness to provide Blackstart resources. Paragraph 1.6 should be limited to BES Cyber Systems required to operate or support equipment in the primary cranking path. Again this would appear to apply to all BES Cyber Systems at such a facility merely because the facility was part of the cranking

#	Organization	Yes or No	Question 7 Comment
			path regardless of their impact on system restoration. Paragraph 1.10 define impact beyond the local area.
7.83	Midwest ISO	Yes	There is no documentation for the justification of the selection of the various thresholds. Justification of these thresholds should be documented and defended.
7.84	SRW Cogeneration Limited Partnership	Yes	There needs to be a category for "no impact". We are a small Cogen plant that does not even sell firm power to the grid. In essence, we are a steam plant that happens to generate electricity. We have no "Critical Assets" as defined by CIP-002. There needs to be an equivalent level for that in CIP-010. If there needs to be a system study performed by the RC to support a "no impact" rating, that's fine. And if a facility is found to be "no impact", then that facility should be exempt from the majority of further CIP requirements, just like today where CIP-004 thru CIP-009 do not apply to facilities with no Critical Assets/Cyber Assets and only R2 of CIP-003 applies.
7.85	Covanta Energy	Yes	There still needs to be some allowance to fewer mandatory requirements associated with smaller generators.... those in the 20-50 MW range (which are unmonitored) who typically have to notify their TOP/BA that they are on the system or off the system (or reduced load if applicable).
7.86	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
7.87	We Energies	Yes	We Energies agrees with EEI Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. We Energies agrees with EEI comments Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term,

#	Organization	Yes or No	Question 7 Comment
			however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. Proposed definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms. We Energies agrees with EEI. Suggest Adding:1.15 Control Centers including Generation Control Centers .Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.
7.88	Ameren	Yes	We generally agree with the criteria used to identify “High” impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not

#	Organization	Yes or No	Question 7 Comment
			limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as “Medium” impact, but should be classified as “Low” impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as “Low” impact, as they likely have little impact on the BES. The use of TPL performance standards would confirm that many of these facilities have a “Low” impact. For 1.1 the 4th sentence should be reworded to say "total obligations for the entire Reserve Sharing Group." 1.3 needs clarification of what a "reliability must run" unit is. Also, clarify 1.4 if it refers to the actual black start unit, or the entire plant in which the black start unit resides. Last, clarify 1.6 on what magnitude of support is required by the facility. Currently this could apply to any Transmission or Generation Sub-system in the path. Performance criteria, such as the loss of 300 MW of system load to qualify for “High” impact or 100 MW of system load to qualify for “Medium” impact, should also be applied to the EHV facilities identified in items 1.7 and 2.6.
7.89	GTC & GSOC	Yes	We recommend that Attachment II be organized to more clearly indicate which items apply to which type of assets. In the case of Control Centers, it appears the primary applicable item in the High Impact category are 1.12, 1.13 and 1.14, but several other items could be misconstrued to apply as well, which could lead to those control centers being inadvertently given a High designation.
7.90	CenterPoint Energy	Yes	While it appears the SDT put a lot of effort in the development of Attachment II, the criteria to be used is arbitrary, is too prescriptive, does not allow for studies or analysis to determine whether or not the loss, compromise, or mis-use of an identified facility would have an impact on the reliable operation of the BES and, in some cases, appears inconsistent. For example; 1.5 Transmission Facilities with four or more Transmission lines operated at 300kV of higher in the Eastern or Western Interconnections or operated at 200kV or higher in the Texas or Quebec Interconnections would require any and all facilities meeting this criteria to be categorized as High Impact without any basis for this rating. Determining a facility’s impact to an electric transmission system involves

#	Organization	Yes or No	Question 7 Comment
			more analysis than counting the number of transmission lines operated at or above a threshold voltage level; 1.14 Transmission Operator functions is based on the number of substations a control center may be able to remotely control. The previous criterion, 1.13 Balancing Authority functions, is based on the mega-watt amount the Control Center operates. Neither offers a basis for either the number of substations or the mega-watt amount under the operation of the Control Center. While CenterPoint Energy would find Attachment II useful as a guide or systems to be considered it is apparent the SDT meant this to be a requirement and therefore CenterPoint Energy does not agree with Attachment II and suggests it be deleted.
7.91	Verizon Business	Yes	1) Attachment II, Item 1.1 regarding Generation Facilities – Suggest removing any reference to "Contingency Reserve" or "Reserve Sharing Group." Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW should be included as a High Impact Rating. Reference to the "Contingency Reserve" (etc.) comments can result in incorrect or inconsistent declaration of a generation asset being a High or Medium impact. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? For the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. This and any other questions from FAQ for CIP-002 should be addressed in the standard.

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

Many entities commented on the need to have the approach provided in the posted CIP-010 and CIP-011: it was pointed out that a substantial amount of work has been done in compliance with a Risk Based Methodology. Many entities commented on the the use of the systems approach, remarking that the flexibility allowed may not be appropriate. Other entities commented that the work done in the current CIP-002 through CIP-009 with Critical Assets should be preserved.

The SDT has reconsidered its approach to the structure of the standards and believes that Version 5 will provide an incremental approach while addressing the FERC directives.

#	Organization	Yes or No	Question 8 Comment
8.1	Constellation Power Source Generation		A guidance document is needed to add clarity, as some terms are still vague.
8.2	Allegheny Energy Supply		A lot of work went into the prepration of the existing CIP-002 standard. This new CIP-010 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to refine the CIP-002 drafts and to create and implement the current identification methodoligies and compliance plans. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components present the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network

#	Organization	Yes or No	Question 8 Comment
			segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. - Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.3	Entergy		A) Giving each individual Responsible Entity the 'freedom' to define "a system" any which way each prefers will almost certainly create similar problems as those experienced with CIP-002-1/2/3 that allowed each Entity to chose a 'risk based assessment methodology' of its own preference to identify Critical Assets. In the abstract the notion of self-conceptualization of "a system" may be appealing, but in terms of the confusion factor relative to NERC's goals for consistent interpretation, application, and subsequent audit-ability across the industry this portends trouble. Entergy suggests that "BES Cyber Systems" should be defined as collections/groups of hardware and software employed cooperatively to execute a Reliability Function in Attachment I. It is not necessary to explicitly define what a "SCADA system" is, but most can agree that there are cooperative components that must work together to execute the functions associated with 'SCADA.' Tangibly, this will no doubt be different in each setting in terms of specific gear used to assemble and operate the systems functions, but taken together they are indeed "a" system. It would seem more appropriate to instruct identification of groups of cooperative components that work together to be treated as a system, and extraneous or stand alone or single-purpose equipment could be distinctly characterized as "unitary systems" when appropriate. There is practical value in logically treating several cooperative components as a system, and requirements for implementation documentation will be more straightforward and simpler if they can be treated as such. B) The fundamental flaw in the combined logic of CIP-010-1 (and transitively CIP-011-1) is the notion that risk to reliable operation of the BES posed by use of cyber assets correlates exclusively with the size of the electric operating site at issue. This single-minded orientation ignores other highly salient cyber security threat vectors in play,

#	Organization	Yes or No	Question 8 Comment
			most notably, concerning what type of data communications technology is used to network within and between sites comprising a BES Cyber System. The CIP V1 SDT correctly recognized the especial vulnerabilities posed by use of routable protocols, if the BES Cyber System is not secured with proper cyber security procedural controls and technical countermeasures. At the same time, less vulnerable - in terms of adverse impact on reliable operation of the bulk electric system as a whole - BES Cyber Systems or Components thereof that communicate using legacy serial, dial-up, or other Data Link Layer data transmission paths pose less of a practical risk in terms of overall BES attack surface due to their inherent lack of an Inter-Network Layer. Absent routable protocols, miscreant cyber navigation to and attack of other systems or components not directly attached to the individual serial link (dial-up or hard line) or Data Link Layer (sub-)network is simply not possible. Furthermore, the binary orientation of applicability of a requirement discussed above actually creates unsavory unintended consequences: in a number of ways a single requirement can mandate unnecessary and costly countermeasures for sites of a certain size regardless of the attack surface presented by the communications medium. That is, rigorous requirements appropriate for BES Cyber Systems/Components at sites that employ routable protocols are also imposed on other sites that do not, e.g., operating sites where only legacy serial lines are used. Finally, requirements for BES Cyber Systems/Components at work in purportedly small-impact grid operating sites where routable protocols are employed are in many cases simply deemed to be not applicable (not required). Summarily, the use of "electrical rating" (size) as the sole determinant of applicability of cyber security requirements will result in both excessive expenditures and undue regulatory risk concerning sites that pose minimal risk of cyber attack. This approach simultaneously fails to apply the Requirements to sites that, while not significant from an electric reliability standpoint, could afford a cyber entry point which could be used to access the larger network via routable protocols. Please see comments under Question 54 for a continuation of the above train of thought for explicit recommendations for improvements concerning both the structural organization and logical substance of CIP-010-1 and CIP-011-1 when taken together.

#	Organization	Yes or No	Question 8 Comment
8.4	Allegheny Power		Allegheny Power does not believe it is necessary to abandon the Critical Asset approach described in CIP-002. The new impact categorization structure proposed by CIP-010 introduces a completely new approach. All of the investment in procedures, training, documentation and other efforts to date to ensure compliance with the CIP standards will need to be redone. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP-002 are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP-002 standard and not abandoning the approach entirely, which would essentially force all entities to start their CIP compliance efforts over from the beginning. Changing the terms, concepts and numbering schemes alone will disrupt continuity of CIP programs and have a major impact on each entity. Not all BES Cyber System components (as defined by CIP-010) face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.5	Green Country Energy		An overall guidance document would be very helpful to the large number of entities that will have to comply with this standard that previously were not critical. Nothing specific, some reference links, examples of expectations, a resource guide.
8.6	CWLP Electric Transmission, Distribution		Any terms used, such as Operational Time Horizon, should be included in the NERC Glossary of Terms.

#	Organization	Yes or No	Question 8 Comment
	and Operations Department		
8.7	Dominion Resources Services, Inc.		Attachment II contains some errors and should be revised in accordance with the following; CIP-010-1 1.3. The term Wide Area is applicable only to a RC area. GOs do not have access to information necessary to make such a designation. This requirement should state that a RC must inform a GO within a certain specified time frame if the RC determines that the GO owns a "must run" unit. Also. there must be some "implementation period" for the GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. CIP-010-1 2.3. It is not clear which entities (e.g., BA, RC, TOP, other) have the responsibility to make such designation. GOs do not have access to information necessary to make such designation. The entities that have access to the information include the RC, TOP and possibly the BA. The RC should make the designation, but with the input of the BA and TOP. If the RC makes such a designation, it is proposed that this requirement be revised to contain a statement that the RC must inform the GO within a certain specified time frame. Also, there must be some "implementation period" for GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. NOTE - Currently, in PJM, units so designated do not impact the entire RTO (equivalent of Wide Area) but are designated due to local import constraint limits (CETL). It appears likely that such generator would be designated as Medium impact. However, in smaller RC areas (e.g., NY), this could result in generators that appear to be equal in size (to a generator designated as medium in PJM) being designated as High because the impact to that RC area is based on size of the area as well as the generators within that area.

#	Organization	Yes or No	Question 8 Comment
8.8	Constellation Energy Commodities Group Inc.		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.9	Constellation Energy Control and Dispatch, LLC		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.10	ReliabilityFirst Staff		Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
8.11	Reliability & Compliance Group		Being more specific with better definitions is a tremendous help with interpreting the requirements. Right now, there is still too much open to interpretation and as such, this will be very hard to make auditably compliant anywhere but to our own procedures.
8.12	City Utilities of Springfield, Missouri		City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
8.13	IRC Standards Review Committee		Comments: NERC should lead a discussion of whether the proposed CIP standards provide an appropriate level of protection from attacks. By level, we mean the granularity of the requirements - or how far down to individual components and personnel procedures. Attempting to put requirements to protect from nearly every possible attack scenario possible on every possible asset and or component that touches the BES is an extraordinary effort that will certainly provide a perception that NERC and the registered entities are doing what they can to protect from threats. There is no argument that if every registered entity protects every asset/component from threats to the nth level of granularity, the industry would be able to state that it has made every possible effort to thwart attempts to sabotage the interconnected grid. But NERC should begin a discussion on whether it is necessary to have such extensive requirements to be able to prevent a system-wide incident. The proposed CIP standards do not seem to align with NERC's approach in setting reliability requirements for more "traditional" system threats such as facility loading and system frequency. With these "traditional" standards, there is a distinction between requirements and procedures that are local in

#	Organization	Yes or No	Question 8 Comment
			nature and those that are needed on a wider interconnection level. For these "traditional" reliability threats, it is accepted by industry and regulators that this is an appropriate approach. For example, NERC does not establish requirements for relay maintenance crews to properly disengage trip coils when testing relays. But NERC does establish standards for registered entities to maintain those relays that impact BES reliability. The details of how the registered entity ensures that maintenance programs are carried out requires a local or individual procedure/requirement. NERC's focus should remain on setting standards to protect from wide area impacts - not on establishing standards that manage individual system components. NERC and the industry need to take a hard look at what exactly the CIP standards should protect from and write standards that can leverage compliance resources to reducing the wider interconnection level threats and leave setting measures or requirements that are local in nature up to the registered entities.
8.14	Southwest Power Pool Regional Entity		Consider combining the Medium and Low categories into a single category. A three tier categorization is not necessary.
8.15	Public Service Enterprise Group companies		Considerable effort was spent by industry stakeholders in classifying assets as Critical Assets (CAs) and as Critical Cyber Assets (CCAs) for CIP v1-v3. An official guide to map identified assets using the CIP v1-v3 CA and CCA terms and the new BES Cyber System Component and BES Cyber System terms is needed. Such will be an aid in ensuring a smooth transition.
8.16	Oncor Electric Delivery LLC		Control Centers and substation need to be considered separately. What is prudent cyber protection at a control center may be totally unnecessary at a substation.
8.17	E.ON U.S.		cyber systems used exclusively for local distribution of electric energy is contrary to FPA Section 215 (1) & (3). Other comments on specific areas of the proposed standards: CIP-010-1 B Requirements Section 3.2,3.3 What constitutes a "change" under these requirements.

#	Organization	Yes or No	Question 8 Comment
			CIP-010-1 C. Measures, M3 E.ON U.S. requests that the SDT clearly define in which requirements this measure applies. CIP-010-1, Violation Severity Levels There is very little difference in risk between failing to update documentation for 60 versus 80 calendar days, yet there are various gradations based on the 10-15 day window from the low-to-severe. CIP-010-1, section 3 "Low Impact Ratings" Maintaining an inventory of all low-impact rated BES cyber systems/ components will result in a significant administrative burden. Given the few prescribed protective measures that apply under CIP-011 to low impact facilities the inclusion of low impact facilities appears to provide little in the way of additional BES reliability.
8.18	San Diego Gas and Electric Co.		Draft Standard CIP-010-1 is a significant paradigm shift from the currently effective Standard CIP-002-2. SDG&E has spent significant resources to be compliant with the current version of the CIP Standards including becoming knowledgeable with the current terminology and applying it within the current CIP Standards. Draft Standard CIP-010-1 departs from the current CIP Standards but at the end of the process, it is unclear whether this change in approach will in fact result in a material enhancement to the reliability of the BES. SDG&E suggests that before continuing to move forward, the SDT needs to specifically understand and communicate to the industry what it is trying to accomplish. What is the target that we are all trying to hit with these proposed changes to the CIP Standards? In so doing, the industry can provide specific alternatives that accomplish the goal at hand. When evaluating the alternatives to meet the goal, it is critical that there is a quantifiable incremental reliability benefit to the BES before proceeding. SDG&E and many other entities have spent significant resources to comply with the current CIP Standards. At this point in time, the industry needs to know that additional resources to

#	Organization	Yes or No	Question 8 Comment
			comply with the proposed CIP Standards will result in an incremental benefit to the reliability of the BES. SDG&E strongly recommends that before moving any further, these questions be answered and that the SDT actually "test" the proposed draft CIP-010-1 Standard on a handful of companies or scenarios to gain some practical experience from the proposed changes. Are the in-scope assets easy to identify and categorize? How does the quantity of in-scope assets compare to that of the current Standards? Perhaps the SDT will find that there is a significant enhanced reliability impact to the BES. On the other hand, the SDT may find that the results do not accomplish the goal that it is trying to achieve and thus another approach would make more sense. SDG&E advocates leveraging the existing CIP Standards as much as possible moving forward, because we (like many others) have a lot of time and resources invested in our current compliance efforts and we'd really like to build from those efforts instead of essentially starting over with a new process.
8.19	BCTC		Emergency Situations - The provision for "emergency situations" should remain at the policy level. BCTC is of the opinion that it is feasible for emergency situations to be unforeseen and, as such, does not agree with the assigning of such contingencies to specific requirements.<See CIP-011-1-R3 below for an example> TFEs - TFEs will continue to be required due to the limitations of technology - i.e. older systems being unable to enforce strong passwords, etc. These limitations are beyond the Utilities control and, as such, it would be considered unfair to be found in non-compliance for such instances. What should be required in such situations is that the Utility implement controls to minimize the vulnerability that results from the TFE.
8.20	Exelon Corporation		Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our

#	Organization	Yes or No	Question 8 Comment
			commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format. Each change in itself represents a significant "change management" issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon's continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not been shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us "starting from square one" to implement. If this shift to CIP-010 and CIP-011 is approved, policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards. Specifically, Exelon would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable

#	Organization	Yes or No	Question 8 Comment
			continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.
8.21	Duke Energy		Explicitly state that terms found in the NERC glossary apply here unless otherwise stated.
8.22	USACE - Omaha Anchor		General comment - committee referred to relays as being addressed in this standard. We are unsure what that interpretation is based in attachment 1.
8.23	Powersouth Energy Cooperative		General Comments: The approach to classify cyber systems according to their impact seems to be a better approach for the industry. Taken in conjunction with CIP-011 that establishes security requirements, it is logical to establish security levels based upon the impact of compromising these assets. The drafting team is commended for this approach. Consideration should be given however to recognizing that while technically some assets are BES assets, they do not materially affect the BES. For example, a small DP may own UFLS relaying however the magnitude of the load that is shed by their entire UFLS program would insignificantly affect the overall objective of the regional UFLS programs to protect the BES. While identifying those assets is reasonable, to require any security measures in CIP-011 is not warranted. Perhaps a "No Material Impact" category should be considered based on load. R1. There is a perception that every cyber system associated with the BES owned by an entity must be identified to determine if the cyber system executes or enables one of the functions in the attachments. It would seem appropriate to review all facilities (i.e. locations) to determine and document the functions that are performed at that location. However, if it is determine that no BES functions are performed documenting each system seems to provide little benefit. Example: A small distribution station is served from a transmission line greater than 100 kV. The station does have multiple cyber systems none of which perform identified BES function. The perception is each system must be documented. Since on a higher level,

#	Organization	Yes or No	Question 8 Comment
			a functional assessment indicated no BES functions are performed, is it necessary to document each cyber asset?
8.24	American Municipal Power		I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
8.25	Matrikon Inc.		I offer to provide a workflow decision diagram I have prepared (Visio or JPG) to show how CIP-010 could be interpreted, but also to see how each of the statements in the requirement are supposed to fit into evaluation of BES Cyber Systems. I am a visual person, and my goal was to visualize the interpretation of CIP-010 for myself and colleagues to have a clearer understanding of its application. Diagram has been sent directly to Lauren.Koller@nerc.net as part of my comments. Use at your discretion, feel free to leverage/expand on my diagram, and share with SDT. My intent is to simply help reduce misinterpretation of the standards and debate on how they should be applied.
8.26	Cogeneration Association of California and Energy Producers & Users Coalition		Is it the intent of the Drafting Team that a cyber system will not be classified as a BES Cyber System if it does not cause a disturbance to the BES within 15 minutes or does not have an effect on real-time operation of the BES within 15 minutes of it becoming unavailable, degraded, compromised, or misused? If yes, guidance will be needed on

#	Organization	Yes or No	Question 8 Comment
			what proof of lack of disturbance is necessary to support an entity not classifying a cyber system as a BES Cyber System.
8.27	EEI		It would be helpful for the drafting team to develop in a separate guidance document more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of compromise.EEI suggests that the drafting team recognize that not all BES Cyber System components face the same risk based on their connectivity. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.28	ISO New England Inc		Modify the purpose statement to be more clear and understandable. Proposed Purpose: To identify and categorize BES Cyber Systems that execute or enable

#	Organization	Yes or No	Question 8 Comment
			functions essential to reliable operation of the BES. Apply appropriate cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.
8.29	Hydro One		Most North American utilities spent significant capital and manpower resources in order to achieve compliance with current version of CIP standards. Version 4 brings a multitude of changes that appear to significantly broaden compliance requirements. Hydro One understands and supports the intent to improve the overall reliability of the BES through reduction of the vulnerability to cyber attacks. Based on the previous experience, in the development of the version 4 implementation plan, the SDT should consider the long time periods necessary to implements the changes required for this version.
8.30	Michigan Public Power Agency		MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities, " between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
8.31	MidAmerican Energy Company		Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too prescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity

#	Organization	Yes or No	Question 8 Comment
			levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.32	Progress Energy - Nuclear Generation		NERC should facilitate the Federal Energy Regulatory Commission (FERC) consideration to suspend implementation of Critical Infrastructure Protection (CIP) Reliability Standards CIP 002 through 009 for nuclear plants in favor of implementing CIP-010-1 and CIP-011-1. Originally, CIP-002 through 009, Version 4, were to be developed to address nuclear cyber requirements as a result of FERC Order 706-B. However, CIP-010-1 and CIP 011-1 are now being developed to address the nuclear cyber requirements. In the mean time, nuclear will be required to implement CIP-002 through 009, Version 3, which do not align with CIP-010-1 and CIP-011-1 to satisfy the FERC requirements. CIP-010-1 and CIP-011-1 could be implemented at the nuclear plants in the same time frame licensees committed to the Nuclear Regulatory Commission for the 10 CFR 73.54 required Cyber Security Plans. Using the current North American Electric Reliability Corporation (NERC) timeline approved by FERC, R+18 of CIP 002 through 009, Version 3, (~ August 2011), the timing of implementation of CIP-010-1 and CIP-011-1 will be well after CIP 002 through 009 and potentially 73.54. This will require multiple reiterations of nuclear licensee cyber security plans and implementing programs and procedures. These changing requirements create potential error opportunities.
8.33	NextEra Energy Corporate		NextEra suggests a re-write of the following provisions as set forth below to provide

#	Organization	Yes or No	Question 8 Comment
	Compliance		clarity: 4.2. Physical Facilities 4.2.1. All BES Facilities under NERC jurisdiction, including those nuclear generating plant facilities that as part of FERC Order 706-B (and other applicable FERC orders) processes are determined to be subject to this CIP Standard. B. Requirements R1. For each BSE Control Center, Generation Facility or Transmission Facility implicated by the Responsible Entity's application of High, Medium and Low Impact Risk in Attachment II to its BES, the Responsible Entity shall identify and document all BES Cyber System Components that it owns and indicate its association with a BES Cyber System. (Violation Risk Factor: High) R2. The Responsible Entity shall ensure that each BES Cyber System Component identified in R1 is in compliance with the applicable protections as required in CIP-011-1. (Violation Risk Factor: High) CIP-010-1 - Attachment I (For informational purposes only) Functions Essential to Reliable Operation of the Bulk Electric System The following provides an understanding of the operating functions which are essential to real-time reliable operation of the BES and are provided for informational purposes only.
8.34	Independent Electricity System Operator		No, but please see our comments under Q9.
8.35	USACE HQ		Please answer to questions 3 and 4.
8.36	FirstEnergy Corporation		Please see Question 1 for FE's Summary view on the CIP-010 and CIP-011 standard.

#	Organization	Yes or No	Question 8 Comment
8.37	BGE		Provide a definition for “Automatic Load Shedding”.
8.38	Puget Sound Energy		Puget Sound Energy notes that the Violation Severity Levels put specific metrics (5%, 10%, etc...) to previously commented on vague terminology. In order for NERC to determine “5% or fewer BES Cyber Systems have not been identified”, there has to be a total number of BES Cyber Systems at an entity. But, with vague, open to interpretation, terms like “restrict” or “affect”, the total list of BES Cyber Systems is subjective to different opinions on what it means to restrict or affect the BES.
8.39	Liberty Electric Power, LLC		RE: VSLs. Smaller facilities with limited cyber assets will pay a much larger penalty for a single miscategorized asset than a large utility. Example: TOP miscategorizes 49 of its 1000 cyber assets, and gets hit with a single lower VSL. Small generator miscategorizes 1 of 8 cyber assets, gets hit with a severe violation. Some method of recognizing the disproportionate affect on smaller entities must be included in the standard.
8.40	LCEC		Recommend that the development and release of implementation guidelines takes place sooner rather than later to assist entities in complying with the new standards.
8.41	Minnesota Power		Regarding the Violation Severity Levels, how does the Standards Drafting Team envision these being applied? If systems are not identified, how will an auditor know how many are missing? For example, VSL R2 mentions “incorrectly categorized” BES Cyber Systems. How will an auditor determine that a Registered Entity has incorrectly categorized systems when they have documented their review and categorization process? Also, for VSL R3, it seems arbitrary that a difference of 20 days takes a violation from a “Lower” to a “Severe” VSL. How were those numbers determined?
8.42	Wolverine Power		See comments listed for 1.a
8.43	Nuclear Energy Institute		Several:

#	Organization	Yes or No	Question 8 Comment
			a) In the Introduction, Section 3 (A.3), the word "could" should be replaced with "would." b) In the Introduction, Section 5: Clarification should be made that upon approval by FERC, CIP 010-1 supersedes, in their entirety, all prior versions of the CIP standards, and that compliance with the requirements of CIP-010-1 must be in accordance with the implementation schedule for CIP-010-1.
8.44	APPA Task Force		The APPA Task Force commends the drafting team on their work on CIP-010-1. We thank the team for its hard work and appreciate the team's consideration of our comments from the previous informal comment period. We think the standard is moving in the right direction and with this next round of comments should hopefully result in a set of standards that will meaningfully improve the reliability of the BES and address the cyber security issue for the industry.
8.45	US Bureau of Reclamation		The changes in the Standards to focus on Cyber Systems is reasonable, but the definitions for Cyber System Components, Cyber Systems, and Control Centers may need further refinement (or application examples) to help implementation staff address fundamental questions. As an example: Is an isolated electronic relay providing generator protection for a single large generation resource a BES Cyber System? Under the present definitions it would appear to be (it certainly qualifies as a BES Cyber System Component). If it is a BES Cyber System, it is subject the requirements of CIP-011 based on the impact of the "System." Is this really the intent of the drafting team(s)? Would it not be better to establish select security criteria for isolated components (specifically components such as cyber-based relays and synchronizing equipment) that fit the nature of their deployment - rather than trying to fit them into a "system" category?
8.46	Southern California Edison Company		The CIP-010 and CIP-011 drafts should indicate how these standards will replace or supplement the current CIP-002 through CIP-009. If the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. A gap of unused numbers

#	Organization	Yes or No	Question 8 Comment
			between CIP-001 and CIP-010 will potentially cause future confusion.SCE also requests the Standards Drafting Team clearly define what should be included as Protective Systems. Additionally, a matrix mapping CIP Version 3 requirements to CIP Version 4 requirements would be very helpful.
8.47	LADWP		The CIPs should evolve in a manner that does not minimize the investment of resources already expended to meet compliance but should leverage the work done already. The draft version 4 is a drastic change and would require multiple years for a Responsible Entity to approach compliance. If CIP version 4 is implemented as currently drafted, there would be a huge resource drain to rewrite language and requirement references that are now part of numerous policy and procedures as well as contract packages.
8.48	Xcel Energy		The definition of BES Cyber System uses criteria that the element must be capable of causing a system disturbance or other impact within 15 minutes. We would like to know if or classification based on the 15 minutes must rely on analysis or if judgment/expert opinion is allowed. 1.5 Please clarify that the “Texas Interconnection” refers to ERCOT. 1.5 If a cyber system can only impact 1 transmission line within a substation containing 4 or more lines, it should not be classified as high. Suggest 1.5 wording be changed to Each BES Cyber system that can affect operations for: “Four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher located at Transmission Facilities within the Texas and Quebec Interconnections 1.9 It is not clear why facilities serving a nuclear site under NUC-001 are high impact if the nuclear site itself is not High impact.
8.49	Dairyland Power Cooperative		The distinctions between systems and facilities are unclear. The Requirements in CIP-010 shift to a systems oriented identification. Yet the Attachment I/II definitions still rely

#	Organization	Yes or No	Question 8 Comment
			on the concept of facilities and almost seem to equate facilities with systems. These distinctions need to be clear.
8.50	Con Edison of New York		The Drafting Team needs to take into account the fact that the ability to work on any cyber systems in a substation will typically already require a detailed work permit process which includes getting a work permit from an operating authority with jurisdiction on the equipment. The employee working on the cyber system must typically be an approved employee to work on these systems.
8.51	FEUS		The drafting team should consider an alternative for the VSL categorization. By basing it on a percentage, it could potentially unfairly affect smaller entities with fewer BES Cyber Systems. A smaller entity will inherently have fewer BES Cyber Systems, so missing a single classification of a BES Cyber System could automatically merit a severe violation. For example, an entity with as few as 5 BES Cyber Systems that misses the identification of a single system would be in a severe category. A larger entity with inherently more BES Cyber Systems can fail to identify more BES Cyber Systems and have a lesser severity level. An entity with 50 BES Cyber Systems can fail to identify 8 before reaching a severe violation level. The risk of failing to identify 8 BES Cyber Systems puts the BES at a much higher risk than failing to identify 1 BES Cyber System.
8.52	Indeck Energy Services, Inc		The FERC directed guidelines to Registered Entities on the risk based assessment methodology are missing.
8.53	PacifiCorp		The low, moderate and high violation severity levels for R3 do not seem to measure the correct violation criteria. The number of days after a change is completed should not be the sole criteria. The number of days after a change is completed should not be the sole criteria for determining whether a violation was harmless or severe. This is especially true for a standard that currently has no meaningful qualifier to allow for routine or de - minimus changes to elements of the BES without triggering a full review. These criteria should track other violation criteria that consider whether the violator had an adequate

#	Organization	Yes or No	Question 8 Comment
			process in place for the types of changes that merit a re-evaluation. Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too perscriptiveprescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.54	National Rural Electric Cooperative Association (NRECA)		The Purpose section of CIP-010-1 and CIP-011-1 should be similar in regards to the facilities it refers to. Add the word in all CAPS to the CIP-010-1 Purpose to bring it in line with the Purpose in CIP-011-1:".... that execute or enable functions essential to reliable operation of the INTERCONNECTED BES..."
8.55	SCE&G		The SDT needs to consider how auditors may interpret the words of the standard

#	Organization	Yes or No	Question 8 Comment
			differently. The language needs to be written clearly and concisely enough so that a consistent interpretation of the standard will be applied by all auditors across all regions. Consideration of Nuclear Facilities: Definitions for BES Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the Nuclear Regulatory Commission (NRC) in NEI 08-09 Revision 6 for Critical System and Critical Digital Asset; recommend for nuclear systems subject Federal Energy Regulatory Commission (FERC) 706-b definitions for FERC and NRC regulated systems are consistent. This will avoid regulatory uncertainty as well as human error at nuclear facilities. CIP-010-1 R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? The implementation schedule for CIP 10 - 11 versus CIPs 02-09 requires doing the same reviews twice and is an unnecessary burden on nuclear licensees as well as other FERC critical assets. The deterministic nature of the security controls in CIP 11 do not provide for acceptance of Common Controls as defined by NIST 800-53. In nuclear facilities with mature physical security programs, engineering control programs, and physical segregation of trusted industrial control system networks from un-trusted networks, CIP 11 should include provision for NIST 800-53 Common Control processes.
8.56	Consultant		There appears to be inconsistency in use of terminology throughout the standard as the terms apply to defined glossary terms, new definitions contained in this standard, and what appear to be 'common terminology' that is not defined. The terminology should be reviewed and applied consistently to avoid ambiguity and confusion. It is not clear that the implied process in the requirements (R1. Identify BES Cyber Systems, R2. Categorize Cyber Systems) is the best methodology. This seems to be missing the first step of the process: 1. Identify the BES assets (Facilities, Elements, &

#	Organization	Yes or No	Question 8 Comment
			Control Centers). The previous versions of CIP-002 started with the identification of BES assets followed by inclusion or exclusion as Critical Assets using the Risk-Based Methodology. As the current standard is written it seems to have lost the step to identify BES assets to which the CIP-010 R1 & R2 steps would be applied. Suggest adding the 'first step' to identify BES assets. This would probably require some restructuring of the current R1 & R2 statements to apply them to the identified BES assets.
8.57	Ameren		There are no system performance requirements as part of the determination of “High”, “Medium”, or “Low” impact to the BES other than item 1.7. The addition of performance requirements from the TPL standards (TPL-003 and 004) could further help to identify which facilities have the biggest impact on the BES and reduce the number of “High” and “Medium” impact facilities identified to provide significant cost savings to the industry.
8.58	WECC		Utilizing the prescriptive nature of CIP-010-1 Attachment II would be very useful as a rewrite of CIP-002-4. The CIP-002 through CIP-009 format lends itself very well to being audited. What is needed is clarification and explicit language. The current standard needs to be made better not replaced.
8.59	Kansas City Power & Light		Very concerned regarding the “lines” that have been drawn in Attachment II. What is the engineering basis for any of the “bright line” thresholds that have been expressed in Attachment II? Recommend thoughtful consideration regarding operating assumptions be developed an analysis be performed to establish the facilities that should be considered HIGH, MEDIUM and LOW reliability impact. Operating criteria should be established to determine what has HIGH, MEDIUM and LOW reliability impact. In addition, there are facilities that have NO IMPACT to reliability of the BES. Whatever criteria is established, a “smell test” should be done to see if the criteria works. There are numerous small Regional Entities that are obviously no impact to the reliability of the BES, and if any of these requirements and definitions draw any of the facilities of these small entities into the CIP Standards, something is wrong and adjustment to the criteria

#	Organization	Yes or No	Question 8 Comment
			needs to be considered.
8.60	ERCOT ISO		Violation Severity Levels: Recommend that VSLs address “identify” and “document” BES Cyber Systems. “Identify” and “document” are noted separately in the requirements. Attachment I: What is the originating source for this? Can it be referenced? What does “BES elements” mean?
8.61	Pepco Holdings, Inc. - Affiliates		We agree with EEI’s comments regarding not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES (e.g. serially attached electronic components versus those that use routable protocols; devices that communicate to each other within a self-contained, isolated network segment versus devices that communicate via routable protocols across multiple geographic or logical boundaries, and devices that use dedicated (and non-routable) point-to-point communications channels versus devices that communicate via routable protocols across multiple geographic or logical boundaries). Would suggest that consideration be given up front in CIP-010 to the types of communication/risk when developing security requirements.
8.62	We Energies		We Energies agrees with EEI. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of

#	Organization	Yes or No	Question 8 Comment
			compromise. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.63	Progress Energy (non-Nuclear)		We need definition of when the CIP requirements "turn on" during new plant construction, commissioning, and/or start-up. Recent major projects with CIP CCA's have been add-ons to existing facilities. We have used the model that until we "logically" connect to the existing facility ESP the full CIP requirements were not required. The next projects will be new facilities with no ESP logical connection to the existing steam plants. We should recommend wording that states that the CIP ESP and PSP requirements do not turn on until the plant is turned over to Energy Supply for commercial operation and it becomes available to ECC. Argument being that during testing ECC manages other generation assets to allow for testing impact on BES. Standard malware protection rules (A/V, etc.) would still apply. Have the regional entities auditing & compliance groups made an initial assessment as to the relative impact when compared to existing standards? For example do they anticipate significant increase in compliance records and audit evidence required? Unofficial Comment Form - CIP-010-1 and CIP-011-1 Cyber Security Order 706 (Project 2008-06)

#	Organization	Yes or No	Question 8 Comment
			Is there expected to be a TFE process for these standards - based on current experience the TFE process is more onerous and adds considerable paperwork without effectively enhancing security of BES. Need consideration for redundancy, backups, alternate systems in relation to required levels of protection - CIP-010-1 R1 makes no provision for considering redundancy, backup systems, or alternate systems which may be in place to 'provide assurance in the resiliency of these functions.' But according to the NERC document Guidance for the Electric Sector: Categorizing Cyber Systems, providing for the 'assurance in the resiliency of these functions' is part of 'The Purpose of Categorizing BES Cyber Systems'. Failure to consider these additional systems as layered safeguards and thereby reducing the criticality of any one of them may mandate that each such BES Cyber System be considered equally essential and critical. The result would be to provide disincentives for the responsible Entities to implement these additional layers - reducing the assurance in the resiliency of these functions. This would be contrary to the stated purpose of 'reducing risk to the performance of functions.' Need better provision for standards tailored to various asset types - Although the new standards will bring even more 'single use' equipment into focus, the standards are designed to protect 'multi function' PC based equipment from the attack vectors that they present. The standards need to take into consideration equipment that doesn't require protection (or extra work such as a TFE) for vulnerabilities that do not exist. Example: A terminal server which is a 'single use' type platform that only does protocol conversion between serial and Ethernet communications presents very few attack vectors. The same functions could be performed by a fully functional PC but that device would present a much larger opportunity for a hacker. The current version of the standards will actually make it more advantageous for entities to implement this function using the larger target of a fully functional PC rather the 'single use' type device simply because of ease of compliance. Recommend implementation timeline:

#	Organization	Yes or No	Question 8 Comment
			High - 4 years Medium - 4 years Low - 4 years
8.64	US Army Corps of Engineers		Will there be official guidance documents, such as the DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems?
8.65	Verizon Business		1. It is not clear whether electricity trading was considered in the draft standard. 2. Attachment III Section 1.11 discusses "BES Elements that perform automatic aggregate load shedding of 300 MW or more." This statement should be revised to specifically exclude Smart Grid Distribution. 3. This standard should be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version are addressed completely. 4. The inclusion or exclusion of "non-routable protocols" under CIP-002-4 needs to be addressed. For instance, if the standard included all protocols, then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems." This would be a substantial change to the Registered Entities, and compliance would be difficult. Overall, non-routable protocols should be included in the CIPs as well as routable protocols. 5. An explanation is required for the inclusion of Distribution Provider in Section 4, Applicability. The inclusion herein has caused confusion for Smart Grid implementation. The Distribution Provider should not be included. 6. In the BES Cyber System Component definition, the word "Disturbance" is capitalized. This word should be defined in the Glossary and could be included as a

#	Organization	Yes or No	Question 8 Comment
			Local Definition in CIP-010. To assist implementing utilities, it would be useful to do some mapping and case studies of the transformation of “Critical Assets” and “Critical Cyber Assets” to “BES Cyber Systems” and “BES Cyber System Components.”

9. **Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?**

Summary Consideration:

There was no clear preference from the compilation of responses received. Many entities liked the approach and structure provided by the posted CIP-010 and CIP-011, while a substantial number would prefer to keep the current CIP-002 – CIP-009 structure. Reasons provided by the latter centered around substantial compliance management frameworks implemented to support the CIP-002-CIP-009 structure. Others offered a hybrid approach, with some grouping.

The SDT has considered these comments and has opted to keep, in large part, the current structure of CIP-002 – CIP-009, with the addition of two new standards, CIP-010 and CIP-011. The two additional standards allow for some requirements from previous standards, where the subject matter did not quite fit, to be separated into the additional standards. In this manner, the SDT believes that each standard consists of a set of related requirements that support an identified purpose.

#	Organization	Yes or No	Question 9 Comment
9.1	WECC		This seems to be essentially a formatting issue. If the same requirements are included in either on single standard or multiple standards, the preference is with the individual reader. Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.Breaking CIP-011-1 into multiple standards lends itself very well to being audited. In either option, what is needed is clarification and explicit language. Regardless of the format, the standard (s) needs to be made stronger, more clear, more concise.
9.2	ISO New England Inc	Break CIP-011-1 up into multiple standards	- Disagree with the current structure- Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone

#	Organization	Yes or No	Question 9 Comment
9.3	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.
9.4	Entergy	Break CIP-011-1 up into multiple standards	A) Compliance Enforcement Problems: From the point of view of both implementation and auditing of Requirements it makes little difference as to the granularity of Requirements contained per Standard. However, from an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF). Consequently, even if only one Requirement in the single document approach is considered a "High" Risk Factor, then the entire Standard must be designated as High. This is problematic first in that not all CIP Requirements contained in either CIP-003-3 through CIP-009-3 or CIP-011-1 are of equal salience in terms of security vulnerability/risk created in virtue of failure to comply - some are indeed High, but by no means all. [However, note that

#	Organization	Yes or No	Question 9 Comment
			determination of Violation Severity Level (VSL) is not especially problematic - it's still a measure of just 'how far out of compliance' the Entity is.] Second, it is hard to imagine any Responsible Entity being 100% compliant with every Requirement in a single large Standard in any calendar year; it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year. Statistically, this does not speak accurately as to the quality of the NERC Standard, its Reliability Standards Program, or the industry's attentiveness or sense of urgency concerning the need for proper cyber security. For the reasons above, Entergy submits that a larger number of Standards, with fewer, more finely focused Requirements in each will serve our collective purposes much better.B) Cost Impact: Moreover, the cost of revising all the existing procedures, database systems, and other compliance programs to comport with a new numbering system alone is prohibitive for any company with a large number of cyber assets. There is no support in the administrative record for the notion that the current numbering system is a problem, or that the proposed combined "all-in-one" standard would improve grid reliability, security, or companies' efforts to comply with the standards. The change to a single CIP-011-1 Standard is arbitrary and of no salient value to anyone. Summarily, Entergy proposes that the: i) Organization and naming/labeling of Version 4 of the CIP Standards remain intact, i.e., simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another;iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact; and,v) Orientation in Version 4 toward protection of "data in motion" is applauded.
9.5	CenterPoint Energy	Break CIP-011-1 up into	As stated above, many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards.

#	Organization	Yes or No	Question 9 Comment
		multiple standards	CenterPoint Energy is concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard. CenterPoint Energy recommends keeping the current format.
9.6	Northeast Power Coordinating Council	Break CIP-011-1 up into multiple standards	Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.
9.7	FirstEnergy Corporation	Break CIP-011-1 up into multiple standards	Break CIP-011-1 up into multiple standards. Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.
9.8	City Utilities of Springfield, Missouri	Break CIP-011-1 up into multiple standards	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
9.9	Reliability & Compliance Group	Break CIP-011-1 up into multiple standards	Combining some of the standards may make sense but combining them all does not make it easier to comply, it instead creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense.Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?

#	Organization	Yes or No	Question 9 Comment
9.10	San Diego Gas and Electric Co.	Break CIP-011-1 up into multiple standards	Due to our previous CIP compliance efforts and all the documentation and Standard Operating Procedures currently in place, SDG&E recommends keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures. We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards. For example, most participating entities would now recognize CIP-004 as having to do with Personnel and Training, whereas combining all the CIP-003 through 009 requirements in CIP-011 just makes it that much more difficult to leverage existing compliance efforts and documentation without a major revamping effort.SDG&E recommends maintaining the current format of standards as CIP-002 to CIP-009, and enhancing the required individual standards as necessary. The existing standards are clear by function and controls - based on general cyber security and systems security practices and controls with the goal of protecting Confidentiality, Integrity and Availability. The implemented standards cover policy, access, change control, monitoring, DR, etc..., and are simple to review, document, communicate, audit and coordinate activities against. Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
9.11	E.ON U.S.	Break CIP-011-1 up into multiple standards	E.ON U.S. prefers that individual standards be used instead of the combined standards as outline in CIP-011.

#	Organization	Yes or No	Question 9 Comment
9.12	Matrikon Inc.	Break CIP-011-1 up into multiple standards	For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.The second reasoning for maintaining similar numbering is the mapping exercise of CIP 002-009 to CIP-010 and CIP-011. If the first priority is to perform the mapping between the two evolutions of the standard, then organically CIP-010/011 will be organized. This will help all affected parties identify the differences, perform gap analysis, and implications to their environment much easier. Unfortunately, all organization will have the exercise of re-authoring a lot of their own NERC CIP compliance procedures to catch up with the new terminology, numbering, and requirements. This will help to maintain compliance with CIP-002/009 while implementing CIP-010/011. Regardless if this is performed by the SDT, every Responsible Entity and Auditor is going to have to do this exercise anyways, with subtle differences.My suggestion is to consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next “decade”, whereby the second-digit is incremented.
9.13	Exelon Corporation	Break CIP-011-1 up into multiple standards	Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability. Unless there is a strong basis for making such a dramatic change to a set of standards that have not been in force for many years, Exelon sees neither need nor value in making such a dramatic change. This change will result in essentially starting from the beginning from a compliance program perspective. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.14	USACE HQ	Break CIP-011-1 up into multiple standards	I suggest to break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System. This way it is more clear what is required for each impact level system.
9.15	Progress Energy (non-Nuclear)	Break CIP-011-1 up into multiple standards	If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.
9.16	Indeck Energy Services, Inc	Break CIP-011-1 up into multiple standards	In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function. Not all of these standards apply equally to all facility types or functions. Unmanned facilities with direct communications with a BES control facility need a different set of requirements from a continuously staffed facility without direct communications with a BES control facility. Requirements for a BA are different than for a GOP.
9.17	MWDSC	Break CIP-011-1 up into multiple standards	It is confusing that the tables for each major category only show those requirements with different impacts, while there are other requirements that apply to all impacts. Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change. This may cause more confusion whether anything else changed and create more wasted paper. Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
9.18	Platte River Power	Break CIP-	It would be clearer if the requirements were organized based on their objectives:

#	Organization	Yes or No	Question 9 Comment
	Authority	011-1 up into multiple standards	physical security, system security, boundary security, personnel management, access, etc. One document would be fine if the requirements matched up with the standards and the sub-requirements matched up with the requirements.
9.19	Allegheny Energy Supply	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
9.20	Allegheny Power	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.21	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.22	MidAmerican Energy	Break CIP-011-1 up	MidAmercian Energy does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed

#	Organization	Yes or No	Question 9 Comment
	Company	into multiple standards	will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.23	CWLP Electric Transmission, Distribution and Operations Department	Break CIP-011-1 up into multiple standards	Monitoring changes to the requirements would be easier if they were separated into different standards.
9.24	Con Edison of New York	Break CIP-011-1 up into multiple standards	Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.
9.25	Michigan Public Power Agency	Break CIP-011-1 up into multiple standards	Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.
9.26	PacifiCorp	Break CIP-011-1 up into multiple standards	PacifiCorp does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.27	Florida Municipal Power	Break CIP-	The addition of sub-headings into CIP-011 is illustrative of the need to separate them.

#	Organization	Yes or No	Question 9 Comment
	Agency	011-1 up into multiple standards	From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
9.28	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.29	Emerson Process Management	Break CIP-011-1 up into multiple standards	The original setup seems indicating some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.
9.30	Southern California Edison Company	Break CIP-011-1 up into multiple standards	The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework.SCE supports the

#	Organization	Yes or No	Question 9 Comment
			modification of the CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements. But on the other hand, combining all controls into "one standard" is a cause for concern.
9.31	LCEC	Break CIP-011-1 up into multiple standards	The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES. Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.
9.32	Old Dominion Electric Cooperative	Break CIP-011-1 up into multiple standards	This draft is far too cumbersome. Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.
9.33	Pepco Holdings, Inc. - Affiliates	Break CIP-011-1 up into multiple standards	We agree with EEI's comments.
9.34	We Energies	Break CIP-011-1 up into multiple standards	We Energies agrees with EEI comments: It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.35	Luminant	Keep CIP-011-1 as one document	future changes that do not impact the compliance domentation numbering should be considered
9.36	FEUS	Keep CIP-011-1 as one document	Having CIP-011-1 as one document makes it more streamlined and is easier to follow. The concern FEUS has is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
9.37	Public Service Enterprise Group companies	Keep CIP-011-1 as one document	Having the requirements in a single standard significantly improves understanding and ease of reading.
9.38	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.39	Southwestern Power Administration	Keep CIP-011-1 as one document	Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
9.40	Dairyland Power	Keep CIP-011-1 as	One document is better.

#	Organization	Yes or No	Question 9 Comment
	Cooperative	one document	
9.41	Green Country Energy	Keep CIP-011-1 as one document	One document makes it a lot cleaner for a smaller entity to deal with.
9.42	Progress Energy - Nuclear Generation	Keep CIP-011-1 as one document	Security controls included in CIP-011-1 are similar to the Security Controls established by Nuclear Energy Institute (NEI) 08-09, Revision 6, Appendices D and E. These security controls are based on one or more National Institute of Standards and Technology (NIST) 800 series standards and have been accepted by the Nuclear Regulatory Commission (NRC) in a letter dated May 5, 2010. Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.
9.43	Consultant	Keep CIP-011-1 as one document	Subject to the following:1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything.3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statment (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be

#	Organization	Yes or No	Question 9 Comment
			implementing requirements for that objective. This approach should also resolve items 1 & 2 above.
9.44	RRI Energy	Keep CIP-011-1 as one document	The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
9.45	Bonneville Power Administration	Keep CIP-011-1 as one document	The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements.Having CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.
9.46	Detroit Edison	Keep CIP-011-1 as one document	The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with subrequirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.
9.47	Dominion Resources Services, Inc.	Keep CIP-011-1 as one document	Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
9.48	Manitoba Hydro	Keep CIP-011-1 as one document	We agree with the proposed approach which creates a clear list of security requirements within a single standard. This addresses some of the complexity with the existing cyber security standards. We are, however, concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The

#	Organization	Yes or No	Question 9 Comment
			proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
9.49	Hydro One	Keep CIP-011-1 as one document	We agree with the proposed format for simplicity purposes. However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
9.50	Minnesota Power	Keep CIP-011-1 as one document	With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.
9.51	Tenaska	No preference	A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
9.52	Network & Security Technologies Inc	No preference	Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
9.53	US Army Corps of Engineers, Omaha Distirc	No preference	Combined this standard covers a very large number of requirements. Note the drafting committee divided the standard into several logical groupings for the presentation of the standard.

#	Organization	Yes or No	Question 9 Comment
9.54	ERCOT ISO	No preference	Either option is acceptable. Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).
9.55	Southwest Power Pool Regional Entity	No preference	Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements. The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references. The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated. Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
9.56	Pacific Gas & Electric Company	No preference	Keeping CIP-011 as one document reduces complexity and makes overall understanding easierBreaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects
9.57	SCE&G	No preference	The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
9.58	Southern Company	No preference	The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

#	Organization	Yes or No	Question 9 Comment
9.59	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	No preference	Violations are by requirement, so whether it is one standard or multiple standards makes no difference.
9.60	Independent Electricity System Operator	No preference	We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standard that applies generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.These comments notwithstanding we still offer some comments on the remaining questions.
9.61	Verizon Business	Keep CIP-011-1 as one document	One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Suggestions for the purpose statement for the draft CIP-011 standard included several suggestions for rewording as well as comments expressing confusion around the term BES Cyber Systems. Several commenters expressed that the owner of BES Cyber Systems should have responsibility for compliance with the Standards and the Purpose statement did not reflect this.

In response to the industry comments received for draft CIP-011, the CSO706 SDT decided to divide up the draft CIP-011 requirements and include them in the multiple Version 5 CIP Standards (CIP-003 through CIP-011). Therefore, the purpose statement included with the draft CIP-011 no longer applies.

#	Organization	Yes or No	Question 10 Comment
10.1	PacifiCorp	Agree	: PacifiCorp agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.2	WECC	Agree	Agree with the genearal purpose however, The term "necessary cyber security protection" in the purpose statement has no meaning without a frame of reference. The purpose statement may be used to clarify intent where the standard language is ambiguous or vague, so it should explicitly state the objectives of the standard.The phrase "...that perform functions essential to reliable operations of the interconnected BES" in the purpose statement is redundant. BES Cyber Systems are defined elsewhere so this clause adds confusion at best, and contradicts at worse.
10.3	Southwest Power Pool Regional Entity	Agree	As an overall purpose, the statement is OK. Consider addressing the issue of "responsibility" as it pertains to multiple entity aspects, including joint ownership

#	Organization	Yes or No	Question 10 Comment
			agreements, different owners versus operators, and the like.
10.4	Old Dominion Electric Cooperative	Agree	I agree under the assumption that this is in line with the enabling legislation in the Energy Policy Act. I disagree that this is the best way to go about achieving this goal.
10.5	Green Country Energy	Agree	I agree with the concept, however as I will repeat through the remainder of the comments, A guidance document is needed to address key points desired to be accomplished by these policies. This will also reduce the subjectivity during audits of this and all the following requirements
10.6	Progress Energy (non-Nuclear)	Agree	It is still unclear if cyber security implies that an external communications capability is available. Definitions and references seem to indicate that we can have a BES cyber system component without external connectivity.
10.7	US Bureau of Reclamation	Agree	Recommend that the Drafting Team change "Functional" to "Registered" in the 1st line of the Purpose. Add "they" between "that" and "execute" in the 3rd line of the Purpose statement.
10.8	Minnesota Power	Agree	This purpose statement is generally acceptable, with clarification or correction to the following: o What is the definition of “responsible”? Minnesota Power recommends changing this to “own” as is stated in CIP-010-1, R1. o The reference to “Functional Entities” should be replaced with “Registered Entities.” “Functional Entities” is not a defined term.
10.9	San Diego Gas and Electric Co.	Agree	While SDG&E agrees with the purpose of CIP-011 as applied to the various requirements, we would like to see additional language that would help clarify the meaning of the phrase “responsible for”. What if an entity owns a particular asset but does not operate it?
10.10	ISO New England Inc	Disagree	- Please provide additional clarification. Especially with regard to “necessary cyber security protection”.- Suggest changes from “cyber security protection” to “cyber

#	Organization	Yes or No	Question 10 Comment
			security controls".
10.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Advise replacing "are responsible" with "operate." Where one Entity may own the BES Cyber System, and another Entity operates the same BES Cyber System, it must be clear who will be responsible for developing and implementing the policies. In many instances, the owner of a BES Cyber System only has monitoring capability, and no control or supervisory role in the BES Cyber System. Owners should not be responsible for creating policies for Systems they do not fully understand; owners should only be responsible for securing the BES Cyber System Components that they operate.
10.12	FirstEnergy Corporation	Disagree	As stated in our opening remarks, we fundamentally oppose the change in terminology. Additionally we disagree with the need for functional categorization as described in Attachment I. Therefore, we do not support the purpose statement of CIP-011.It is suggested that the proposed definitions for BES Cyber System and BES Cyber System Component could be combined to redefine the existing Critical Cyber Asset term allowing industry to better leverage its existing CIP implementation.Additionally, there is a concern, in going with the concept of "BES Cyber Systems" that it will expand beyond the systems that are directly responsible for the reliable/safety of the BES and into business systems.
10.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
10.14	ERCOT ISO	Disagree	Consider: "To ensure Responsible Entities develop cyber security programs to provide for appropriate protection of the BES Cyber Systems for which they are responsible that execute or enable functions essential to reliable operation of the interconnected BES."
10.15	Consultant	Disagree	Cyber security policies or cyber security protection do not 'execute' functions essential to reliable operation of the BES. Suggest removing the word 'execute'."interconnected BES" is not a defined term. Suggest removing the word 'interconnected'.

#	Organization	Yes or No	Question 10 Comment
10.16	US Army Corps of Engineers, Omaha Distirc	Disagree	Delete everything after "for which they are responsible." It reads awkward and is merely restating the meaning of BES Cyber System.
10.17	Kansas City Power & Light	Disagree	Do not agree with ensuring security policies in the purpose. The express purpose of these requirements should be to identify the cyber systems that require protection and the level of protection to achieve. There is no need to include a purpose of entering into the management of an organization and the levels an organization deems necessary to achieve compliance with the these CIP Standards or any other NERC Reliability Standard.
10.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the statement as follows: "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems."
10.19	American Municipal Power	Disagree	I feel the purpose is not based on reliability. The purpose should not restate the applicability section.
10.20	Wolverine Power	Disagree	I have a concern with how to detrmine hat constitutes a "BES Cyber Ssystem" I don't think the standards are clear.See comments listed for 1.a fro explanation and proposed solution
10.21	Turlock Irrigation District	Disagree	Is the use of the words "the BES Cyber Systems for which they are responsible" above meant to be the same as the words "the BES Cyber Systems that it owns" which are used in CIP-010-1 R1? The Purpose of CIP-011-1 focuses compliance responsibility on the entity that is responsible for the BES Cyber Systems while CIP-010-1 R1 focuses compliance responsibility on the owner of the BES Cyber Systems.
10.22	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."

#	Organization	Yes or No	Question 10 Comment
10.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes implementation responsibility of protection methods should tie back to facilities under the entities control and ownership.
10.24	Reliability & Compliance Group	Disagree	Recommend adding the words “and implement”. Also the phrase “execute or enable functions essential to reliable operation...” needs a more concise definition.
10.25	Independent Electricity System Operator	Disagree	See response to Q9.
10.26	Network & Security Technologies Inc	Disagree	Suggest replacing “enable functions essential to...” with “support functions essential to...”
10.27	Allegheny Energy Supply	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.28	Allegheny Power	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.29	EEI	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.30	Nuclear Energy Institute	Disagree	The phrase “and that execute or enable functions essential to reliable operation of the interconnected BES” should be struck as it is redundant to the definition of BES Cyber Systems.
10.31	APPA Task Force	Disagree	The purpose is not to “develop ... policies” as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. The APPA Taskforce suggests inserting the following “Purpose”

#	Organization	Yes or No	Question 10 Comment
			section:Purpose: To safeguard the reliability of the Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources.The APPA Task Force further recommends that each of the Requirements be reworded to separate out the stated objective to be accomplished from the text of the actual requirement and to state the objective prior the text of the Requirement. Auditors should not be placed in the position of having to evaluate if an entity has met the objective stated in the requirement, since this is essentially a subjective judgment. We feel this objective should not be part of the requirements. Here is one example of our proposed format illustrated with Requirement R5: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems. The APPA Task Force recommends adding the following "Objectives" section after the Purpose in this standard:A. Introduction 1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES. 4. Objectives:a. Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. b. Physical Security for BES Cyber Systems: To prevent and/or detect unauthorized physical access to BES Cyber Systems.c. Personnel Risk Assessment: To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. d. etc...If the Objectives are not incorporated into the Introduction, we recommend they be removed from the requirement all together. If the team determines they are necessary, they must be in a separate sentence prior to the requirement. See comments on Question #12 and all other questions regarding the requirement title.
10.32	Florida Municipal Power Agency	Disagree	The purpose is not to "develop ... policies" as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. FMPA suggests the following:np"To safeguard the reliability of the

#	Organization	Yes or No	Question 10 Comment
			Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources."
10.33	Indeck Energy Services, Inc	Disagree	The purpose of CIP-011, assumes that every facility registered with NERC is a cyber threat. It needs to differentiate functional entities to determine the impact on BES ALR. The functions identifies in Attachment I of draft CIP-010 are all important. Many of them are provided by hundreds or thousands of facilities. The cyber policies envisioned cannot ensure (that is guarantee) that there will be no blackouts due to cyber attack. [suggestion] "To require Functional Entities to develop, coordinate and apply adequate cyber security protection to the BES Cyber Systems for which they are responsible and that will achieve BES Adequate Level of Reliability." The coordination is to avoid unnecessary duplication of cyber security protection. This may require a different type of requirement that links connected parties, such as TO and GO, as to protecting particular facilities.
10.34	Manitoba Hydro	Disagree	The purpose statement appears to be missing words in the last line. Consider adding the words 'as outlined in this CIP-011-1' after the word 'responsible'.
10.35	Constellation Energy Control and Dispatch, LLC	Disagree	The purpose statement will need to be developed for each standard if CIP-011 is broken up into its major components.
10.36	Platte River Power Authority	Disagree	This comment is referring to an earlier comment suggesting a mechanism for identifying a "Responsible Entity" who is responsible for implementing and demonstrating compliance. With the "Responsible Entity mechanism in place I would suggest the following revision:To ensure the Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems that execute or enable functions essential to the reliable operation of the BES.
10.37	Entergy	Disagree	This Requirement uses the qualifier: "for which they are responsible." In Requirement 1 of CIP-010-1 (Question 3) the qualifier is "that it owns" - these two requirement statements must be consistent one way or the other.

#	Organization	Yes or No	Question 10 Comment
10.38	ReymannGroup, Inc.	Disagree	Vendor management and due diligence of 3rd party vendors is a growing area of risk across multiple industries, including the bulk power system. We believe the "Purpose" language should be enhanced to clearly cover the Functional Entities' internal practices and those of its 3rd party resources. This should include all 3rd party vendors that may have on-site or off-site access to the BES hardware, software, or data. For example, the information security risk associated with a growing use of data recovery service providers is not addressed in the NERC guidelines. Data Recovery is defined in Wikipedia as the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. The definition of a BES includes programmable electronic devices such as hardware, software, and data. It makes sense that as the demand for such electronic storage devices continues to rise, more equipment will be damaged or will fail due to daily wear and tear, physical damage, data corruption, or natural disasters (e.g., flood, fire, etc.) If backup copies of lost data on the BES are not available, the need for data recovery services will increase to keep pace with the use of BES technology. It could be made more clear to emphasis that Cyber security protections are applicable while the BES is in operation and off-line. BES could be taken off-line for repair or other incidents such as a damaged hard drive and recovery of BES data, which will require a 3rd party vendor to recover sensitive data from the BES device.We recommend that NERC consider adding a new Requirement for Vendor Management as described in our comments to Security Governance and Policy (R1) and updating the R25 and R30 guidelines to address this 3rd party vendor data recovery risk. It is a very small aspect of day-to-day operations in the scheme of the Entity's priorities, which is why it has gone unnoticed - until now. As one regulator commented to us recently, "this is not a potential problem - it is a real problem." It can create a huge risk with a huge downside, if it is not controlled. Most organizations don't even realize that this "sleeper risk" exists, until it is too late. The good news is that with minor updates to proposed guidelines, NERC can educate entities and others about the risk associated with the use of data recovery service providers and provide meaningful tactical guidance on how to manage such risk. The current initiative to revise the CIP Cyber Security Reliability Standards is a timely opportunity to take the initial steps.

#	Organization	Yes or No	Question 10 Comment
			Perhaps some organizations have included data recovery security practices and protocols in incident response or recovery planning. The challenge here is that it usually requires a material event to activate the incident response or recovery plans. In such instances, these plans do not address the proper day-to-day use of data recovery service providers that would not be considered a material event. Frequently, the use of a data recovery service provider does not trigger a formal recovery plan or incident response plan. It is unlikely that most entities would execute a recovery or incident response plan to recover data from a failed BES device in the normal course of day-to-day activities. In the interim, it would be helpful to Functional Entities and others if NERC issued supplemental guidance specific to this topic. This will help establish an immediate awareness of the risk and share much needed guidance on appropriate due diligence and security protocols for data recovery service provider activities, selection, and use. Specifically, the data recovery risk exists from a lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers.Whether a breach of sensitive information occurs from a hacker, cyber threat, insider threat, or a data recovery service provider, the potential cost, fines, reputational damage, and loss of trust that an organization would experience is huge. In short, data recovery service provider risk can create as much damage as other risks that are addressed in existing NERC guidelines, if adequate controls are not defined and implemented. A typical security and compliance budget will allocate funds to protect people, information, and assets within the perimeter. Many entities are also focused on protecting data on the inside of their organization from outside attacks. Data recovery, however, frequently falls into a low priority category that does not pop-up on the CISO's radar or in an information security risk assessment. The need for data recovery is frequently associated with an immediate sense of urgency, e.g., the data contained on the damaged storage device must be recovered right away. o Help Desk personnel or office technicians are usually tasked with the responsibility of selecting an outside third party vendor to recover the data quickly. o Such third party vendors may or may not be listed on an approved vendor list. o Frequently, the due diligence and selection process of such a vendor is limited to its financial stability, the cost of its services, and a fast

#	Organization	Yes or No	Question 10 Comment
			“turnaround time.”According to an independent national study - Security of Data Recovery Operations - published by the Ponemon Institute in December 2009 and conducted among IT security and IT support practitioners, there is a gap in security guidelines when selecting data recovery service providers. Specifically, o Sixty-four percent of the respondents decentralize the selection for data recovery vendors to the local level, e.g., Help Desk, while 24 percent are not sure how the vendor is selected. o Sixty-nine percent of the respondents do not have or are unsure if they have a policy for ensuring the protection of data during the recovery process. o Forty-nine percent say IT security is not involved in the selection process. o Only 20 percent believe data security is a major selection criterion. o Eighty-two percent say that it should be.A large percentage of respondents in this study (83 percent) reported at least one data breach in the past two years. Of the 83 percent who said the organization had a data breach, 19 percent said the breach occurred when a drive was in the possession of a third-party data recovery service provider. Forty-three percent of those respondents who said the breach occurred while at the vendor say it was due to a lack of data security protocols. Most organizations also have some additional backup and recovery procedures that overshadow the sense of urgency for more attention to data recovery practices on devices that were not backed up. In short, even with a strong backup recovery program, data recovery needs still arise. Seventy-nine percent of the respondents to the Ponemon study noted that their organizations have used or will continue to use a third-party data recovery service provider to recover lost data.Additional guidance is needed on how to extend current information system program practices to clearly address the protection of sensitive data, while it is in the possession of a third party service provider for data recovery. If the Entity has a strong vendor risk management program, it should include ALL vendors that have access to sensitive data, including data recovery vendors. Mandated vendor management practices apply to all stages of the information life cycle. Specific to data recovery vendors, this includes:âˆš Pre-selection and negotiation of Master Service Agreements with appropriate vendors. These should be reviewed by a risk management committee and audited on an annual basis.âˆš Due diligence of all third party vendors (e.g., financial stability, client references, information security

#	Organization	Yes or No	Question 10 Comment
			practices, etc.)âˆš Verification of the vendor's security procedures to govern the transfer of devices and sensitive information.âˆš Proof of internal information technology controls and data security safeguards, e.g., ISO 27001 certification, NIST SP 800-53 Audit Report, FFIEC Service Provider Examination Report, BITS Shared Assessment Report, or SAS 70 Type II Audit Report (especially if the data recovery involves financial information). The appropriate certification and audit report will vary depending on the service provider's client base.âˆš Proof of current training and certifications of engineers in all leading encryption software products and platforms.âˆš Adequate chain-of-custody documentation and network security.âˆš Vetted and performed background checks of its employees.âˆš Adequate procedures for the secure and permanent destruction of devices, when required.âˆš Capabilities for encryption of data files in transit and storage.âˆš Adequate clean room facilities, e.g., certified ISO 5 (Class 100).âˆš A security procedure for the analysis of the information and device upon return to the organization to ensure malware and other malicious software has not been loaded.The lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers is not a potential problem - it is a real problem! NERC guidelines are a key resource that can help educate functional entities and others to this sleeper risk and identify prudent risk management practices and controls.
10.39	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
10.40	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.41	GTC & GSOC	Disagree	We recommend the language should be consistent with CIP-010 "owns" versus "responsible for." As indicated in comments on 1.b above, "owns" may be problematic.

#	Organization	Yes or No	Question 10 Comment
10.42	Xcel Energy	Disagree	We suggest the Purpose be revised to state "...and apply necessary cyber and physical security protection..."
10.43	Verizon Business	Agree	Any "carryover exceptions" from CIP-002 to CIP-009 need to be identified. Specifically, OSI Layer 2 Protocols need to be explicitly addressed.

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many commenters requested more clarity regarding the terms used (including the following: "formal," "annually," "boundary protection," "security roles and responsibilities," "personnel," etc…). Commenters requested to have the terms used throughout the standard defined in this section. Additional clarity was sought in terms of the policy expectations, purpose, and structure. Specifically, there were numerous questions about what is meant by "policy language," along with concerns about how to demonstrate compliance with a policy. Some commenters also noted that the policy requirements were too prescriptive. There were some comments that led the SDT to believe that there was some possible confusion surrounding general policy hierarchy.

The SDT agrees with the need for additional clarification and clearer expectations with regard to the policy. The drafting team has provided clarification through the addition of guidance material related to items that should be included in policy, and has implemented a style for the measures in each requirement that can be used as an aid in setting clear expectations for possible audit evidence.

Some commenters raised questions about the requirements with respect to the Senior Manager; specifically with concerns about delegation and the potential for conflict with R3, or claims of double jeopardy between R1 and other requirements.

The SDT appreciates the concerns about double-jeopardy issues and the prescriptive nature of the requirements. As such, the SDT has proposed moving the prescriptive elements of the requirement to guidance. This approach will allow the Responsible Entity greater flexibility to create a policy that is meaningful for its unique environment, while still providing the foundation necessary for an effective cyber security program.

#	Organization	Yes or No	Question 11 Comment
11.1	Entergy	Agree	"Annually" must be defined. At least once every twelve months? At least once per calendar year (this could extend past 12 months). Please clarify.
11.2	Green Country Energy	Agree	Agree with the list, however I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these policies. Because the policies / requirements were designed not to be to prescriptive they in turn need references to give some expectations as to the points to be addressed within the

#	Organization	Yes or No	Question 11 Comment
			policies. This will allow flexability as to tailor the policy to each business, the policy will meet with the objectives of NERC / FERC and make the policies easier to audit. Is this what results based standards is all about...
11.3	Covanta Energy	Agree	Annually may be needed due to frequent challenges and changes to cyber hacking techniques.
11.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
11.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent, but believes the following improvements should be made:What does “formal” mean, does the drafting team intend a Company Policy?Terms used in later requirements ought to be defined here, such as unauthorized access, Cyber Security Incident(s), and electronic access controls.Terms that are ambiguous, such as “Boundary protection” and “media sanitization” ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clear the “Personnel ...” used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8, consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7
11.6	National Grid	Agree	In 1.2 please elaborate on “security roles and responsibilities”. What is the SDT looking the entities to include as part of this document?
11.7	Minnesota Power	Agree	Minnesota Power would like to see more detail regarding each of the topics on the list to help clarify the expected content of these policies. For example, item 1.3 requires the naming of a single senior management official, with no mention of the ability to also name delegates. Yet, Requirement R3 includes the following language: “...that are approved by the single senior management official...or their delegate...”

#	Organization	Yes or No	Question 11 Comment
11.8	Bonneville Power Administration	Agree	NOTE: This following comment deals more with structure of the document than it does with content: NIST SP 800-53 lists 19 families of security controls for Government systems. Although the purposes of 800-53 and CIP-011 are not equivalent, there seem to be 800-53 families missing from CIP-011 that address areas that should be of interest in CIP-011. Even if the individual controls are addressed in CIP-011, listing the families would be useful. In particular, it is unclear why Audit and Accountability, Contingency Planning, Identification and Authentication, Personnel Security, System and Communications Protection, System and Information Integrity, and Program Management are not addressed. We believe that incorporating these would be an improvement to the document. In the CIP versions 1, 2 and 3 standards organizations have had numerous and almost endless discussions about what “annual,” “annually review,” etc. means. Hours have been spent trying to figure out what these terms mean. Some have said that “annual” means within 13 months. Annual meaning “within 13 months” makes absolutely no sense. It would be extremely helpful to the industry if clarity were provided in CIP-011-1. The debate needs to end. There appear to be four different phrases that could be used to provide more clarity:1. “at least once every 12 months” - let’s assume that the organization reviews all of the various policies referenced in R1 on July 15, 2010, and again on March 15, 2011. Using this phrase and example, however, raises a couple of questions. When must the next review be completed? Is it no later than July 15, 2011, or no later than March 15, 2012? In other words, is there a window in which "annual" events must occur, "12 months +/- a month" or if you perform something early for efficiency's sake, does your annual date reset to the earlier date?2. “every 12 months” - the review would occur on the same date each year. This would be virtually impossible to manage. 3. “within 12 months of the last . . .” - in this case let’s assume that a review is performed on March 15, 2010. The next review would have to occur no later than March 15, 2011, but could occur earlier (let’s say it occurred on December 15, 2010). If it occurred on December 15, 2010, the subsequent review would have to occur no later than December 15, 2011.4. "anytime during the calendar year" - which would give the organization maximum flexibility in accomplishing the compliance activities.The Standards Drafting Team (SDT) should

#	Organization	Yes or No	Question 11 Comment
			provide more clarity as to what is intended and use an exact phrase rather than the word “annually” review. #3 - “within 12 months of the last . . . .” appears to be clearer than either of the others while #4 would provide a hard deadline that would not result in "date creep."
11.9	Dominion Resources Services, Inc.	Agree	Please see Dominion’s response to Question 9.
11.10	Reliability & Compliance Group	Agree	This could be better clarified. Some may interpret this to mean that procedures that address those topics will satisfy the requirement. A global definition of cyber security policy might help.
11.11	ISO New England Inc	Disagree	- Suggest changing the word “annually” to “a defined time frame” provided example at the end.- Suggest removing the “one or more formal” and add “documented and approved cyber security policies.”
11.12	Garland Power and Light	Disagree	* Please clarify the words "one or more" - does this require the review of all policies for the following functions
11.13	Consultant	Disagree	1. The list should include "Governance" as the first item. Suggest the first three items should be subheadings to the Governance item.2. Technically, R1 does not require designation of a CIP Senior Manager. As worded it requires a policy addressing the "Identification of a single senior management official...". Suggest an additional requirement statement requiring the Responsible Entities to designate a CIP Senior Manager, and document that designation.3. The mechanism for assigning responsibility is typically not a policy. Consider modifying the statement "Identification of a single senior management official with overall authority..." with "The senior management official's authority..." as an item to be addressed in the policy.
11.14	FEUS	Disagree	1.3 does not allow for delegation of authority for situations when the identified senior manager is unavailable. The Drafting Team should consider allowing a delegate or

#	Organization	Yes or No	Question 11 Comment
			alternative designated by the senior manager.
11.15	USACE HQ	Disagree	1.3 is missing the language that the single senior management official has the power to delegate some or all of the functions and/or actions to one or more named delegates. Also, double jeopardy is present since Requirements 6, 7, 11, 14, 15, 16, 17, 18, 20, 21, 23, 24, 25, 26, 27, 29, 30, and 32 cover part of or all of the policy documentation been required in 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, and 1.13.
11.16	Alliant Energy	Disagree	Alliant Energy agrees with EEI on verbiage suggestions and clarifications.
11.17	FirstEnergy Corporation	Disagree	As written the requirement and the list will require significant rework of existing policies for negligible benefit. In fact, the retraining that will be required will cause confusion and increase the challenge of achieving and maintaining compliance.Provide a standard that addresses all access issues (physical, logical, informational, etc.) instead of it being in multiple sections. Would also like to see emergencies being brought back into the main document, instead of having it part of each section.
11.18	Poplar Bluff Municipal Utilities	Disagree	Based on past experience, saying "Each Responsible Entity shall..." causes the Regional Entity to apply all CIP Standard requirements to all entities even if they own no Critical Cyber Assets. CIP-011 should clearly state that its requirements only apply to Entities that own BES Cyber Systems.
11.19	Con Edison of New York	Disagree	CIP-011-1 refers to timed requirements in various ways. The requirements should define the meaning and differences between annual, every year, within 3 calendar years, once every 12 months etc. There continues to be multiple interpretations of how within 365 days, within 12 months or in 2 calendar years, etc is defined.The term “annual” and “annually” should be defined. A suggested definition follows:Annual and Annually shall mean approximately every 12 months, but any period of no less than 9 and no more than 15 months.
11.20	E.ON U.S.	Disagree	CIP-011-1, R1.3 does not specify delegation by senior manager as currently permitted

#	Organization	Yes or No	Question 11 Comment
			under CIP-003-2. E ON U.S. proposes that delegation of authority by the senior manager be included as currently provided in CIP-003-2.
11.21	Dairyland Power Cooperative	Disagree	Communications between components/systems at different facilities or between different entities is an area lacking governance. Boundary protection is not sufficient.
11.22	ERCOT ISO	Disagree	Consider: “Each Responsible Entity shall develop, implement, approve, and annually review formally documented cyber security policies that address the following for its BES Cyber Systems:” Please clarify the meaning of “1.1. Applicability to organizational and third-party personnel”.
11.23	Progress Energy - Nuclear Generation	Disagree	Existing nuclear document hierarchy programs require review of policies, procedures, programs, and directives. The periodicity of the reviews should be consistent for nuclear generating facilities.See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
11.24	Southern Company	Disagree	For R1, What does “Addresses” mean? For 1.1...These are not usually actual third parties; the correct term is probably “non-employees acting on behalf of the Entity”.R1.3 and R3 create a requirement (a single responsible figure) that does not exist in any other NERC standard. Governance structures should be determined by the Entity and should not be regulated; the focus should be on the meeting of the other requirements and on the overall culture of compliance, so that the Entity can focus on creating the organizational structure that allows it to best meet the needs of CIP-011. This clause should be removed.Change the word "policy" in R1 to "policy or equivalent document".”Boundary protection” is undefined.
11.25	ReymannGroup, Inc.	Disagree	In many situations, outsourcing information technology tasks offers the Entity a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines or BES Systems that use it. Because the functions are performed by an organization outside the

#	Organization	Yes or No	Question 11 Comment
			Entity, the risks may be realized in a different manner than if the functions were inside the Entity resulting in the need for controls designed to monitor such risks. An additional security policy on 3rd Party Due Diligence and Vendor Management should be included. Functional Entities' should be required to establish a formal risk management processes to establish, manage, and monitor IT outsourcing relationships.
11.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	It is not clear what the Entity is responsible for if they do not own or operate any BES Cyber Systems. The assumption is not clear if the BES Cyber Systems list is null that Requirement R1 is then not applicable. Further, if a Low Impact BES Cyber System is the one and only System an Entity is responsible for, it is not clear whether a policy corresponding to an item (such as 1.5. Physical security) is required when the subsequent related Requirement pertaining to that item has a null listing for the Low Impact column in the following table (see Requirement R5). We advise the following change: "Each Responsible Entity who owns or operates one or more BES Cyber System shall develop, implement, and annually review formal, documented cyber security policies addressing applicability found in Requirements R2 through R32. The cyber security policies shall address each of the following categories, and include a statement of non-applicability for a category where appropriate:"
11.27	Western Area Power Administration	Disagree	It seems the requirement wants us to make the Physical Security Plan a part of the Cyber Security Policies? Is that what is intended?
11.28	Duke Energy	Disagree	List of topics need to be better defined. For example, 1.8. "boundary protection" may need to be changed to "electronic boundary protection". 1.9 should be changed to "Change Management" and "BES Cyber system maintenance" to "Configuration Management" for better alignment with NIST, COBIT and other control framework documents. Also, this policy is the only place where a Sr. Management official is mentioned. Does one or more imply a different policy per requirement or per business unit? If we have more than one policy, does the same Senior Manager need to manage and implement the requirements of the standard?

#	Organization	Yes or No	Question 11 Comment
11.29	NextEra Energy Corporate Compliance	Disagree	NextEra comments that during an emergency situation, a utility's primary objective is to end the emergency situations as soon as possible. For example, before, during and after the impact of a hurricane, the affected utility will mobilize much of its workforce to address system and customer restoration efforts. This may cause certain CIP requirements or deadlines to be missed for a short period of time. Moreover, there may be a need to relax CIP requirements, such as contractor qualification requirements for unescorted physical access into substations. Given the unforeseeable nature of emergencies, it is not possible to ensure all deadlines are met ahead of time, nor is it possible to pre-qualify all contractors, because it is not always known which contractors will be available or needed for emergency situations. A provision for emergency situations in the cyber security policy provides the utility and auditors alike with a framework and vehicle to ensure that any missed CIP deadlines or requirements that were relaxed are tracked, documented and that after the event, any missed or relaxed CIP requirements are addressed within a reasonable time after the emergency situation has ended. To implement emergency provisions and add clarity to other issues, NextEra proposes the following revisions:Each Responsible Entity shall have a documented cyber security policy related to the protection of BES Cyber System Components and BES Cyber Systems. The cyber security policy shall be reviewed every year during the month of March and updated, as necessary, no later than March 31st . The cyber security policy may also be updated as necessary. The cyber security policy shall include the following:B. The applicability of cyber security policy to employees and contractor personnel, including the manner in which the cyber security policy will be made available to employees and contractor personnel; C. The list of employees responsible for authorizing unescorted physical and/or cyber access to a BES Cyber System component consistent with R2-R4; D. The identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard, including contact information; E. A provision that addresses the Responsibility Entity's response to emergency circumstances in the context of CIP compliance. This provision shall address how the Responsibility Entity will track and document any missed CIP deadlines or CIP requirements held in abeyance

#	Organization	Yes or No	Question 11 Comment
			because of the emergency, and documents how, after the emergency condition has ended, any missed CIP deadlines or CIP requirements held in abeyance were brought back into compliance. An overview of the Responsibly Entity's approach to compliance is indicated with the following:
11.30	Ameren	Disagree	Overall this Requirement is vague and it will be open for interpretation during an audit. Suggest adding references to the corresponding requirements for sub-requirements R1.1 through R1.13. Also, if corporate policies cover all these areas would that be sufficient to prove compliance? Does the Senior Manager still need to approve this policy? These questions need to be answered to provide necessary clarity.
11.31	Tenaska	Disagree	R2 Clarify Sound Security PracticeR3 If a CCA were to go DOWN (NOT running) and the only vender that is available at that time that can fix it is not trained and/or criminal background and identity verified, does the standard address how to utilize the vendor and not violate the standard?
11.32	Exelon Corporation	Disagree	Requirement 1.3 should be revised to state a "Single Senior Management Official as per the entity's registration". Exelon is concerned that as presently written, Requirement 1.3 could be interpreted that Exelon as a corporate entity would need to have one and only one "single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard".
11.33	Manitoba Hydro	Disagree	Requirement R1 states that each Responsible Entity shall "... annually review one or more .... cyber security policies..." which implies that a entity could review a single policy in a year. If an entity developed a policy for each of the R1 sub-requirements, it would take 13 years to complete the policy review. Consider including cross references to each of the specific Requirement numbers in 1.1 to 1.13.
11.34	Southern California Edison Company	Disagree	SCE first makes the following specific comments in relation to this Requirement: (1) R1.1 "third-party personnel" is vague and needs to be more clearly defined; (2) CIP-001-1-R1 does not include provisions for emergency situations; and (3) R1 appears to exceed the

#	Organization	Yes or No	Question 11 Comment
			mandates of FERC Order 706, paragraph 355, in that a finite list of topics to include in the policy were not required by FERC.In addition to those specific comments, SCE also makes the following general comment: the contained list attempts to be too prescriptive but does not seem to be exhaustive at the level of detail that is chosen. For instance, R1.5 and R1.6 are essentially sub-components of R1.8. Policy objectives should be such that they are at a higher level and yet clearly state the desired cyber security control objective in a manner that can drive the development of procedures and tools. The drafting team should consider dividing the standards into thematic areas that require policy statements for each thematic area.
11.35	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that the Requirement R1 in CIP-011 be re-worded to change the text “annually review formal documented cyber security policies” to "annually review a formal documented cyber security policy framework that includes policies, standards, and guidelines." Not everything within the framework would be a policy.
11.36	Independent Electricity System Operator	Disagree	See response to Q9.
11.37	Allegheny Energy Supply	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:”Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.38	Allegheny Power	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber

#	Organization	Yes or No	Question 11 Comment
			Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.39	EEI	Disagree	Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.8.It is unclear as to the distinction between "1.9. Configuration change management;" and "1.11. BES Cyber System maintenance;" EEI suggests additional language to bring clarity or removing R1 1.11.
11.40	Alberta Electric System Operator	Disagree	The AESO suggests removing "formal, " from the proposal as it is subjective.
11.41	APPA Task Force	Disagree	The APPA Task Force agrees with the intent, but believes the following improvements should be made:What does "formal" mean? Does the drafting team intend a Company-wide Policy?Terms used in later requirements ought to be defined hereTerms that are ambiguous, such as "Boundary protection" and "media sanitization" ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clarified that

#	Organization	Yes or No	Question 11 Comment
			"Personnel ..." as used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8. Consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7The APPA Task Force believes that a number of the requirements listed in the tables throughout CIP-011 should be part of an overarching policy developed by each registered entity. While each utility's approach may be different, each registered entity should establish a coherent approach to cyber-security for its BES facilities. Requirement R1 should be viewed as the cornerstone of defining what is important to that utility. We believe the subsections of R1 are confusing and need clarification. Since revocation of access is common to many of the requirements The APPA Task Force believes the following Additional/Edited cyber security policies should be addressed in each entity's policy:1.2.1 Revocation of Access - Triggering Criteria
11.42	Southwestern Power Administration	Disagree	The phrase "leading and managing" is too restrictive, particularly for larger entities whose single Senior Management Official may have overall authority and responsibility, but his or her managers are the personnel who are responsible for leading and managing the details of the cyber program.1.3 Identification of a single senior management official with overall authority and responsibility for implementation of requirements within this standard;
11.43	Kansas City Power & Light	Disagree	The requirements here for a policy statement are much too prescriptive and are unnecessary. Policy statements should be global and encompassing and provide overall guidance. Recommend removal of a policy statement requirement from this proposed Standard. What purpose does this requirement serve or problem does this requirement solve? If this requirement is not included, what process or procedure will not be done in support of the remainder of the requirements? What is important are the processes and procedures that are in place to support the meat of the Standard. Mandatory and enforceable requirements are sufficient to stand alone. If a company feels they need a policy statement to support the CIP Standards, or any other Standard, let that be their decision.Do not agree with the need for requirement 1.3 regarding the need to appoint a single senior management official for overall authority and responsibility for leading and managing implementation of the CIP requirements. These requirements cover a broad

#	Organization	Yes or No	Question 11 Comment
			spectrum of systems and can engage many organizational parts of a company that one person may not be meaningful over all parts. NERC Reliability Standards compliance is sufficient weight to allow a company to determine the level of approval it needs to achieve and ensure compliance throughout an organization for CIP and any other NERC Reliability Standard.This Standard should focus on identification of cyber systems that need protection and an appropriate level of protection needed and move away from requirements that manage an organization such as R1.
11.44	LCEC	Disagree	The requirements of a formal policy should be defined.Boundary protection should be definedmedia sanitization should be definedCyber Security incident should be defined
11.45	Progress Energy (non-Nuclear)	Disagree	The term annual needs to be defined. Is it during a year, per 12 months, Jan 1 to Jan 1, 365 days, from what starting date, etc.R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.46	Michigan Public Power Agency	Disagree	The term annually is not consistently applied throughout the industry. For some organizations, this term means sometime in a calendar year, others apply it to their fiscal years. Some have applied it to mean a 12 month period based on the last event. The term either needs to be defined similarly to R3, where there is a local definitions box or the wording should be altered to remove the ambiguity.
11.47	US Bureau of Reclamation	Disagree	There are 6 "definitions" provided in CIP-011 which are needed to enforce the standards. Those 6 "definitions" need to be formally proposed as definitions in order to ensure enforceability of the standard.
11.48	Southwest Power Pool Regional Entity	Disagree	This requirement is not objectively auditable as written. Some level of explanation or direction needs to be defined to assist the entity and the auditor in a common

#	Organization	Yes or No	Question 11 Comment
			understanding of the expectation. While a simple regurgitation of the applicable enumerated (not "R") requirements is undesirable, the required polic(ies) need to state expectations in sufficient detail for the entity and its contract / vendor support personnel to understand the requirements of the policy as they pertain to implementing the standard(s).
11.49	American Municipal Power	Disagree	This requirement seems to be too prescriptive.
11.50	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
11.51	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"We Energies agrees with EEI: Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.52	American Electric Power	Disagree	What burden of proof is needed for items 1.4-1.13 to demonstrate implementation? Would this be the same proof that would be required to prove R2-R32 have been met? Is this an instance of double jeopardy? Failure to meet an item in R2 would also mean failure to implement the cyber security policy in R1. Suggest removing "implement" and allowing the R2-R32 requirements stand as proof of implementation.To what level of detail must the cyber security policy address the items? Is it sufficient to outline how they will be addressed? Different auditors may have different levels of detail in mind. Is this meant to outline a Responsible Entities Cyber Security Policy? The majority of the

#	Organization	Yes or No	Question 11 Comment
			details for compliance will be found in the procedures, not in policy statements. Does this do anything more than demonstrate a Cyber Security culture for a Responsible Entity?
11.53	ReliabilityFirst Staff	Disagree	What does the term “addresses” in Requirement R1 mean? How does an entity “address” sub-requirements 1.1 through 1.13? Sub-requirement 1.3 needs clarification regarding the definition of the phrase “single senior management official”. Does this phrase mean one individual for an enterprise or one individual for each registered function, or either?
11.54	WECC	Disagree	While we agree with the general proposal and list, this requirement should be rewritten to more clearly indicate what is required. The word formal should be defined in this context. The level of detail required in the policies should be indicated. Suggest changing review annually to "review at least every 365 days" or to "once during the calendar year" depending on what SDT's intent is for the requirement.(1.1) The phrase,” Organizational and third-party”, is inconsistent with phrases used in other requirements. Consider utilizing the same language used to describe individuals with access to cyber systems, or simply state “everybody”. (1.3) No specific documentation is required.(1.4 through 1.13) These requirements are very vague and offer no guidance at all as to the level at which these topics must be addressed. As written this requirement provides no value whatsoever, and is essentially unauditable.
11.55	Verizon Business	Disagree	1) Revise 1.9 Configuration Change Management to two separate lines – one for “Change Management” (which would apply to procedure compliance, etc.) and one for “Configuration Management. 2) The list is too vague. The prior approach with CIP-003 identifying the specific policies needed is preferable. 3) Item 1.8, “Boundary Protection” should be defined. The requirement should state whether it is consistent with the definition in NIST 800-53. 4) Revise 1.5 to read “Physical Security of BES Cyber System Components.”

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Note: CIP-011-1 R2 through R4 now resides in CIP-004-5 R1 through R3.

Several commenters suggested training related to networking, hardware, software, and electronic interconnectivity was either unnecessary or inappropriately targeted to individuals who have no working knowledge of the subject. The SDT agrees, and has made the training 'role-appropriate'; meaning only individuals whose roles necessitate such knowledge must receive the training.

Some commenters suggested the awareness requirements were not clear; specifically, use of the terms "proper use", "essential", and "sound security practice" were highly subjective. In response, the SDT has removed those terms and provided a requirement that can be audited more objectively.

In addition, some commenters suggested the quarterly reinforcement timeframe was too frequent. However, the SDT believes the requirement to update security awareness material is not overly burdensome and serves the reliability benefit of getting up-to-date threat information to a wide audience of individuals who can protect the BES Cyber Systems.

Some commenters suggested the annual timeframe for training individuals was inflexible and should allow for additional time to have individuals trained. The SDT agrees and has suggested the alternative use of the phrase "at least once every calendar year, but not to exceed 15 months between training."

Some commenters suggested the requirement for photographic identification was not necessary, since it adds the additional requirement for individuals to be on site for a personnel risk assessment. In response, the SDT acknowledges the requirement for photographic identification would necessitate individuals to be physically present. However, the requirement has been modified to require identity verification only for the initial personnel risk assessment performed for each individual.

Some commenters also suggested background checks were overly burdensome by requiring entities to cover all of the locations of residents within the past seven years. The SDT appreciates these comments but does not feel an adequate personnel risk assessment can be made without such information.

#	Organization	Yes or No	Question 12 Comment
12.1	Alliant Energy		Alliant Energy agrees with EEI to strike "sound" and "essential from R2. Also, additional

#	Organization	Yes or No	Question 12 Comment
			clarity around awareness training and the term “provide” and whether that requires completion tracking. Suggestion: Use the term “distribute” instead of “provide” to remove that implied obligation for awareness training.Additionally, R3.2 is not a practical requirement. Role based training is good; however, training should be specific to the responsibilities within the BES Cyber System and should not be prescribed by the standard. What is “specified” and why is training on networking hardware and connectivity required for users/operators of BES Cyber System Components who are not network administrators. What benefit is provided by providing technical training to personnel whose core competency and job duties do not require this level of expertise or understanding?R3.5 introduces a rolling creeping calendar. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.R4.1 is too prescriptive and does not take into consideration personnel with access and zero need for onsite presence.
12.2	National Rural Electric Cooperative Association (NRECA)		In R4, other than performing, documenting and updating personnel risk assessments, is there anything else that is required regarding personnel risk assessments? It does not appear there is, but wanted your confirmation on that.In R4.3, please specify what "at least once every seven years" means. This needs to be made clear so there are no misunderstandings. For example, if the last assessment was done on Jan. 15, 2001, does this provision mean the next one must be completed by Jan. 15, 2008?In R4.3, if a person never had an assessment completed and they already has access to BES Cyber Systems, when must the initial assessment be completed?
12.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R2The phrase “to ensure that personnel maintain awareness ...” should be removed from the requirement as it adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? It

#	Organization	Yes or No	Question 12 Comment
			seems like the drafting team is trying to add an objective for the requirement. If that is the case, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished. This comment should be carried on to all of the requirements.What does “reinforcement” mean?R3The term “granted authorized ... access” seems to be superfluous. Authorizing and granting are two different activities and the standard seems to prohibit granting access without first authorizing access (unless under certain specified exceptions). Consider just using the term “granted” in this requirement. The confusion between the terms “granted” and “authorized” is throughout the document and ought to be clarified.Consider correlating the training requirements in R3 with whether the person is a “user” or “administrator”, and whether the training is “job training”, a “refresher”, or “awareness”, with separate levels of training frequency and content for each of these categories.3.1 should not include “procedures” since these procedures are not identified elsewhere in the standard. The word “program” should be struck from “Visitor control program” since nowhere else in the standard is there a requirement for such a program. There should be no “back-door” requirements for procedures or programs such as these.3.5 should use the term “annually” instead of “at least once every twelve months” to give entities flexibility around various business needs on when during the calendar year to hold training flexible.R4The term “granted authorized” is superfluousConsider shortening “ensure a personnel risk assessment is performed” to “perform a personnel risk assessment”
12.4	Regulatory Compliance	Agree	R2 - Awareness - please clarify what are accetable forms of awareness.R3.2 - suggestion - STRIKE the reference to networking hardware and softwareR4 - Question: How do you propose to close the gap in regards to a criminal background check of an employee who has lived outside the country for a period of time in the past seven years that may not equal the 6 month period but long enough to be involved in supicious activities?
12.5	Emerson Process	Agree	R2 and R3 do not have tables for their applicability to three impact-types of BES cyber systems. Would it be better to include the tables for consistency with the rest of the

#	Organization	Yes or No	Question 12 Comment
	Management		standard?
12.6	Northeast Utilities	Agree	Recommend that R2 be clarified to indicate whether or not documentation must be provided that awareness material was received and understood by the CIP authorized personnel.Also, it is recommended that more guidance is provided on the level of training expected under R3.2 when stating "include training on networking hardware and software and other issues of electronic interconnectivity". The clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES Cyber System to become network engineers. For example: for operations personnel, what is the level of knowledge expected concerning networking hardware and software?
12.7	Green Country Energy	Agree	Will their be any guidance, footnotes or would ANY cyber security training be acceptable?
12.8	Independent Electricity System Operator	Disagree	- Suggest changing R3.2 so that it is only required based on personnel having a role in networks, etc. An operator and other personnel do not need to know how a firewall or switch works or its software. They may need to know how to use their token for t
12.9	Reliability & Compliance Group	Disagree	: "Sound security practices" is too vague of a term. How is this going to be audited? Who will determine what a sound security practice is? There needs to be an industry standard used. Is it going to be security practices listed under NIST 800-53? What about physical security practices? Without a benchmark, how can we measure adherence to the standard?R3 is way too cumbersome the way it is written. Keep the first part of the standard written the way it is. Then start a new sentence that says, "exceptions to this requirement must be specifically outlined in the responsible entities policies and are limited to emergency situations and acceptable alternative training." The part of the standard that reads, "impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems" is just confusing to read and understand. No matter what is done, try and make this requirement more than one sentence.R3 is better than the old

#	Organization	Yes or No	Question 12 Comment
			standard in how it defines how training should be handled for different roles and responsibilities. The 12 month timeframe needs to be tightened down even further. Is that 12 months +/- one month or is it every 365 days?
12.10	USACE - Omaha Anchor	Disagree	3.2 - should be worded closer to 3.3. or 3.4. You are giving training on network hardware and electronic connectivity to everyone with electronic access. This is counterintuitive - these folks for the most part do not have a need to know. They should only be given as much information as necessary to do their job.
12.11	Luminant	Disagree	3.5 We would prefer that training be conducted annually (completed within a calendar year) to avoid the confusion of tracking multiple comliance dates. How much documentation must be maintained? 12 months? 24 months, 36?
12.12	Platte River Power Authority	Disagree	Access to “any BES Cyber System” shouldn’t automatically require training on networking hardware and software or other issues of electronic interconnectivity. The training should be tailored to the individual’s job junction and not based on the BES Cyber System they have access to. For example, an operator doesn’t need to know the brand, model, configuration, or connectivity of the networking hardware that they’re using. They need only know the proper use of the asset they’ve been granted access to. I would like to avoid training individuals on the interworkings of our network when they have only been granted limited electronic access.
12.13	Liberty Electric Power, LLC	Disagree	CIP-011 R2 requires quarterly training for all plant personnel in cyber security. This is too frequent, and I would suggest changing to annual.CIP-011 R4.3 repeats the error of CIP-004 concerning the word “update”. There were many comments about requiring entities to have their long-time employees provide government-issued ID every “update” in the RFI, and the recordkeeping and potential for violation over trivia continues by not addressing the issue. I suggest changing the wording to define update as doing the background check again, and not getting into the realm of potential violations over lost wallets.

#	Organization	Yes or No	Question 12 Comment
12.14	E.ON U.S.	Disagree	CIP-011-1, R3.5 unnecessarily inhibits an organization's flexibility by mandating training every 12 months. E ON U.S. proposes that the Standard state "annual training", as currently required.CIP-011-1, R4 contains requirement of the Personnel Risk Assessment that should be revised. When seeking information from foreign nations concerning someone having resided in those foreign nations, compliance with these literal requirements may not be possible or feasible. An exception should be included to address a failure to obtain this level of evidence following a good faith attempt to do so.CIP-011-1, R4.3 ignores practical problems with requiring background checks of contractors and/or service vendors. Privacy concerns have raised many questions as to whether literal compliance is possible (especially in the context of this Standard which eliminates some of the language from the former CIP-004). E ON U.S. proposes that the requirement provided by the Regional Compliance Implementation Group ("RCIG") in RCIG-A-002 be adopted conceptually in this Standard.
12.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
12.16	LADWP	Disagree	Consultants or employees who lived abroad for a time may not be able to meet the 4.1 requirement to cover all locations where subject has resided. This could prevent proper authorization to BES systems.
12.17	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. CenterPoint Energy also suggests changing R3.2 to: "For personnel having job duties that require a role in BES Cyber System networking and electronic interconnectivity, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems."Numbering of sub-requirements for R3 and R4 conflicts with numbering of requirements in Tables R3 and R4 (there are two 3.1 and 3.2 and two 4.1 and 4.2).

#	Organization	Yes or No	Question 12 Comment
			CenterPoint Energy suggests moving all sub-requirements for R3 and R4 to tables to be consistent with other sections in CIP-011.
12.18	FEUS	Disagree	Disagree with Comments: 3.2 requires personnel with electronic access to have training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems. Extensive training on networking hardware and software should be limited to support staff or personnel with administrative privileges. It is not clear what 'other issues of electronic interconnectivity' is?3.5 requires training to be conducted every 12 months from the date of 'initial' training. The Drafting Team should consider revising the wording to allow for training more frequent to align with a regular training schedule for more personnel.4.1 requires a seven year criminal history check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. How would the Responsible Entity verify 'all locations' were identified by the subject for the criminal history check? If a subject is attending an out-of-area school via online courses it is not logical to perform a criminal background check for the location of the school.
12.19	Southern Company	Disagree	For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.For R3, How does "granted authorized electronic access" interact with the situation where a network service on a system is available to anyone who can get a packet to it? For 3.5, A specified 12-month cycle makes the training program much more difficult to administer without any benefit to reliability. A 14-month cycle would allow a reasonable annual training program to work.3.2 does not actually address any security need for the large majority of personnel with access. While Order 706 requires that NERC address the issue, that FERC requirement could be considered to have been met by the standards comment process without the wording making it into the final standard.Suggested rewrite of R3: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or

#	Organization	Yes or No	Question 12 Comment
			authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training, when specified in CIP-011-1 Table R3 - Cyber Security Training, prior to their being granted authorized access in order to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Temporary authorized access may be granted for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. Suggested rewrite of R4: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, undergo a personnel risk assessment, when specified in CIP-011-1 Table R4 - Personnel Risk Assessment, prior to their being granted authorized access in order to ensure that personnel have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.Temporary authorized access may be granted, without prior personnel risk assessment, for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. R4 is difficult to implement for the case of vendor support through remote access and for vendor support staff who are not citizens of the US, Canada, or Mexico.
12.20	Progress Energy (non-Nuclear)	Disagree	For R3 - the definitions in the box should be included as formal definitions. It is confusing with these text boxes hanging with only certain R#s.R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.For 3.1 - cyber training included incorrectly here...last bullet. Move to 3.2.4.1 First bullet comments- this new requirement appears to be a duplication of the E-Verify/I-9 process in which employment eligibility is verified for all new hires. All employers are required to verify their employees’ employment authorization and confirm that the identification documents presented are legitimate, thus establishing an individual’s identity covering

#	Organization	Yes or No	Question 12 Comment
			both the employee and contractor population. Additional verification through the PRA or requiring completion of the PRA after completion of the employment eligibility requirements adds additional steps to the process with no added value.4.1 Second bullet comments - the current regulation requires a 7 year criminal check. It does not specify that the check needs to cover everywhere the person worked or went to school and lived for > 6 months. The new language appears to be taken from a response to the interpretation given to the Army Corp of Engineers by NERC regarding how a PRA should be performed, which PE disagrees with.The current wording requires companies to gather much more data on an individual from the individual (as that is the only source of the information). Not even Nuclear attempts to gather this kind of data (everywhere worked and went to school for > 6 months) when they perform their checks. Based on historical experience, for those who have had multiple employments the information provided by the individual with regard to employment will likely not be accurate.PE suggests running a 7 year criminal history on all addresses that show up on the application or in the credit databases and then running a nationwide search to cover any other areas. An alternate to that may be fingerprint checks if utilities can be given access to the data.Either of these approaches will streamline the process.CIP-011-1 R3.1 (Cyber Security Training) - It appears that R3.1 was written with the intention of providing a level of training appropriate to job functions (language which was explicitly in previous versions) in regard to those with only unescorted physical access (such as janitors, electricians, HVAC technicians, etc); however the last bullet point 'Identification and reporting of a Cyber Security Incident' could easily be misinterpreted to be requiring training of a cyber nature rather than those of a physical nature directed against cyber assets (which I believe is the training we should be providing an individual with the aforementioned responsibilities)
12.21	Alberta Electric System Operator	Disagree	For R3.1, consider removing "and storage media" from bullet "The proper handling of BES Cyber Systems information and storage media" because information handling should be implemented regardless of the media type.For R4.1, consider changing the seven year time horizon, and make time horizon dependent on BES Cyber System impact level. For example, Low Impact could be seven years, Medium Impact five years, and High Impact

#	Organization	Yes or No	Question 12 Comment
			three years.
12.22	American Municipal Power	Disagree	I agree with the intent, but I feel there is some redundancy between requirements for training, awareness, risk assessment, etc. that should be addressed more concisely (less requirements)
12.23	GE Energy	Disagree	i) R3.2 lists a requirement for training on networking hardware for all users having electronic access. Perhaps this should only be for users with administrative access to network hardware. If this requirement is really calling out the need for VPN or similar training, this should be more specific than "network hardware".ii) Is it possible for vendors' personnel risk assessment process and records to be ratified/certified by NERC, so that individual Responsible Entities do not have to duplicate the effort for those vendors who have teams providing services to multiple REs? This would be more efficient and secure.iii) Vendor privacy issues are a concern regarding the background screens. Some clarity on the expectation between the client and vendor and the paperwork required to validate a screen, and clarity on who should actually conduct the screens would be helpful (client versus vendor). The expectation should be for the vendor to maintain their own records.
12.24	Public Service Enterprise Group companies	Disagree	In CIP v1~v3 the requirement for refresher training was "Annual", where "Annual" was understood to mean sometime within a calendar year. The new requirement of "once every 12 months from the date of initial training" implies that a daily checks are required for each person that had previously been training on whether training has expired. This imposes undue administrative overheard on Registered Entities without significantly enhancing cyber security. More flexibility is needed to accommodate vacations, illness, etc. One possibility is that training is required annually, with an up to 90 day extension for good cause or administrative efficiency.
12.25	National Grid	Disagree	In R2, National Grid recommends an annual reinforcement.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training"

#	Organization	Yes or No	Question 12 Comment
12.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
12.27	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.28	Minnesota Power	Disagree	Minnesota Power requests that the Standards Drafting Team consider replacing the phrase “provide all” with “make available to all,” in order to ensure clarity and avoid the potential that this phrase may be interpreted to include the requirement to document that the materials were actually received by all personnel. For example, it would be difficult to document that bulletin board postings were “provided” to each individual employee.Regarding Requirement R2, “...under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems” Minnesota Power has the following comments: o What security awareness program is being referenced? The Standard does not require the creation or implementation of a security awareness program. Minnesota Power recommends removing “under their security awareness program” from the Requirement. o What are “the cyber security practices that are essential?” The way this is stated infers that there is a known list of essential practices, which are particular to BES Cyber Systems (as opposed to general IT security practices), though none are referenced. Regarding Requirement R3, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to access being authorized as specified in CIP-011-1 Table R3 - Cyber Security Training. This training is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and

#	Organization	Yes or No	Question 12 Comment
			impact the reliability of the BES or emergency response." In addition, Minnesota Power has the following comments regarding Requirement R3: o R3 makes reference to a delegate for the senior management official, however R1 does not allow for the ability to assign a delegate for any purpose. o The box of definitions for R3 includes definitions for "routable protocol" and "non-routable protocol" however; these definitions are not used in R3 and therefore should be removed. o Sub-section 3.1 references a visitor control program which is not defined anywhere in this requirement. In light of the Standards Drafting Teams intentions to remove the "how-to" components of these Requirements, Minnesota Power recommends removing references such as this to a "program" and replacing with a statement such as "How visitor access is managed." o Regarding sub-sections 3.2, 3.3 and 3.4, as these sub-sections are currently written, it is not clear that this training is required for those individual's with a "need to know" only. o Regarding sub-section 3.2, what is the word "specified" in "specified electronic access" referring to? Minnesota Power recommends removing this term from the phrase as it doesn't add to the meaning of the sentence. o Regarding sub-section 3.2, "training on the networking hardware and software and other issues of electronic interconnectivity" is overly broad and could be interpreted as in-depth technical training, which would go beyond the intent of this Requirement. Minnesota Power recommends the following alternate wording, "training on the cyber security policies, access controls and procedures for the BES Cyber Systems to which they have electronic access." o For sub-sections 3.3 and 3.4, Minnesota Power recommends adding a comma following "...BES Cyber System recovery," for 3.3 and "...BES Cyber System incident response," for 3.4. o Regarding sub-section 3.5, the term "This" at the beginning of the sentence should be replaced with "Each" to be consistent with the other Requirements. o Minnesota Power recommends adding a statement to Requirement 3 that the training referenced in subsections 3.1 through 3.4 can be performed in a single training session or in multiple training sessions each covering one or more of the required topics. Regarding Requirement R4, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems,

#	Organization	Yes or No	Question 12 Comment
			including contractors and service vendors, have undergone a personnel risk assessment prior to access being granted as specified in CIP-011-1 Table R4 - Personnel Risk Assessment. The completion of this assessment is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and impact the reliability of the BES or emergency response. This is to ensure that personnel who have such access have been assessed for risk, subject to existing collective bargaining unit agreements, in accordance with federal, state, provincial, and local laws."In addition, Minnesota Power has the following comments regarding Requirement R4: o Regarding sub-section 4.1, the use of the phrase "personnel risk assessment program" seems inaccurate. Rather, 4.1 only defines what a personnel risk assessment itself shall, at a minimum, include. Minnesota Power recommends that the term "program" be removed from this sub-section as it's not required to demonstrate compliance. o The addition of "via photographic identification documentation issued by a government agency" to sub-section 4.1 could create an unnecessary burden on Registered Entities, especially for those vendors and contractors who do not come on-site. Minnesota Power recommends utilizing the language of the current CIP-004-2 Standard and requiring SSN verification for U.S. residents and photographic identification documentation for non-U.S. residents. o In the event that Standards Drafting Team chooses to leave the language of sub-section 4.1 as is, Minnesota Power recommends that photographic verification of identity be done at the time of initial access and that it is not necessary to renew this verification every 7 years. o Regarding sub-section 4.2, what does "document the results" mean? Under the current NERC CIP-002 - CIP-009 Standards there has been some confusion regarding what a Registered Entity needs to show compliance with this type of Requirement. Does this mean keep a redacted copy of the personnel risk assessment or would logging a summary of the results (e.g., "no findings"), including dates, source of background check, etc., be adequate? The Standards Drafting Team should consider clarifying what is meant by "document the results" so that consistency can be established.
12.29	NextEra Energy Corporate	Disagree	NextEra believes that the former standard provided valuable examples of awareness training methods which should be part of this revised standard. One question that arises

#	Organization	Yes or No	Question 12 Comment
	Compliance		is how will the delivery of this awareness training be measured? The standard should clarify the requirement. Also, the standard should provide examples of exceptional circumstances under which exception from training and PRA requirements may be documented.
12.30	Garland Power and Light	Disagree	o Disagree or need clarification with 3.1 - 1st bullet “The proper use of BES Cyber Systems” What does “use” mean - The EMS control system is operated by NERC certified operators and updated / maintained by qualified technical personnel. For CIP training, what is meant by train on the “use” of this system o Clarification on 3.2 should apply only to personnel having a role specific to support services for "networking hardware, and software and other issues of electronic interconnectivity supporting the operation and control of the BES cyber systems" and should be limited to security features. Training of all personnel in these areas will reduce cyber security.
12.31	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested revision:R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.32	Kansas City Power & Light	Disagree	Quarterly reinforcement is excessive and places an unnecessary administrative burden on Regional Entities and a poor investment of time and effort distracting from the productive work of maintaining cyber system security and integrity. Annual training is sufficient for the FERC Standards of Conduct, for important reliability functions in the EOP Standards such as black start and energy capacity emergencies, and for CIP sabotage recognition and reporting. Annual training for the personnel with access to identified cyber systems is sufficient to ensure the importance of maintaining the security and operation of identified cyber systems.R3.2 requires training that is much too detailed for personnel with access to a cyber system. Would this make sense for someone whose task was to wire in a Remote Terminal Unit for acquisition of field data into an EMS? The training specified in requirement R3.1 is sufficient for these kinds of

#	Organization	Yes or No	Question 12 Comment
			personnel. Recommend removal of R3.2.R3.5: Requiring annual cyber security training 12 months "from the date of initial training" is an unnecessary burden on the Regional Entity. It is enough provide for an annual training within a calendar year for those personnel who have physical and electronic access to cyber systems. What issue is this addressing? It is more important to focus investments of time, energy, and finances toward the actual security and integrity of the cyber systems than to support an administrative system to ensure training is done at a specific time rather than the training itself.R4.1 is too prescriptive in specifying the actions that are required to achieve the background check objectives. There may be other regulatory restrictions that prevent adherence to the prescription described here. Recommend removal of such prescription and include the language from CIP-004-2 that states to perform such checks "as permitted by law and subject to existing collective bargaining unit agreements".
12.33	Con Edison of New York	Disagree	Quarterly training is excessive for the large number of people likely to be involved. This training should be annual or at maximum twice a year. This training will get very expensive given the large number of people to be added to the training pool.
12.34	Dominion Resources Services, Inc.	Disagree	R2 - Based on the SDT's comments at the workshop, the intention of the Awareness program is not to require documentation of security awareness at an individual level. This interpretation is evidenced by the differentiation between the intent of security awareness versus the intent of security training. As defined in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program", awareness is not training. The purpose of awareness is to focus attention on security. Many of the techniques commonly used to deliver security awareness topics (e.g., posters) do not lend themselves to tracking at an individual level. On one hand, awareness topics are intended to allow individuals to recognize IT security concerns and respond accordingly and, on the other hand, training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus attention on an issue or set

#	Organization	Yes or No	Question 12 Comment
			of issues. Consequently, the SDT's intentions are correct and consistent with industry best practices. Given that the intent of this requirement is to reinforce cyber security program expectations for those personnel with access to BES Cyber Systems and not to document evidence of individual training, the following alternate wording is proposed: "Each Responsible Entity shall establish a security awareness program. The program shall provide for reinforcement, at least quarterly, on selected topics of security expectations and practices required to ensure the protection of BES Cyber Systems." 3.2 - Requirement R3.2 proposes training personnel who have electronic access to a BES Cyber System "on the networking hardware and software and other issues of electronic connectivity supporting the operation and control of BES Cyber Systems." Dominion recognizes that networking and network transport mechanisms (i.e., connectivity) involve specialized skills requiring a high level of expertise and experience. Because of the specialized nature of networking, providing this training would provide only a very limited security benefit at best, and could encourage personnel without the full qualifications and experience necessary, to take actions affecting network connectivity that would adversely impact the reliability of the BES. Based on Paragraph 434 of the Directives in FERC's Order No. 706, the Commission's intent was only that training programs encompass this training, not that any individual who has electronic access to a BES Cyber System receive such training. This requirement should be removed.3.5 - The change from annual to 12 months appeared to cause some confusion at the workshop and does not provide for a grace period (e.g., 12 months plus or minus a month to allow for shift workers and emergencies). Dominion requests that the SDT consider returning to using "Annual" and define how annual is to be used for these standards. Dominion prefers that "Annual" be defined as "12 months plus or minus a month" since this provides some flexibility in completing the task and also allows the Responsible Entity to not be forced into 11 month cycles so as not to miss a 12 month deadline. For example, Dominion had a training session set up for certain field personnel. The night before the meeting, a storm came through the system and caused enough damage that the meeting had to be cancelled because everyone was needed for restoration activities. The logistics involved in setting up these training sessions are often complex and a grace

#	Organization	Yes or No	Question 12 Comment
			period would provide the flexibility for rescheduling without compromising the spirit or intent of the training objective. Dominion understands that the "12 months plus or minus a month" definition is being used throughout the nuclear industry. Dominion suggests the following alternate wording for R3.5:"Initial training shall be conducted prior to granting access to BES Cyber Systems. Re-training shall be conducted annually."R3.5 contains requirements that are not identified in Table R3. All requirements should be contained within the associated table. Please see Dominion's response to Question 9. 4.1 - With inclusion of the nuclear plants, time horizons for personnel risk assessments are shorter than currently required by the standard. For example, Nuclear does background checks for unescorted access authorization every 5 years. Since they are done every 5 years, they do not check history for the last 7 years. To accommodate this difference, which effectively exceeds the requirements of this standard, it is recommended that the language in the 2nd bullet of R4.1 be revised to read:R4.1 o A criminal history records check initially and at least every 7 years thereafter, covering all locations where, during the time from the last check to the current time, the subject has resided . . .
12.35	Southwestern Power Administration	Disagree	R2 - Replace "shall provide" with "shall make available to" to clarify that the Responsible Entity must make quarterly awareness available, and not document that all personnel have reviewed and understand the awareness material.R3 & R4 - what would be an exceptional circumstance that would warrant training exception and/or investigative exception from the senior manager for personnel who are granted authorized electronic access and/or authorized unescorted physical access? If this is where the SDT is attempting to replace the previous "Exception to Policy" requirement, the placement of that language in R2 and R4 may need to be revisited, as these requirements seem to focus only on managing controls for personnel that DO have authorized access rights - not emergency personnel or non-authorized personnel access in emergency situations.R3.2 - This requirement is ambiguous in its inclusion of the phrase "other issues of electronic interconnectivity" A better approach would be to list the minimum coverage or topics to be covered. R3.5 - The requirement can be interpreted to read that everyone with authorized access will have to be trained exactly 12 months from his or

#	Organization	Yes or No	Question 12 Comment
			her initial training date. This would cause the responsible entity to be continually training and tracking staggered dates and creates an overly burdensome documentation effort, leading to the opportunity for mistakes and missed course deadlines. It is much more efficient and advantageous to do annual training in a group format. A better approach would be to state: "The Responsible Entity shall maintain documentation that such cyber security training is provided or offered once every 12 months, and documentation that personnel having authorized electronic access and/or authorized physical access to BES Cyber Systems have completed such training within 60 calendar days of such training being offered."
12.36	Ameren	Disagree	R2 - Without examples of what minimally constitutes reinforcement, this requirement will be problematic to audit. Would oral reinforcement count and how would you document that? Give examples such as posters, emails, events, or meetings would at least give an indication of the need to document evidence of the reinforcement taking place. A quarterly review seems extensive and an administrative burden. Once or twice per year should be sufficient.â€,â€,The bullets under R3.1 and R4.1 should be numbered as sub-requirements so that they can be cross referenced for audit purposes, i.e. R3.1.1 or R4.1.1 etc. Using the same numbering in the tables and in the requirements is confusing. The tables should use letters or roman numerals so they would not be confused with the sub-requirements indexing.
12.37	EEI	Disagree	R2 contains two very subjective words: "sound" and "essential." EEI suggests striking these words.For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.
12.38	Allegheny Energy Supply	Disagree	R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.

#	Organization	Yes or No	Question 12 Comment
12.39	Allegheny Power	Disagree	R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.
12.40	Constellation Power Source Generation	Disagree	R2 states quarterly reinforcement in sound security practices under their security awareness program. This may be training, but it does not have to be, as stated in the CIP V4 Workshop. However, this requirement as written does not seem to be auditable. How can an entity prove that an email/screensaver/poster/meeting meets the reinforcement stated in the requirement? Further clarity is needed, either within the requirement or in a guidance document.
12.41	Madison Gas and Electric Company	Disagree	R2, We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.Within R3 and R4 there is an exception of “except for program specified exceptional circumstances “ that is modified with the phrase “and impact the reliability of the BES or emergency response” (R3 only), please clarify. Is this exception giving the single senior manager the ability to wave cyber security training in the event that a non trained person is required to accomplish a task that they alone have the skill set for completion of said task (ie, a software engineer associated with the company that designed your SCADA system)?R3.1, The first bullet states “The proper use of BES Cyber Systems” and should be deleted since that is assumed as stated within the actual requirements of R3.1. The intent should be that training should be focused on protection of the BES Cyber System not how the particular BES Cyber System works, Please clarify.R3.2, The word “specified” is used and is not understood. Please clarify. If this is to mean additional training outside of the training within R3, than please “specify” that the entity shall have additional training program (module) for “specified” training that is not covered by R3. Please clarify if this is the required training differences between users and system administrators?The following requirements do not include a table of Low Impact, Medium Impact and High Impact (where the word “required” is

#	Organization	Yes or No	Question 12 Comment
			used under each column):R2R3.3R3.4R3.5R4.3Is this to indicate that all Entities must comply with these requirements whether or not they have BES Cyber Systems? Please clarify?
12.42	LCEC	Disagree	R2. The reliability benefit statement should not be included within the requirement section. This would be better positioned under the purpose section of the standard where it does not add confusion to the specific requirements that are being audited. The ISO27001 standards include an "objective" statement for each set of security controls which adds clarity and serves as a good best practice example.What is meant by reinforcement? How will this be demonstrated to an auditor?What is meant by sound security best practices? How will this be demonstrated to an auditor?R3 Remove or rewrite all content in the first paragraph after Table R3 - Cyber Security Training. The intent of this is unclear and very confusing.Split performance and program requirements into separate requirements for ease of auditing. If there is a requirement to have a program it should reside in its own requirement. Ref bullet 3 3.1Personnel with electronic access need to have an understanding of the risk associated with interconnectivity not necessarily the specific hardware involved. Personnel with the ability to change hardware configurations should have an understanding of hardware, software and interconnectivity impact.Training requirements should be tailored to user versus administrator and job based versus.The table should include the full range of requirements, like Table R5, and if not applicable should explicitly state that, not through blank cells. This leads entities to interpret that no training is required for these systems.4.2 in the table R4 should read unescorted physical access.
12.43	US Army Corps of Engineers, Omaha Distirc	Disagree	R2. meaning of quarterly reinforcement is vauge seems like it could be difficult to maintain audit records. 3.2 All users with electronic access do not need to know or understand networking hardware and software. Such information is usualy limited to those who support the network/system and have a need to know.
12.44	CWLP Electric Transmission, Distribution	Disagree	R2. Quarterly reinforcement training of cyber security practices seems excessive. This could be reduced to an annual obligation consistent with the training obligation in

#	Organization	Yes or No	Question 12 Comment
	and Operations Department		requirement 3.5. R3.2. This appears to require training on all systems connected to the BES, not just the specific system a user may require access to. A user accessing a server, PC or relay should not require training on network devices such as switches, routers, etc. This should be limited to requiring training on the specific area of the BES Cyber system the user is utilizing. R3.3. Similar to R3.2 this requirement should provide wording specifying that the training obligation is limited to the specific role the user has in regards to the Cyber System. R4. Requires a definition of “Electronic Access”.
12.45	Consultant	Disagree	R2. Suggest deleting the word "all" as redundant.R2. Suggest deleting the words "practices under their security awareness program". The requirement should be for dissemination of security information, not to create a program.R2. Change the words "that are essential to" to "associated with". Essential is a subjective term.R2 - R3 This is an example of where the insertion of 'local definitions' makes reading the requirement text difficult. Also, "For the purpose of this standard" is unnecessary and essentially not true. If the term is defined in the standard it is expected to be included in the next update to the NERC glossary, as that is how terms get in the glossary.General Comment- the term "and/or" is bad grammar. The word "or" is all that is necessary.R3 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R3.R3 - This is three requirements and an objective statement stuffed into one convoluted sentence.R3[-1] shall ensure personnel complete training prior to be being granted access as required in the Table.R3[-2] personnel under this requirement includes employees, contractors, and service vendors.R3[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without completed training.R3[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.-- Suggest rewriting as individual requirements for better clarity.R3.2 Suggest deleting "specified" as an unnecessary word.R3.2 Suggest deleting "any" as it is not consistent with the requirements in Table R3. Training is not required for "any" access, only for those systems identified.R3.2 Suggest specifying the training is for the security aspects of "networking hardware and software and other issues of electronic interconnectivity" not training on installation,

#	Organization	Yes or No	Question 12 Comment
			programming, or other aspects of these components.R4 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R4.R4 - This is three requirements and an objective statement stuffed into one convoluted sentence.R4[-1] shall ensure a personnel risk assessment is performed prior to be being granted access as required in the Table.R4[-2] personnel under this requirement includes employees, contractors, and service vendors.R4[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without a completed personnel risk assessment.R4[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Suggest rewriting as individual requirements for better clarity.R4 - "assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." The personnel risk assessment is not performed in accordance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements". It is performed in accordance with the Registered Entitie's policies and procedures, and should be in compliance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." Suggest modifying the wording of to clarify.Wording between R3 and R4 is inconsistent. R3 - completed security training & R4 - personnel risk assessment is performed. Suggest consistent wording as completed security training & completed personnel risk assessment. R4.1 suggest deleting the word "program" as unnecessary. It is the personnel risk assessment that has the specified identity check & background checkLogically, the topic in R3 should precede R2. It would seem to make more sense to grant access prior to providing security awareness on that access.Likewise, the topic R3.4 should precede R3.3. It would seem to make more sense to respond to an incident prior to recovery from an incident.Clarify annual for review of the policies, and for training. Suggest using the regulatory basis of over 30 years from the nuclear industry in dealing with periodicity for defining these periodic timelines. Should probably be a definition in both new standards to relate to periodic requirements.

#	Organization	Yes or No	Question 12 Comment
12.46	Western Area Power Administration	Disagree	R2: Please clarify whether "all personnel" includes "contractors and service vendors".R2: Please clarify what is meant by "reinforcement" required quarterly.R2: Needs some language clarifying intent. Does authorized electronic access = unescorted physical access? If so, this has major ramifications for support.R3: Requires the Responsible Entity to ensure that contractors and service vendors complete cyber security training - it does not specify that they must complete OUR training, just that they can provide proof of training that includes the specifics of R3.1. Is this the correct intent?R3.2: This requirement is too vague. What training on networking hardware and software are required? Is the intent to have training on the various forms of electronic access (VPN, dial-up, direct connection to equipment with a laptop or other diagnostic tool, etc.)? Is it directed at users like dispatchers who connect to the system via a console or workstation? All of the above? Each category of electronic access would have different training requirements.R3.3: Does this requirement specifically relate to disaster recovery/COOP/Business Resumption Plan? Would it also include training for field staff doing repairs on specific systems? Will we have to document all of the training they receive, including training on the maintenance and repair of all substation electronic equipment?R4: What is the definition of “program specified exceptional circumstances”? R4.1: Why are we changing to photographic versus finger printing? Photographic is easily fooled.R4.1: Would an entity be responsible for maintaining the results of a 7 year criminal check for outside entities having physical access (foreign utility workers, vendors, contractors, etc.)? If the other entity is also a NERC defined CIP applicable entity, is verification by that entity that the employee is properly vetted satisfactory? This is sensitive information that other entities may not be able to divulge due to local, state or national laws.
12.47	Southwest Power Pool Regional Entity	Disagree	R3 and its included requirements should be clarified to require training appropriate to the roles and responsibilities of the recipients. It is likely inappropriate to train a janitor or security guard with physical-only access on the proper use of BES Cyber Systems the same way a person with electronic access would be trained. Similarly, it is likely unnecessary to train a vendor support staff with only remote electronic access on the

#	Organization	Yes or No	Question 12 Comment
			physical access controls and visitor control program. 3.2 requires training for personnel having "specified" electronic access. What is "specified" electronic access? Additionally, it is likely not appropriate to train a dispatcher/operator on networking hardware, software, and connectivity issues, although they have electronic access. Greater granularity or assignment of responsibilities to roles may be necessary. 3.5: is the 12-month requirement a hard 12 months? Or is there some grace period permitted, such as +/- one month, to avoid calendar creep? And, does the 12-month timer reset with the completion of the latest training received or is the expectation that the training is actually performed approximately the same time every year regardless of any training that might be completed at a different time of the year? Additionally, rather than specifying the "date of training" shall be documented, consider using language similar to "[t]he responsible entity shall maintain documentation demonstrating that the required cyber security training is completed at least once every 12 months." Let the entity determine what is necessary to demonstrate compliance. R3 Overall, consider requiring a minimum expectation as to the quality of training. For example, should there be some sort of post-training assessment to determine if the recipient understands the course material? 4.3: Consider clarifying the requirement to "...update each personnel risk assessment within seven years of the previous personnel risk assessment" and make it clear that in this instance the requirement is from the actual date of the previous personnel risk assessment, not "in the same calendar year" or "+ / - some grace period."
12.48	The United Illuminating Co	Disagree	R3. Introduction is a run-on sentence with clauses nested within it. It is unduly confusing. I would reword for the SDT, but I can not understand the clausa relationships.R3.1 to R 3.4: There are employees who will require training in 3.1 thru 3.4. This amount of training could cover multiple days separated by periods of time. The requirement does not allow for General training on one day, Vyber incident response with the response team on another day, and training in backup restoration with a third team on a different day. R3.2: What specified electronic access triggers this requirement? Electronic access is not synonymous with remote electronic access, so what is being directed with this requirement. A user with a password does not require these topics. R 3.5 annual training from the initial date of training is too restrictive.

#	Organization	Yes or No	Question 12 Comment
			Union workforces are trained in groups and training schedules shift from year to year. Also a new union higher may receive an initial one-on-one training session and then be synchronized with the rest of the workforce by repeating the training in under 12 months.Suggest “once every 12 months from the date of the initial training, or the last completed training date” This will allow flexibility to reset the training date without going over the 12 months between training classes.Also request the SDT consider allowing a two month grace period in the requirement. UI suggests including a requirement for venors/contractors who provide support via remote access only (EMS/SCADA vendors). These vendors do not require training in physical access control procedures, or visitor control processes. Additionally, they often service multiple organizations and should not be required to view the same cyber security program as the BES cyner system owner employees. The suggested wording is:”For personnel requiring electronic access only training shall include at a minimum:- The proper use of BES Cyber Systems o The proper handling of BES Cyber Systems information o Identification and reporting of a Cyber Security Incident
12.49	Black Hills Corporation	Disagree	R3.1 & R3.2 does not allow for role-based training. Need to have unique numbering between sub-requirement and table references. (There should only be one 3.1 in R3)
12.50	Detroit Edison	Disagree	R3.2 requires “training on the networking hardware and software and other issues of electronic interconnectivity”. Training system operators on network gear is beyond the scope of their job duties. At the Dallas workshop, the drafting team stated that this training was required by FERC order 706 paragraph 434. That paragraph also says “we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee’s duties, functions, experience, or access level”. We don’t believe that FERC is requesting all personnel be trained on network gear, only that the training is appropriate to the person’s job functions. System administrators and network engineers would need to have training on the network, operations personnel do not.R3.2 also requires training prior to access of any BES Cyber System which is inconsistent with table entry 3.1 which does not require training for Low Impact or Medium Impact with routable connectivity.R3.5 removes the

#	Organization	Yes or No	Question 12 Comment
			term “annual” that was used in CIP-004 and replaces it with once every 12 months. This is too restrictive. Consider an entity that has a window for training in the month of May. Requiring every 12 months would cause the calendar to creep earlier in the year so eventually the training would be moved to April. We prefer “at least once per calendar year, not to exceed 14 months between instances”. The identity verification via photographic identification required in R4.1 is too prescriptive. The standard should be the “what” not the “how”. Previous versions of CIP-004 required an identity verification with the example of SSN verification. Consider changing the first bullet to “Identity verification (e.g., Social Security Number verification in the U.S. or via photographic identification documentation issued by a government agency i.e. Federal, State or Provincial)”.Table 4.2 should only require a PRA for unescorted physical access.
12.51	SCE&G	Disagree	R3.5 12 months should be changed to annually to allow entities to utilize a "calendar year" to setup training pools to conduct the necessary CIP training. Otherwise provisions should be made to allow initial training to be conducted during the implementation period of the standard.R4 SDT should consider allowing entities to leverage PRA controls in place (i.e. Nuclear PRA process)SDT should develop requirements for entities to validate a vendor's/contractor's PRA process. This would impose the burden of conducting the administrative work for the PRAs on the contractors/vendors, while still maintaining the compliance burden with the entity.
12.52	Powersouth Energy Cooperative	Disagree	R3.5 Suggest additional consideration be given to the requirement “every 12 months from the date of initial training.” Suggest the following wording: “no later than the end of the calendar month that the 12 month anniversary of the individual’s initial or previous training falls in” or similar to extend the window to a reasonable time to allow training to be done in a schedule fashion to allow some leeway for unanticipated delays that could previously lead to non-compliance due to a hard deadline. R4. Request additional language be added to clarify the allowance of reciprocity of PRA’s between a contractor or vendor and the responsible entity. It is understood that PRA’s are an important component of proper security but due to the volume of contractors and vendors used at any given time, a mechanism for the third party to perform their own

#	Organization	Yes or No	Question 12 Comment
			PRA and provide assurance that the PRA meets the requirements of the registered entity in both substance and time requirements will reduce cost and complexity greatly.
12.53	American Electric Power	Disagree	R3: In regards to "are approved by the single senior management official identified in Requirement R1 or their delegate and...", does this statement add any benefit to security? Is a senior manager or delegate's approval needed each time an emergency situation is declared?3.2, 3.3, 3.4: This is an attempt at role based training. Would it be better to combine 3.2, 3.3, and 3.4 together into a single requirement? Suggested wording: "The cyber security training must be role based for personnel that are users, administrators, responsible for system recovery, and responsible for responding to or investigating cyber security incidents of BES Cyber Systems."3.5: Regarding "conducted at least once every 12 months from the date of initial training", will this result in a date backup? Does an entity need to keep the initial date of training for all users? Does it seem feasible to still have the initial training records 20 years down the road?If training is completed on 6/30/2011, would it need to be completed before 6/30/2012? If it was then completed on 4/15/2012 would the next date of training be before 6/30/2013 or before 4/15/2013?Suggested wording: "at least once every 12 months from the last completed training date".
12.54	ISO New England Inc	Disagree	Recommend rephrasing R3 so that is clear that the Entity does not need to list all potential emergency responseTraining should be on policy, procedures, standards, and process and how to conduct oneself. Training should not be on networking,hardware,software. Companies have personnel that have the background in each function that are subject matter experts. That is there job and should not need to be trained each year on it since that's what they do every day. For R3 there is a sub requirement 3.2 and then another requirement in table 3 numbered 3.2 this can confusing.R3.2 in table 3 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?For R4 there is a sub requirement 4.2 and then another requirement in table 4 numbered 4.2 this can confusing.R4.2 in table 4 please defined what is meant by external connectivity. External to BES Cyber

#	Organization	Yes or No	Question 12 Comment
			System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next. This should be done to all the section that have 12 months. Scenario...In 2010, we roll out the training on June 1.Person A, who has access to CCAs, completes the training on June 15. In 2011, we roll the training out again on June 1.Person A, who has access to CCAs, completes the training on June 25. Under the new language, it could be interpreted that Person A has been out of compliance for 10 days if access was not revoked.The following are items we have in our training today, that will become requirements under the new standard: o Visitor control program (R3.3.1) o Identification and reporting of a Cyber Security Incident required(R3.3.1) o Recovery - note, this was required, but the language is more specific here (R3.3.3)The following are new requirements that will impact the training programs: o Training on networking hardware and software and other issues of electronic interconnectivity (R3.3.2) o BES Cyber System incident response action plans and procedures (R3.3.4)
12.55	Hydro One	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.We were wondering if the intent of R3.2 is to prevent access to a launch point for a multi location attack. (i.e. why limit the physical access to only sites with external connectivity?)
12.56	Northeast Power Coordinating Council	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training".

#	Organization	Yes or No	Question 12 Comment
12.57	ERCOT ISO	Disagree	Recommend the following be more clearly stated as an exception: “except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response”. R3.1: Consider: This cyber security training shall cover these requirements as well as policies, access controls, and procedures developed for the BES Cyber Systems, and include, at a minimum, the following required items: R3.2. Please clarify the intent of “training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems”. Examples of curriculum would help. R3.5. The requirement does not address retaining records of completion of initial training. R4: Recommend that “except for program specified exceptional circumstances that impact the reliability of the BES or emergency response” be addressed more clearly as an exception.R4.2. Consider: “Each Responsible Entity shall document the results and review of each personnel risk assessment.”
12.58	ReliabilityFirst Staff	Disagree	ReliabilityFirst is not clear on the meaning of the phrase “. . . except for program specified exceptional circumstances that are approved by the single senior management official. . .” If this is intended to cover the language of CIP-003 Requirement R1.1 referring to, “. . . including provision for emergency situations.” we believe the proposed language needs more clarity. In Requirement R3.1, the use of the word “specified” is unclear as to the intent of this requirement. We believe the drafting team should add language to clearly express the intent of this requirement and, more importantly, the intent of the word “specified”. Regarding Requirement R3.5, please provide guidance on the phrase, “once every 12 months”. For example, if an individual is trained on December 1st one year, can the individual receive the training on December 12th the following year and still be in compliance? Regarding R2, there is no documentation of implementation required, making auditing of the requirement impossible. A requirement to document the quarterly reinforcement is needed. Also regarding R2, a “security awareness program” is mentioned, but not required here or elsewhere and should be added.

#	Organization	Yes or No	Question 12 Comment
12.59	Constellation Energy Control and Dispatch, LLC	Disagree	Remove the phrase "sound security practices" or identify and define what the phrase means, i.e. sound security practices as defined in the cyber security policies.
12.60	BGE	Disagree	Remove the verbiage “sound security practices” or identify and define what this means.
12.61	US Bureau of Reclamation	Disagree	Requirement 2: Agree, but requirement should emphasize Program first then quarterly awareness refreshers.Requirement 3: AgreeRequirement 3.1: Agree, but revise "at a minimum" to "in addition" in the introductory statement.Requirement 3.2: Disagree. The requirement for network training should not be applied to everyone with logical (electronic) access, only to those who administer network and/or system administration. As written, this requirement could be taken to apply to operations staff (operators) with access to operations consoles. They do not need network training. Further, what is "specified network access." Requirement 3.3: Agree. Role-based training is probably a good idea, but this might be handled with a general statement.Requirement 3.4: Agree, see above.Requirement 3.5: Agree, but there should be some tolerance so that there is no date creep.Requirement 3 (in Table): The requirements R3 and R4 include tables which are in themselves requirements. Since the numbering system is the same as other requirements, this could result in confusion with what the actual requirements are. It is suggested that Tables R3 and R4 be clarified.Requirement 4: This requirement needs to be simplified. It is wordy and confusing.Requirement 4.1: The requirement should not limit identification processes to photographic means. Fingerprints are and should be acceptable. Further, the criminal check requirement, with local information, is beyond what can normally be addressed. Suggest this check be limited to a national level only. The risk assessment process needs to specify that an adjudication process needs to be completed.Requirements 4.2 and 4.3: Agree.
12.62	Network & Security Technologies Inc	Disagree	Requirement 3.2 (training on networking hardware and software), as written, seems to require that ALL personnel with electronic access to BES Cyber Systems receive such training. This frankly makes no sense. Will SCADA/EMS operators be expected to understand the intricacies of Cisco IOS? Furthermore, it violates the principal of “need to

#	Organization	Yes or No	Question 12 Comment
			know." Suggest this requirement be reworded in a manner that makes it similar to 3.3 and 3.4 and limits its scope to personnel responsible for hardware and software.
12.63	Oncor Electric Delivery LLC	Disagree	Requirement 3.2 is not appropriately worded. Most users with electronic access to our Cyber Systems have no need to know anything about the networking hardware, software, or interconnectivity issues. The personnel responsible for maintaining this equipment may need additional training but most have required skill sets as specified by their job descriptions.Requirement R4.2 uses the term "results" of a Personnel Risk Assessment. Different auditors may interpret this term differently. We propose this to be a binary result, ie pass/fail and stated as such, for clarity.
12.64	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Requirement R2 has all BES Cyber System operators to have a security awareness program that will maintain cyber security practices. However Requirement R3, R5 and R6 exempt Low Impact BES Cyber Systems. How can an Entity begin a security awareness program where Initial training (R3) and physical security (R5 & R6) is not required? This is very confusing.
12.65	San Diego Gas and Electric Co.	Disagree	Requirements 3.2 - 3.4 in CIP-011-1 seem to imply that a Registered Entity must have a separate training program for these three subjects. Unless the requirement is intended to be that prescriptive, SDG&E recommends a single training requirement that addresses the requirements in R3.1 - 3.4. This will help make the training requirements more manageable.Attempting to split hairs between training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to unnecessarily increase risk exposure for a Registered Entity and complicates the process and controls needed to meet R3 and R4 of CIP-011-1.
12.66	Southern California Edison Company	Disagree	SCE requests clarification on the scope of R3.1. This requirement requires people listed on Table 5 (those with physical or electronic access to "high impact BES system[s]" to receive training on the "proper use of the BES cyber system". This requirement as currently written is unclear whether the training requirement only applies to people who work with affected systems, or whether the requirement more broadly applies to

#	Organization	Yes or No	Question 12 Comment
			everyone who is permitted unescorted physical access to a PSP. If it is the former, then SCE believes that would be the correct application of this rule. However, if it is the latter case, then persons who are granted unescorted physical access rights to a PSP, but who do not themselves operate these systems (for example, CIP-cleared security guards), would have to receive training on the "proper use" of the protected system. Such training should only be required of individuals who actually work with protected systems, and not to everyone who has unescorted physical access rights to a PSP.SCE also seeks clarification on Requirement R2. As written, R2 requires quarterly "reinforcement". The drafting team should clarify the distinction they imply by using the term "reinforcement" rather than "training" as used in R3. Finally, SCE ask for clarity on Requirement R3. As written, Requirement R3 seems to allow for exceptions in the training requirement. The drafting team should clarify why an "organizational infeasibility" is being allowed while a structured method to seek technical feasibility exceptions is being eliminated. Both conditions create a situation where strict compliance with the standard is impossible to implement.
12.67	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
12.68	Idaho Power Company	Disagree	Sub requirement 3.2 is too broad. Dispatcher/operating personnel who have electronic access via an EMS application would not need training on networking hardware and software but it would be appropriate for EMS support staff. Cyber security incident identification and reporting would be sufficient for Dispatch/Operations personnel.
12.69	APPA Task Force	Disagree	The APPA Task Force agrees with the changes proposed by MRO-NSRS to replace "provide all" with "make available to all." We also believe the term "reinforcement" is not a defined term and should be replaced with "awareness material." As stated in our response to question 11 above, it is important to reference the required policies under requirement R1.If the drafting team does not follow Objective format suggested in response to Question 10, the APPA Task Force recommends the following format:R2.

#	Organization	Yes or No	Question 12 Comment
			Objective:Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. R2. Requirement:Each Responsible Entity shall make available to all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly awareness material in sound security practices under their security awareness program. The security awareness program will be part of the policy developed under requirement R1.The APPA Task Force cautions the drafting team on using the terms "grant" and "authorize" interchangeably. The following is our recommended revision to R3 with the Objective removed from the requirement:R3. Objective:To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.R3. Requirement:Each Responsible Entity shall ensure all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for program specified exceptional circumstances that are approved authorized by the single senior management official identified in Requirement R1 or his/her delegateR4. Objective:To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being authorized access when called for in CIP-011-1 Table R4 - Personnel Risk Assessment, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response,
12.70	Indeck Energy Services, Inc	Disagree	The definition of Cyber System is so broad that these requirements are applied on a one size fits all basis. A control center computer system requires a different level of requirement than a substation RTU. This lends itself to differentiating the standards by function and/or functional entity. R3.2 applies IT networking requirements on the operator who logs in to use the functionality, without any ability to program it. The term

#	Organization	Yes or No	Question 12 Comment
			"specified electronic access" is overly broad.
12.71	Manitoba Hydro	Disagree	The meaning of "quarterly reinforcement" is unclear. Consider whether Requirement R3.5 should refer to "Each Responsible Entity", rather than "This Responsible Entity". Requirement R4 appears to be missing the explicit requirement that access would be prohibited based on the negative or poor results of a personnel risk assessment; it just speaks of a personnel risk assessment being required. The structure of Requirement R3 and Requirement R4 is confusing and needs to be corrected. As written, the Table CIP-011-1 R3 applies to each of the sub-requirements, which may not meet the intent of the requirement - how does Table 3 item 3.2 for physical access relate to Requirement 3.2 for electronic access? What does "specified" mean in Requirement 3.2? The duplicate use of the same numbering of the requirements and the table items is very confusing. The format of requirements together with the use of tables for R2 to R4 should be consistent with the rest of the proposed standard. Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore is not auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
12.72	WECC	Disagree	The new way these requirements are written is very confusing. Too many levels, sub-levels, bullets and tabled criteria. Please simplify. Consider replacing with a requirement for Training and Awareness program that addresses the criteria that the SDT feels is critical for security and reliable operation of BES Cyber Systems.Regarding the phrase, "all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors", consistent language should be used through the standards. It may be useful to create a term for this group of people, define it, and use it in place of this long phrase.The last half of the requirement sentence lacks clarity. It is difficult to understand what is being required. If the intent is to create an exception process for training, the text should be removed. Standards should not have exceptions written into

#	Organization	Yes or No	Question 12 Comment
			them; they should establish a high bar of excellence.(3.1) “Visitor control program” needs definition or explanation.(3.2) The training requirements in this sub requirement seem vague.(3.3) Regarding the reference to “Systems;” most controls apply at the device level, and therefore should be required at that level.(3.5) Time intervals need to be clearer and well defined.(Table R3) Why no training for low impact systems? Seems arbitrary.
12.73	Bonneville Power Administration	Disagree	The objectives of these requirements (“to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems,” “to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems,” and “to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.R3: Exception is somewhat confusing. In particular, is "or emergency response" an alternative to "...are approved by..."? In other words, it could be read that exceptional circumstances require either approval or an emergency. However, it could also be that the "or emergency response" is an alternative to "impact the reliability..." It appears that the former is more likely, but the reader should not have to parse the sentence to get there. Some selected bulleting would help.Suggested rewrite of R3:Recommended Changes - Objective 3 - To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems. R3. The Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, have completed cyber security training prior to their being granted authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for - Program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the

#	Organization	Yes or No	Question 12 Comment
			reliability of the BES, or - Emergency responseThis assumes the first interpretation of "or"3.1 is acceptable3.2 Needs clarification, as it is not clear what the intent is. In a non control center environment, persons who have electronic access to BES Cyber Systems often do not have nor require knowledge or training in networking hardware and software. They make electronic connections and use their electronic access to collect electrical system information such as fault data, monitor device functions or do electrical systems analysis. It is not their job to understand networking.R3.3 and R3.4 are acceptable.R3.5 requires that training be conducted, but does not specifically require that every individual complete it. Also, it addresses the first annual training, but doesn't clearly stated what to do afterwards. The intent seems to be that each person complete training within each year. In other words, if the initial training was on July 1 2010, then training would be needed sometime in 2011 (say September), some time in 2012 (January?) and so forth. As currently written, a separate 12-month clock would be needed for each person. Finally, it's not clear if the required documentation is for the initial training, the annual training, or both. The SDT should be very specific as to what it means for how frequently an individual must take cyber security training. Suggested rewrite: Rewrite 3.5 to address annual training only: "This Responsible Entity shall ensure that all such persons receive annual training at least once each calendar year, starting the calendar year after they are granted access. The Responsible Entity shall remove authorized access from any individual who fails to complete such training in a timely manner." This removes some flexibility from the entities, but produces an unambiguous and manageable annual training program.We believe that a new requirement, 3.6, is needed to address documentation: "This Responsible Entity shall maintain documentation of any cyber training addressed in R3 or its subrequirements, includinge the date the individual's training in completed."Header in Table R3: Doesn't address annual training: Suggest "Cyber Security Training is Required Prior to Obtaining and For Continued:"R4: Has the same issue with the intent of "or emergency response" that R3 has. We suggest the same solution.The way that R 3.5 is written, it appears that two things must be done: the Responsible Entity must maintain documentation and each individual who is required to take cyber security training must take it as specified.

#	Organization	Yes or No	Question 12 Comment
			Would a violation of R 3.5 be due to an organization not maintaining documentation or due to an individual not having taken the required cyber security training in a timely manner? Or could there be two violations of R 3.5 - one for an organization not having up-to-date documentation and one (or many) for an individual(s) not having taken the required cyber security training in a timely manner? There is no indication in R 3.5 what should happen if an individual does not take the cyber security training as and when required. Should that individual's electronic access and/or unescorted physical access be revoked until the cyber security training has been completed? Or is what is important here only that the documentation be maintained regardless of whether each individual takes the cyber security training as and when required?For large organizations with a thousand or more people that must take cyber security training, is it possible that R 3.5 could indicate those organizations can provide the cyber security training during specific times of the year (say within a 3-month window) without regard for each individual having to take the training at a specific time? In this case, there would be no violation in an individual did not take the training exactly 12 months apart (or whatever the time requirement is) if the individual took the training within the 3-month window in each of two years.
12.74	Exelon Corporation	Disagree	The quarterly reinforcement requirement as spelled out in CIP-004 R1 Versions 1 through 3 is more specific and should be continued into this version. Requirement 3.2 as currently stated could cause someone such as a control room operator using an EMS system to be required to receive training on networking hardware and software for which they have no business need to know. It also could impact job specific training that is focused on improving reliable operations, due to the loss of precious training time being used for training that is not required for their position. We would suggest including wording such as "....appropriate to personnel roles and responsibilities"Requirement 4.1 second bullet states that "a seven year criminal history check" be performed. It is not clear from the requirement as to what agencies would need to be contacted to accomplish such a check. If local Police agencies are envisioned to be part of this check, that does not seem to be a very practical approach. R4. The need to show a photo ID is unnecessary to ensure a valid Identity Verification. The methods currently used to cross

#	Organization	Yes or No	Question 12 Comment
			reference and verify identity are satisfactory. To now require photo identification provides no additional benefit but would make it extremely difficult for remote personnel since we would now need someone to personally view the original photographic document. This would eliminate the ability to electronically transmit the required information.
12.75	Duke Energy	Disagree	The reinforcement requirement in R2 is vague and is up for interpretation by auditors. The Responsible Entity should only have to prove that the reinforcement information is provided. Previously, various means to provide the information, including posters, etc. were acceptable. This should still be the case. If so, is should not be necessary to prove that all personnel read the poster. R2 is open to interpretation as to what kind of evidence is sufficient. Explicitly state that materials are sufficient. Explicitly state which levels of Impact apply to R2. Need clarification on the program exception in R3. Does this apply to electronic and physical access? Must every situation need to be accounted for in the program or may it be case-by-case? Also, Requirement R3 contains a run-on sentence that makes the requirement hard to understand. Please consider breaking this into 2 or more smaller sentences.Requirement R3.2: What is meant by "specified electronic access?" Also, the requirement is vague in that it can be interpreted that the user of a BES cyber system needs detailed networking hardware and software training, when this is not the case. The user typically needs to know that device A is connected to device B and needs to know how to use the software. Said user does not need to know that the network communication routes through a brand XYZ switch using Ethernet and that the software was written in C# and so on. Clarification needed for audits, etc.Requirement R3.3: This requirement also needs bounds. If Employee A has a role in the recovery of BES Cyber System 123 only, then Employee A needs training on action plans and procedures to cover only BES Cyber System 123.R3.4 seems to be incomplete.Requirement R3.5: Is there any grace period on the 12 months? If there were "exceptional circumstances" such as in R4? For example, what if Technician A was due for training in June and was called for emergency storm duty and missed the training as a result? For 4.1, who will keep track of photographic identification? What is BA/TOP doing for Areva evidence of photo IDs? Will we have to gather the photo ID every 7

#	Organization	Yes or No	Question 12 Comment
			years? Suggest changing 4.3 to only include the criminal history check.
12.76	Nuclear Energy Institute	Disagree	The use of the expression "authorized electronic access" should be clarified, in all requirements in this standard where used. The correct expression should be "authorized electronic administrative access." Users who have access but no authorization to perform administrative functions on a BES Cyber System Component are of greatly less concern than those individuals having administrative access. Performing, as required by R4.1 a seven year background check, on each individual with non-administrative access to a Component is inappropriate. The focus should be on individuals who would pose a direct challenge to the system's reliable operation. An alternate solution may be to define "authorized electronic access" in the "Definitions" section.
12.77	FirstEnergy Corporation	Disagree	Though role based training is appealing, this activity is difficult to manage and maintain. It becomes administratively difficult to develop, maintain and track different training programs. A better approach would be having training that is differentiated by access (e.g. logical vs. physical.)For R3.2 qualifications should be made for only those people responsible for supporting networking hardware and software. There is no valid reason to provide networking training to non-networking personnel.If 3.3 and for 3.4 remain: Replace '...having a role...' with '...responsible for...'. Training for recovery plans and incident response is fundamentally different than the general cyber security training and should not be rolled into a 'one size fits all' training requirement.More clarity is needed on identity verification, how often does it need to be checked, does a copy need to be retained.
12.78	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
12.79	We Energies	Disagree	We Energies agrees with EEI suggestion: R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.
12.80	GTC & GSOC	Disagree	We recommend removing the word "all" in R2 to ensure that you do not have to track

#	Organization	Yes or No	Question 12 Comment
			and document reinforcement for each and every individual. We also recommend that R3.2 “For personnel having specified electronic access to any BES Cyber System” be clarified to identify to what “specified” access this is intended to apply.We recommend R2 through R4 should distinguish between the different types of users and administrators that have different responsibilities and access and therefore need different levels of training.R4 needs to be revised to better reflect the limitations of performing background checks on persons who have resided even briefly in foreign countries.
12.81	Xcel Energy	Disagree	We think R2 should be clarified to note that wide-distribution information such as company newsletters or e-mails satisfy the quarterly reinforcement requirement and that tracking on an individual basis is not required.
12.82	MRO's NERC Standards Review Subcommittee	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.83	The Empire District Electric Company	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.84	Entergy	Disagree	Wording in R2 is very awkward. Language needs to be written more concisely to show that awareness modules simply need to be disseminated. Current language allows for misinterpretation. It could be assumed that evidence to prove that modules have not only been disseminated but have also been received by appropriate personnel is required. The language incorporated into R3 for emergency provisions is similar to that found in CIP-003-3, R1.1, but seems to be restrictive to only cyber security training and personnel risk assessments in R4. These emergency provisions (which should be approved by the Senior Manager or Delegate) should continue to be allowed for all

#	Organization	Yes or No	Question 12 Comment
			standards/requirements, if a potential impact to emergency response or the BES subsists. Efforts to add newly created topics to the cyber security training module should be minimal. R3.5 adds clarity by replacing the word "annual" with "every 12 months". CIP-011, R4 is largely unchanged from CIP-004-3, R3. Criteria for an acceptable personnel risk assessment appears to be more lenient and allows for identity verification via a government-issued photo ID, as opposed to the social security check that was required for v3. Language is a little unclear as to which types of government-issued IDs are permissible. Are government-issued IDs from different countries (Mexico, Iran, etc.) acceptable? Additional specificity is needed.
12.85	Verizon Business	Agree	For section 3.1, "Escort Management:" should be a required item for the Cyber Security Training. In paragraph R4, the first sentence should be revised to read as follows (bolded is added text): "Each Responsible Entity shall ensure a personal risk assessment is performed and reviewed and approved by the Responsible Entity for all personnel…." 4.1, First Bullet – This could refer to the requirements of U.S. Form "I-9" for verification to work in the U.S. By passing the requirements of I-9, one satisfies this CIP-011 requirement. In paragraph 4.2, the requirement should be amended to read (bold is added text): "Each Responsible Entity shall document the results of each personnel risk assessment and they shall document that the results were reviewed and accepted or rejected as an acceptable risk for the Responsible Entity.

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

Summary Consideration:

While some commenters indicated support for local definitions, most commenters suggested moving the definitions to the NERC Glossary instead. In response, the SDT has moved all definitions to the NERC Glossary and discontinued the use of local definitions.

Several commenters expressed the need to bring back the concept of an Electronic Security Perimeter, because otherwise, the definition of "external connectivity" makes it difficult to determine at what point in the communication path a device is external. The SDT generally agrees with these comments and has reintroduced the definition of an "Electronic Security Perimeter" as a collection of Electronic Access Points.

Several commenters made suggestions about the use of the term "routable." The suggestions provided include more examples of routable versus non-routable protocols and the use of the OSI seven-layer network model. Others noted the term "routable external connectivity" is used, but "routable protocol" is never used. In response, the SDT has only defined the term "**External Routable Connectivity**" as follows: *"The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol."*

Commenters expressed confusion about the term BES Cyber System and requested additional guidance. In response, the SDT has added considerably more detail about the Reliability Operating Services a BES Cyber System performs along with the types of assets considered as part of the BES Cyber System.

#	Organization	Yes or No	Question 13 Comment
13.1	WECC		This should be defined at the top of the standard, dislike the definition box in the middle of a requirement.The use of external connectivity and/or enabled routable protocols to differentiate between required and non-required controls should be reconsidered. In most cases, the controls are still necessary to protect against insider threats.
13.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 13 Comment
13.3	ReliabilityFirst Staff	Agree	Does the drafting team intend to include these terms in the NERC Glossary of Terms?
13.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	However, this does not come up until well into the Standard. It is not clear how programmable electronic devises having no external connectivity, routable protocol, or non-routable protocol are treated. How shall programmable devises be treated when the only connectivity is on site connection to a laptop computer?
13.5	Puget Sound Energy	Agree	Puget Sound Energy would like to note that, with the widespread use of Internet Protocol (IP) as the communication protocol for the majority of Cyber Systems on the planet, if the standard is trying to be more inclusive of routable protocols than just IP, it should give some examples of others. "Routable Protocols" is an extremely technical concept, when talking about routable protocols other than IP, which could greatly impact scope, reliability, response, and overall compliance. If the standard is being specific to IP, then it should clarify that. If the standard is referencing other routable protocols than IP, then it should give some examples. (Ex: Routable protocols include, but are not limited to, IP, DecNet, MPLS, etc...).
13.6	Kansas City Power & Light	Agree	Recommend moving these definitions with R6 where routable protocol is first referenced.
13.7	Emerson Process Management	Agree	The current draft standard does away with the perimeter concept. It becomes slightly difficult in defining "internal" and "external."
13.8	LCEC	Agree	The definitions sound good but I do not agree with the use of "Required for external connectivity only" within the tables as they do not make sense most of the time.
13.9	SCE&G	Agree	The proposed definintions should be added to the "definitions table" at the front of the standard, rather than just in the boxes throughout the standard.
13.10	Allegheny Power	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their

#	Organization	Yes or No	Question 13 Comment
			functionality/vulnerability.
13.11	EEI	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.Suggested modification for R3:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response."Suggest elimination of Table R3.Suggested modification for Requirement 3.2:"For personnel that have a role in maintaining networking hardware and software supporting a BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems" In general, the drafting team needs to account for a person's "need to know" within the training program.
13.12	Florida Municipal Power Agency	Agree	These definitions ought to be associated with the first requirement that uses the definitions. As it appears now, these definitions seem associated with R3 on training, which has nothing to do with these definitions.
13.13	Electricity Consumers Resource Council (ELCON)	Agree	We agree with the definitions but they should be applied to limit the applicability of all the requirements in the standard.
13.14	Cogeneration Association of California and Energy Producers & Users Coalition	Agree	We agree with the definitions; however, they should be applied to limit the applicability of all of the requirements in the standard.
13.15	We Energies	Agree	We Energies agrees with EEI comment: The proposed definitions are helpful, and should

#	Organization	Yes or No	Question 13 Comment
			be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.We Energies agrees with EEI: Suggested modification for R3:Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.We Energies agrees with EEI: Suggest elimination of Table R3.Suggested modification for Requirement 3.2:For personnel having electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
13.16	FirstEnergy Corporation	Agree	While in agreement with the definition of routable protocol, it does not provide enough clarity. Would like to see the definition expanded to include protocol encapsulation.
13.17	US Bureau of Reclamation	Agree	Yes, but the definitions appear in the wrong location within the Standard.
13.18	Independent Electricity System Operator	Disagree	- External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?
13.19	Consultant	Disagree	1. Suggest deleting the words "for the purpose of this standard". These words are unnecessary and obfuscate the term being defined. Once the standard is approved these terms should be added to the NERC glossary as part of the next update process for that document.2. The term being defined should be capitalized, as it is now a defined term.3. Suggest listing these definitions in a section of the standard, and deleting these text boxes. Locating them in these text boxes makes the requirements difficult to read.4. If the definitions have to be injected like this, it is not clear why these definitions are located here. Nothing in these requirements discusses the terms being defined.5.

#	Organization	Yes or No	Question 13 Comment
			Suggest deleting "is defined as" as unnecessary. Suggest the format below:External Connectivity - Data communication across the protected electronic boundary. (Addressed in R20.) This definition also relates to the definition of Electronic Access Point in R20.Routable Protocol - a communications protocol that contains a network address as well as a device address thereby allowing packets to be forwarded from a device on one network to a device on another network. Non-Routable Protocol - a communications protocol that contains only a device address and not a network address that not incorporate an addressing scheme for sending data from a device on one network to a device on another network.
13.20	NextEra Energy Corporate Compliance	Disagree	Although on the surface these definitions are straight forward, NextEra believes there is a need to make a transition from the previous requirements for access points. There is not a strong tie between the definition for external connectivity (routable or not) to the requirements in the following sections. For example, Is a serial connection to a BES Cyber considered an Access Point to be protected? The definitions and requirements for protection need to be consistently applied across different levels of impact.
13.21	Garland Power and Light	Disagree	Comment - TOP definition needs to reword as follows:For the purpose of this standard, external connectivity is defined as a data communication path from a BES Cyber System Component to a device external to the BES Cyber System.Suggest better routable and non-routable protocols definitions - give examples of routable and non-routable protocols ie. tcp/ip, netbios, ipx, appletalk,
13.22	Network & Security Technologies Inc	Disagree	Current proposed definition of “external connectivity” is basically circular and could be interpreted in a number of ways. As written, it could even be applied to situations where two discrete BES Cyber Systems are connected to the same LAN segment, which we assume is not what the SDT intended. Suggestion: Unless the SDT really does intend for any network connection not entirely “within” a BES Cyber System to be considered “external,” rewrite the definition to provide a better point of reference than the BES Cyber System itself. Towards that end, the SDT might reconsider its decision to scrap the term, “Electronic Security Perimeter” (which, we note, still appears in CIP-011 in the

#	Organization	Yes or No	Question 13 Comment
			language of R20). We believe that in the context of current CIP Standard CIP-005, "external" connections are widely understood to be defined relative to the logical boundary of an ESP.
13.23	US Army Corps of Engineers, Omaha Distirc	Disagree	Definition of external connectivity is loose and problematic in the interplay with the loose definition of BES Cyber System. Does a communication path exist through a firewall? Does the term mean only intended paths?
13.24	Dominion Resources Services, Inc.	Disagree	Dominion has concerns about the definitions of external connection and electronic access point (Boundary Protection) as illustrated in the following example:A power station has 3 units with the same control system and a shared process I/O bus. Each unit has a control room with MMI, a dedicated server that is networked to the servers at the other 2 units, a front-end processor that is networked to multiple PLCs which are connected to smart I/O controllers. The servers are connected through a firewall to the central engineering office.Under this scenario, it is unclear where the BES Cyber System boundaries should be drawn. If the boundary is drawn around the station, everything is likely to be classified as High Impact and hundreds of I/O transmitters would be included that would normally be Low Impact. If an attempt is made to break the BES Cyber Systems down by unit, every interconnection between the units becomes an external connection and an electronic access point. Excluding a PLC from being part of the High Impact system is difficult because the PLC becomes the electronic access point and its data becomes an external connection. Boundary Protections with the PLC or its connection to the data bus cannot be met.The definition of a "communications path" needs to be clarified. Dominion proposes the following alternate wording to clarify the intent of the definition for external connectivity: ".....external connectivity is defined as any digital communication with a BES Cyber System component from a source external to the BES Cyber System."
13.25	E.ON U.S.	Disagree	E.ON U.S. believes that external connectivity should specify that it is going through an "access point" per the current definition of an access point. The definition of "external connectivity" references the existence of a "data communications path." Does this take

#	Organization	Yes or No	Question 13 Comment
			into consideration any protective measures that assist in the isolation or blocking of data communications? For instance, if a BES Cyber System or Component has a network connection, even an indirect one with multiple levels of firewalls and other security protective devices, to another "external" devices, does it have external connectivity? If so, virtually every system is externally connected; only those that are completely electronically/network-isolated would not be
13.26	USACE - Omaha Anchor	Disagree	External connectivity definition is incorrect. Would prefer a definition external to the facility or external to the electronic security perimeter (understanding that term doesn't exist in this standard.)
13.27	Black Hills Corporation	Disagree	External Connectivity is too open to interpretation; needs to distinguish between external and remote connectivity.
13.28	Luminant	Disagree	External connectivity should include any path and not just those that are considered part of the system functionality. Should also only include routable connectivity
13.29	Progress Energy (non-Nuclear)	Disagree	How are these terms applicable? Is this the key that will take many of our microprocessor relays in Transmission out of scope? If so, we need a clearer linkage to the definitions. It is still not clear if a non-routable protocol like VanCom is definitely excluded. If VanCom is not excluded as it was with previous standards, then every transmission RTU is pulled into consideration.Why have these definitions if the programmable electronic device definition is in play? Again is NERC's intent to manage at component, subsystem, or plant system level? Seems like impact would vary depending to what level of detail we need to get to.These terms are used very limited in CIP 11 and when used they are not used as individual terms. They are combined ie. "external routable connectivity".Do we have to use "routable protocols" term versus the ISO model...like layer 3 and greater?
13.30	Turlock Irrigation District	Disagree	In the definition of external connectivity the use of the words "data communications path" are confusing. Perhaps external connectivity could be defined as "Any electronic

#	Organization	Yes or No	Question 13 Comment
			access point that allows data to be transmitted and/or received between a defined BES Cyber System and a device that is not part of the defined BES Cyber System".
13.31	Southwest Power Pool Regional Entity	Disagree	It is unclear whether the definition of routable protocol includes Layer 2 devices in its scope, understanding that entities have had a difficult time distinguishing between a communications protocol and the networking infrastructure supporting the protocol's use. Additionally, given that the standard is now identifying BES Cyber Systems based upon the reliability functions they perform or support, is it even appropriate to continue to distinguish between routable and non-routable protocols? It is the function and the span of control of the Cyber Asset that determines the impact categorization and requirements applicability.
13.32	National Grid	Disagree	National Grid recommends changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary"
13.33	LADWP	Disagree	Needs brighter lines.
13.34	ISO New England Inc	Disagree	needs work - removable of ESP has implications. Needs better definition, use of routable protocol clouds issue. External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?Recommend changing from "from a device external to the BES Cyber System " to "from a device external to the BES Cyber System Boundary"
13.35	Dairyland Power Cooperative	Disagree	Once the identification of external connectivity is made, why is it relevant to distinguish routable vs. non-routable? A serial cable connected to an unprotected facility may be much more risky than a routable protocol with strict limitations on routing. There may be distinctions to be made in system or communication related requirements, but for training, the external connectivity criteria alone would be the best criteria for the impact level distinctions.

#	Organization	Yes or No	Question 13 Comment
13.36	Public Service Enterprise Group companies	Disagree	Please define the meaning of “routable external connectivity”. The terms “external connectivity”, “routable protocol”, and “non-routable protocol” were defined but not “routable external connectivity” is not. In particular, please clarify the language to provide that if an IP based protocol is in use for a BES Cyber System (e.g. at a substation) where the network address is not required and there is no “external connectivity” (i.e. the IP routing capabilities are disabled - there are no routers or devices capable of routing an IP datagram), this would result in the BES Cyber System being categorized as not having “routable external connectivity”.
13.37	Hydro One	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.38	Northeast Power Coordinating Council	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.39	Con Edison of New York	Disagree	Routable Protocol is defined as a communications protocol that contains a single address which identifies both the network and a unique device on that network.
13.40	San Diego Gas and Electric Co.	Disagree	SDG&E recommends rewording and clarifying the definitions of an External and Internal BES Cyber System and Remote Access. Connectivity is defined as “a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.” 1) What are the standard elements, configuration items, or technology implementations which would distinguish an internal and external BES Cyber System? For example, using this definition, Cyber System A could be on the same LAN as Cyber System B, but considered “external” because the “data communication path” exists (and is switched and not routed) between the 2 Cyber Systems, and 3) does a “data communication path” include serial, USB, Wireless, Channel Attached, or other data communication types of transport? We feel that the access concepts and Remote Access definitions are unclear and difficult to decipher.

#	Organization	Yes or No	Question 13 Comment
13.41	Northeast Utilities	Disagree	Suggest revising the local definition for external connectivity to add “boundary” so the definition would read “... from a device external to the BES Cyber System Boundary”.
13.42	Allegheny Energy Supply	Disagree	Suggest that the External Access definition be revised to include the concept that external access is communcations path access outside of the electronic and physical protection boundaries of BES Cyber System or its connected networks.
13.43	Duke Energy	Disagree	Suggest using these definitions in CIP-010. For generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the protected network rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.44	Alberta Electric System Operator	Disagree	The AESO would like to see the terms “network address” and “device address” further defined, to limit possible ambiguity. Consider taking frames (e.g. Ethernet or 802.3) into account in the definition, in addition to packets.
13.45	Southern Company	Disagree	The definition of external connectivity should make it clear that a data communication path does not include human action as an intermediate step.
13.46	Matrikon Inc.	Disagree	The definition of routable protocol should be congruent with the OSI networking stack <http://en.wikipedia.org/wiki/OSI_model>. Routable protocols are those which provide capabilities to communicate at OSI "Network" Layer 3.External connectivity definition still has room for interpretation. If we continue the approach of following the OSI model, then external connectivity is: a communication data "session" using a routable protocol, to an external network requiring OSI Layer 3 "router" or "access point"in order to communicate to an extended network.

#	Organization	Yes or No	Question 13 Comment
13.47	Entergy	Disagree	The definitions for routable and non-routable protocol appear to be satisfactory. However, the definition of external connectivity could prove troublesome, depending upon one's interpretation of a BES Cyber System. For example, a backup site may be classified as a different BES Cyber System than that of a primary site, thus making each one external from the other. Utilizing this interpretation could cause complications from an external connectivity perspective. Conversely, if both sites were classified as a single BES Cyber System, then the issue for external connectivity would not exist.
13.48	US Army Corps of Engineers	Disagree	The proposed definition states that external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System. Does the use of the word "existing" mean that the data communication path is permanent? If a plant allowed dial-up connectivity to their BES Cyber System, but would need to physically connect the modem for the outside person to dial-in everytime, and then disconnect the modem when completed, leaving an air-gap, would that count as "external connectivity" in this definition?
13.49	Indeck Energy Services, Inc	Disagree	The term “routable protocol” is used only once and the term “non-routable protocol” is never used except in the definition. “Routable connectivity” or “routable external connectivity” are used multiple times without definition.
13.50	Nuclear Energy Institute	Disagree	These definitions should appear in the “Definitions” section.Additionally, for generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.51	MidAmerican Energy Company	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal

#	Organization	Yes or No	Question 13 Comment
			and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.52	PacifiCorp	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the

#	Organization	Yes or No	Question 13 Comment
			endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.53	GTC & GSOC	Disagree	We recommend that local definitions for a specific Reliability Standard be documented in a section prior to the requirements sections instead of interspersed throughout the requirements. While it may improve the initial readability of the requirements, it is problematic in the long term determining if and where a particular word is defined.We also recommend "external connectivity" should be limited to situations where an external device can initiate a connection to the BES System Component. If a firewall limits connections to only those initiated by the BES System Component itself (i.e., connections are only one-way: out), the component should not be considered to have external connectivity.We recommend deleting the portion referring to network and device addresses because not all protocols make a clear distinction between a network address and a device address. The functional packet-related distinction is sufficient. The second and third paragraphs of the definition would read: "For the purpose of this standard, a routable protocol is defined as a communications protocol that allows packets to be forwarded from one network to another.For the purpose of this standard, non-routable protocol is defined as a communications protocol that does not incorporate an addressing scheme for sending data from one network to another."
13.54	Bonneville Power Administration	Disagree	We understand the need to keep definitions close to where they're used, it is also important to have them centrally located. We understand that this leads to a document maintenance issue. However, most document creation tools have solutions. For

#	Organization	Yes or No	Question 13 Comment
			instance, in Microsoft Wordâ„¢, you can make the definition a bookmark, and then insert a cross-reference somewhere else. The definition of "External Connectivity" is too broad. Consider an example: A user in a Control Center is logged into a workstation that is part of a BES Cyber System. The user opens a connection from that workstation to another BES Cyber System in the same Control Center. The communications path is totally under the control of the Responsible Entity, and all systems and communication paths involved are under the physical and electronic protections of the Control Center. Yet, this would constitute and external connection to the second BES Cyber System, and thus constitute remote access to that system. This is an untenable situation, especially considering the tight controls justifiably required for connections from outside the control of the Responsible Entity.Recommendation: "...defined as a data communications path to a BES Cyber System that encompasses, in some or all portions, links outside the control of the Responsible Entity." The definition of "Routable Protocol" is acceptable.The definition of "Non-routable Protocol" is slightly broader than necessary. It excludes point-to-point protocols. For instance, RS232 is one of many serial communications protocols that contains no address of any kind. Recommend changing "...that contains only a device address and not a network address." to "...that contains at most a device address and no network address."
13.55	Verizon Business	Disagree	1) The definition should explicitly state that a “Routable Protocol” includes TCP/IP. Also, the definition should explicitly state that MPLS is considered a “Routable Protocol” because MPLS is considered OSI Layer “2 ½” and hence there may be disagreement whether it is routable. For a “Non-Routable Protocol,” an example like a protocol in the OSI Layer 2 should be provided. 2) The term “external connectivity” requires more explanation. It is unclear whether it would include two BES Cyber Components that are connected to each other, regardless of the length of separation.

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R3 and R4 have moved to CIP-004-5 R1 through R3.

Several commenters expressed confusion regarding the purpose of specifying routable connectivity in the applicability for training requirements. The SDT agrees and has modified the applicability to include all High and Medium BES Cyber Systems.

In addition, several commenters suggested the training and personnel risk assessment should apply across all impact levels. One commenter suggested the training and personnel risk assessment should only apply to the High Impact level of BES Cyber Systems, and another commenter suggested there should also be a "no-impact" level. The SDT has changed the requirements for training and personnel risk assessments to apply to High and Medium Impact BES Cyber Systems. These requirements do not apply to Low Impact BES Cyber Systems because of the significant effort required to track the Low Impact BES Cyber Systems and the persons who have authorization to access those systems.

#	Organization	Yes or No	Question 14 Comment
14.1	US Army Corps of Engineers		In Tables R3 and R4, the phrase "Physical access to BES Cyber Systems" is qualified with the words "with routable external connectivity" but these words are not referenced in any of the paragraphs R2-R4. Paragraphs R2-R4 state physical access as "authorized unescorted physical access to BES Cyber Systems." Should we assume that both terms are the same?
14.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
14.3	Northeast Utilities	Agree	Please change Table R4 to read "Personnel Risk Assessment".
14.4	Madison Gas and Electric Company	Agree	Thank you for adding these helpful tables immediately after the requirement. This reduces the confusion of turning a page to an appendix.

#	Organization	Yes or No	Question 14 Comment
14.5	GTC & GSOC	Agree	We recommend making sure there is consistency with impact levels for authorizing physical and authorizing electronic access
14.6	Black Hills Corporation	Agree	Would like to know if an entity exceeded any NERC requirements as internal policy, and subsequently had an individual miss training who did not interact with a BES Cyber System, would this be considered a violation by NERC.
14.7	ERCOT ISO	Disagree	3.2 & 4.2: Please clarify why "with routable external connectivity" is addressed.
14.8	US Army Corps of Engineers, Omaha Distirc	Disagree	3.2 not clear as to purpose of this training or how external connectivity relates. Without electronic access the most they could do is damage hardware. Does this only apply to hardware providing external connectivity such as firewall etc?
14.9	Tenaska	Disagree	5.3 Consider leaving the word "uniquely" out or change it to say individually identify.
14.10	BCTC	Disagree	Â We are in strong disagreement with R3.2. We have various parties who have electronic access to our BES Cyber Systems but do not agree that training these individuals on networking hardware and connectivity would increase the security of the BES. Could you please clarify the objective of this requirement? - i.e. why would someone who simply accesses a console to view BES Cyber System data require network-related training? We recommend that the requirement be worded something like "... personnel will be supplied training on applicable NERC CIP devices that they are authorized to work on and the associated related security controls, as identified in the CIP Standards..." Above we have recommended above that "emergency situation" language remain at the security policy level. A potential scenario in this requirement is an emergency occurs (i.e. a critical piece of equipment breaks) whereby the closest service provider available to fix the problem is minutes away but has not completed CIP training or a PRA; from an operations (i.e. "keeping the lights on") perspective we would identify this as an emergency situation, seek approval from our Senior Manager or delegate to allow this person to access our facility, and allow the repair to occur. In this scenario we are assuming our 'regular' service technicians are unavailable or far way

#	Organization	Yes or No	Question 14 Comment
			from the facility.Â We have encountered an issue where some non-North American countries will not disclose criminal histories so it will be difficult to meet the requirement that states ... “A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.” We can have new employees from these countries start employment but lived in North America for less than 7 years. For such a scenario we recommend that the language be revised to indicate that the Utility requests a seven year criminal history check on a best efforts basis; i.e. we can ask for the information but there is no guarantee the originating country will provide us with the results - this is beyond our control. FYI, simply denying a person on these grounds in Canada violates out employment legislation.Â R4.2 We currently retain a “clear”/ “not clear” result with all PRAs for contractors and employees. Please confirm that this requirement does not require the Utility to retain detailed records (i.e. listing of criminal offenses, charges, etc.)
14.11	Hydro One	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Suggest changing to annually for consistency.Such classification will add additional unnecessary burden since specific training will need to be generated and tracked depending on the type of system access
14.12	Northeast Power Coordinating Council	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Clarify “12 months”.
14.13	ISO New England Inc	Disagree	Agree provided the external connectivity definition is updated per answer #13 Table 4 title uses “personal” instead of personnel.
14.14	San Diego Gas and Electric	Disagree	Attempting to split hairs between PRA and Training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to

#	Organization	Yes or No	Question 14 Comment
	Co.		unnecessarily increase risk exposure for an Entity and complicates the process and controls needed to meet R3 and 4 of CIP-011-1. SDG&E recommends that the requirements for both of these tables be required for High Impact BES Cyber Systems only
14.15	E.ON U.S.	Disagree	CIP-011, R3 states that contractors and service vendors with authorized electronic or unescorted physical access are to complete cyber security training before given this access. However, this begs the question of what constitutes satisfactory evidence of this training for these individuals? If vendor-provided training is adequate, what evidence is needed to maintain this training?a. (3.2) "...shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity..." For most users of these systems, training on the networking hardware and software provides little or no value. Unless these are systems administrators tasked with responsibilities for managing / monitoring these systems, users (and associated training) should be focused on the functions of the system to support operation, monitoring, and control for which they are responsible.CIP-011, R4 requires background checks for contractors and service vendors. The new requirements do not clarify the acceptable evidence required to be maintained by entities. Is it acceptable for a service provider to conduct the background checks? If so, what evidence of background checks does the registered entity need to maintain?Does the requirement apply for everyone that has access to the BES cyber system ? Would this include support personnel and janitorial staff? E.ON U.S. suggests that the requirement be tied to job function rather than a blanket requirement for all.E.ON U.S. requests clarification as to how personnel that only have remote access to the system should be verified. Photo IDs are neither practical nor required.
14.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
14.17	US Bureau of Reclamation	Disagree	Cyber access training and personnel risk assessment requirements should be applied to

#	Organization	Yes or No	Question 14 Comment
			all three impact levels.
14.18	BGE	Disagree	Define “electronic access” as noted in table R3 (3.1). 3.2 Should say “Physical access to BES Cyber Systems (remove routable external connectivity). Table R4 (4.2) should add “unescorted” physical access to BES.....
14.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. This requirement as currently drafted is unduly burdensome for field personnel that have local access to programmable electronic devices. These personnel need not be aware of network considerations to securely perform their job duties.
14.20	Luminant	Disagree	Does R4, 4.1 need to be modified to address valid identification for foreign nationals with remote (overseas) access to BES Cyber Systems?
14.21	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.If an entity is required to restrict physical access, then they should also be required to provide training.
14.22	The Empire District Electric Company	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external

#	Organization	Yes or No	Question 14 Comment
			connectivity only".If an entity is required to restrict physical access, then they should also be required to provide training.
14.23	Platte River Power Authority	Disagree	Is the intent that prior training is not required for Physical access to BES Cyber Systems without routable external connectivity? In other words, the table says that prior training is only required if Physical access is granted to a BES Cyber Systems with external connectivity. Is that the intent?
14.24	Entergy	Disagree	It appears nonsensical to require cyber security training and personnel risk assessments for electronic access to BES Cyber Systems classified as Medium-impact, but not for physical access to Systems with external connectivity. Requiring these items for only one type of access and not the other merely increases the likelihood of misinterpretation of the requirements by the Entity. PRAs and training should be required for both types of access or neither.
14.25	FirstEnergy Corporation	Disagree	It would be very difficult to administer training and PRAs based on impact levels. It seems like it would be easier to just have one level for all. We suggest eliminating the tables/impact levels for R3 and R4.Training and PRAs should be required for all levels. It is easier to maintain, track and move employees around if they are all trained and background checked, especially with the need to continuously reassign employees.
14.26	Manitoba Hydro	Disagree	Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore should not be auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
14.27	Progress Energy (non-Nuclear)	Disagree	May not be an issue since most our personnel that require access will very likely require access to all three impact levels and will require adherence to the highest security level anyway. It does not seem practical and reasonable to develop and maintain three different security programs based on the three impact levels.The question with most of

#	Organization	Yes or No	Question 14 Comment
			the impact level requirements is the difficulty and cost associated with developing and maintaining three different levels of security, monitoring and controls and making sure that the appropriate levels are applied with an increase in impact level.Again is NERC's intent to manage at component, subsystem, or plant system level? Impact will vary depending to what level of granularity we need to get to.Section R3.1 appropriately provides for a level of NERC CIP training consistent with physical only access. The last point 'Identification and reporting of a Cyber Security Incident' should be clarified to be the physical aspects of a cyber security incident. Since this is the type of training that we will be providing to janitors/HVAC repair technicians/electricians, there should not be a requirement to provide any type of cyber training. The full 'Identification and reporting of a Cyber Security Incident' can be included under R3.2 - which is intended for those with actual cyber access.
14.28	National Grid	Disagree	National Grid agrees provided the external connectivity definition is updated per answer 13.Recommend changing Table R4 from "personal" to "personnel".
14.29	LCEC	Disagree	No. These tables should include all standards and clearly indicate their intent.
14.30	American Municipal Power	Disagree	Please add a little or no impact category.
14.31	Puget Sound Energy	Disagree	Puget Sound Energy, as stated earlier in this document, would need to see more specific definition to "Low", "Medium", and "High" impact, as well more specific definition to subjective terms such as "restrict" and "affect". If specificity can be provided to the subjective areas of the definition to "Low Impact", "Medium Impact", "High Impact", "restrict control", and "affect situational awareness", Puget Sound Energy agrees with the tables.
14.32	ReliabilityFirst Staff	Disagree	Requirement R4.1; ReliabilityFirst is concerned that permitting documents other than Social Security Identification for identity verification could lead to questionable results. Requirement R4.3 only addresses updating a PRA every seven years but does not include

#	Organization	Yes or No	Question 14 Comment
			a requirement to update the PRA "for cause." Table R3 and R4, Medium Impact BES Cyber Systems should be required for rows 3.2 and 4.2 respectively.
14.33	Southwest Power Pool Regional Entity	Disagree	Some degree of physical and electronic access training is basic security training that should be applicable to all impact categories. The extent of the training could perhaps be adjusted to reflect the impact categorization. 4.2: See the discussion regarding the need for distinguishing between routable and non-routable protocols. The Personnel Risk Assessment should be required prior to access for at least High and Medium impact BES Cyber Systems, both physical and electronic, regardless of any communications protocol being used.
14.34	Network & Security Technologies Inc	Disagree	Suggest (1) dropping "routable external connectivity" qualifier for High Impact systems in 3.2 and 4.2 and adding Medium Impact systems to 3.2 and 4.2.
14.35	EEI	Disagree	Suggest elimination of Table R3. EEI suggests making training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Suggest elimination of Table R4. EEI suggests making personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.36	Emerson Process Management	Disagree	Table R3 implies that Cyber Security Training is not required for people who have physical access to a high impact BES Cyber System as long as this system does not have routable external connectivity.Per 3.1, the training shall cover the policies, access controls and procedures.This is unclear about the connection between the needed training and the lack of routable external connectivity.Same note applies to Tabe R4.
14.37	American Electric Power	Disagree	Table R3, 3.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized, unescorted physical access".Current

#	Organization	Yes or No	Question 14 Comment
			wording seems to require training for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need cyber security training?Table R4, 4.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized unescorted physical access"Current wording seems to require personnel risk assessment checks for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need personnel risk assessments?
14.38	Alberta Electric System Operator	Disagree	The AESO suggests that security training and PRA are required for all impact levels for 3.1, 3.2, 4.1, 4.2 in the tables. The SDT should consider devising a graduated implementation scheme, or let the RE determine how much and to what extent the training and PRA should include for each impact level.
14.39	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to require cyber security training in Table 3.1 and Table 3.2 for all impact levels. The training requirements for Table 3.1 and Table 3.2 Low Impact, should only be required to comply with R3 sub-requirement 3.1, at a frequency of every 2 years. These Low impact facilities should not be required to comply with the specific requirements detailed in R3, sub-requirements 3.2-3.5. We suggest the table state; “Applies to sub-requirement 3.1 only, Frequency: Every 2 years” for Low Impact facilities. We agree with the MRO-NSRS comments on item 3.2; MRO-NSRS proposes removing “with routable external connectivity.”The APPA Task Force feels there is confusion with blanks in the tables. For example, in Table 4.1 we have assumed that a blank under the Low Impact category means a Low Impact BES cyber system is not required to conduct any Personal Risk Assessments Prior to Obtaining Table 4.1 and 4.2 access. If this is the meaning of such blanks it is our recommendation that the drafting team make that clear and insert a N/A for Not Applicable in all blanks throughout the document and define N/A in the introduction.For R4 Table 4.2, the APPA Task Force agrees with the MRO-NSRS proposal to remove “with routable external connectivity”, and to add the following under Medium Impact: “Required for routable external connectivity only”.The APPA Task Force suggests the following text for the noted tables:R3 Table 3.1: Low Impact: Required (Applies to sub-requirement 3.1 only) at

#	Organization	Yes or No	Question 14 Comment
			least once every 24 monthsMedium Impact: RequiredHigh Impact: RequiredR3 Table 3.2: Low Impact: Required (Applies to sub-requirement 3.1 only) at least once every 24 monthsMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR4 Table 4.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR4 Table 4.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
14.40	Duke Energy	Disagree	The format in these tables is confusing. The requirements tell “what” the requirement is, and the table tells “who” the requirement applies to.
14.41	Con Edison of New York	Disagree	The R3 Dialog box defines external connectivity. It is not clear whether external activity is between systems in all cases, or does it mean between systems that are within different electronic boundaries. The wording needs to make this clear.The requirement to check photographic ID’s seem appropriate initially, or during the hiring process. As written it will require checking photo ID’s every seven years for an employee that has been working in for the Company for the entire period and whose identity should no longer be in question. The recurring requirement should not apply. R3.2 - it is unrealistic to expect to train operators on network equipment, software, and protocols, which is a separate and distinct job function.R3.3 - Review of DR procedures is appropriate, but specific training on DR is not
14.42	Consultant	Disagree	The 'required' blocks for electronic access would seem to imply that there is no connectivity between low impact assets and medium or high impact assets. If this is the case, then the table seems adequate. Or there should be a 'highest impact rules the network access controls' qualifying statement.The 'required' block for physical access would seem to imply that there is no co-located assets of different impact levels. This seems less likely than electronic access segregation. There should be a 'highest impact rules the physical boundary access controls' qualifying statement.
14.43	Idaho Power Company	Disagree	The table does not address training requirements for personnel with access to sensitive information about BES cyber systems but do not otherwise have electronic or physical

#	Organization	Yes or No	Question 14 Comment
			access to the system itself. It would be difficult to be compliant with R24 if personnel are not trained to recognize sensitive information or trained on the proper labeling and handling procedures.
14.44	Florida Municipal Power Agency	Disagree	The tables are ambiguous. For instance, is the blank in the table for R3 for Low Impact supposed to mean that no training is required, as FMPA interprets? FMPA believes that some level of training ought to be provided for all levels of impact, correlated with the impact level (e.g., biennially instead of annually for Low Impact for instance). FMPA suggests embedding the bullets into the table in a similar manner as R5 and leaving no blanks in the table to make clear what is required for each impact level.
14.45	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The tables should clearly specify unescorted physical access.
14.46	Constellation Energy Control and Dispatch, LLC	Disagree	-There should be a row in the R3/R4 tables for each Requirement/Sub-Requirement-Define "electronic access" in table R3 (3.1).-Table R4 (4.2) should say "unescorted" physical access to BES Cyber Systems with routable external connectivity.
14.47	Bonneville Power Administration	Disagree	Training and especially a PRA should be required for physical access to any High or Medium impact system, regardless of whether it has routable external connectivity. A hammer to a RAS system could cause severe issues, whether or not the system connects to field units with a routable protocol. In addition, physical access to BES Cyber Systems is potentially far more dangerous that Electronic Access (especially at field sites) The requirements in the table should be at least the same for physical and electronic access. In both Tables R3 and R4, the word “unescorted” should be added at the beginning of Items 3.2 and 4.2.
14.48	WECC	Disagree	Training should be done for all employees with any level of access to a minimum level. Additional criteria for training should be done dependent on the level of access and their

#	Organization	Yes or No	Question 14 Comment
			role. See previous comments about suggestion to replace with a requirement for a training and awareness program with specific criteria.These requirements should apply to all impact levels. Awareness, training, overall education, and personnel risk assessment are the building blocks for a successful security program.
14.49	We Energies	Disagree	We Energies agrees with EEI: Suggest elimination of Table R3. Make training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Suggest elimination of Table R4. Make personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.50	Minnesota Power	Disagree	While the impact levels seem reasonable, it is the inclusion of the term “external connectivity” as a qualifier in sections 3.2 and 4.2 of Tables 3 and 4 respectively that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that sections 3.2 and 4.2 of Tables 3 and 4 respectively simply state “Physical access to BES Cyber Systems.”

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many of the commenters expressed concerns with the timing of the revocation requirements as being unrealistic, especially for authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access. Commenters stated that the time required for revocation should be extended to 72 hours or to the next business day, whichever is longer, to allow for communications of this circumstance. Timing issues regarding the termination of access for contractors and/or service vendors were also raised.

The SDT has clarified that the timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform the assigned functions, that access should be revoked. Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services). CIP-004-5 Requirement 7 enumerates the proposed requirements under a variety of conditions regarding revocation of access.

Some commenters expressed confusion regarding the use and meaning of the terms “grant” and “authorize” and their use in these requirements. Also, the term “Physical Access Control Systems” was requested to be defined, as the term will likely have different meanings for different entities and auditors and could lead to difficulties in implementation and auditing. The SDT has provided additional clarity in the requirements and has proposed the following definition for **Physical Access Control Systems**: *“Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.”*

Physical security at remote substation sites was also raised as not being cost effective in preventing or detecting cyber attacks, especially for remote substations with only dial-up communications. Commenters indicated that physical security should only be required at Control Centers and High Impact substations with IP-based communications. While some commenters generally liked having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards, the commenters expressed concern that the clarity that was intended was not provided, as the language used is vague and confusing. Some restructuring of the requirements was suggested to improve the clarity of the standards.

While some restructuring of the requirements for physical security has been implemented by the SDT in the Version 5 standards, each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. CIP-006-5 defines the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the

emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

#	Organization	Yes or No	Question 15 Comment
15.1	National Rural Electric Cooperative Association (NRECA)		In R5.5, the statement to "Authorize unescorted physical access....." makes it sound like the utility should provide blanket authorization for unescorted physical access. I don't believe that is the case. Please clarify R5.5 -- I believe what is intended here is to have policies and procedures in place to detemine who has authorization to have unescorted physical acess.
15.2	Idaho Power Company		R6 is confusing. The headings suggest the need for a physical security plan but the tables pertain to requirements to protect physical access control systems. 6.1 should read "Restricting physical access to physical access control systems that are protecting BES Cyber systems identified in Requirement R5 Part 5.1, 5.2 5.3." 6.2 should read similarly. The current wording suggests that a physical access control system would be identified in Requirement 5 but it is not a BES cyber system because it does not perform a function listed in the attachment 1.
15.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.In R5 and R6, "prevent" is an objective (or purpose) and should not be embedded in the requirement, e.g., if unauthorized physical access occurs such as someone driving a bull-dozer through a building, is the entity non-compliant? Objectives should not be mixed with the actual requirement.In the bullets to R5 and R6, the areas in and of themselves do not "protect" BES Cyber Systems, they "contain" them.R5The requirement to "apply criteria" is not a strong requirement. FMPA suggests: "Each Responsible Entity shall apply the security controls specified in CIP-011-1 Table 5 - Physical Security for BSE Cyber Systems."In the bullets, there is confusion among the terms "grant" and "authorize". "Authorize" is senior manager approval, "grant" is being given the key or card. The requirements should keep these two concepts clear. For instance, in 5.5, "authorize" should be changed to something like: "Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized

#	Organization	Yes or No	Question 15 Comment
			such access". Also, in order for 5.8 and 5.9 to apply to Medium, then 5.5 needs to apply to Medium.5.7, 5.9 and 5.9 will be open to interpretation. If an employee was given key and card access, is revoking card access sufficient or both the key and the card?5.7 should apply to Medium5.8 and 5.9 should be combined and the time durations correlated with the impact level instead of Control Center vs. Facility.5.10 strike "access"R6The order of R5 and R6 seems backwards. It would seem development of the physical security plan (R6) should come before implementing the plan (R5)
15.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
15.5	Independent Electricity System Operator	Disagree	- R5.1 in table 5 please define what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?- 5.3 and 5.4 should be consistent in
15.6	Reliability & Compliance Group	Disagree	: Putting data retention into a separate section of the standard is confusing without a reference. If you want to keep data retention separate, you should refer to the data retention rules in the standard. i.e. Retention rules for R5 can be found in section 1.4.1 and 1.4.3 of this standard.Also, visitor control should be included for medium impact systems as well. If not, why are we restricting access to those systems if we can routinely open the door for anyone to come in and wander around unescorted. One interpretation of this would be to have some employees given access rights and others would be daily guests who are not logged or monitored.
15.7	Regulatory Compliance	Disagree	5.7 - qualification should be made in regards to a service vendor that the 24 hour period should start once notice is received from their company.5.8 - prefer 7 day revocation deadline5.9 - prefer 7 day revocation deadline
15.8	USACE - Omaha Anchor	Disagree	A) Dislike that methods to achieve compliance were removed from standard and will be placed in a guidance document. Guidance documents aren't binding. B) 5.9 - how do

#	Organization	Yes or No	Question 15 Comment
			you revoke access when it was never formally granted in the first place?
15.9	Duke Energy	Disagree	a) We generally like having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards. However, the clarity that was intended is not provided as the language is vague and confusing.b) The standard has eliminated terms like the Physical Security Perimeter, 6 wall boundary and Physical Security Plan but it appears that they will be expected in order to achieve compliance. In fact, R6 includes a reference to "...one or more physical security plans..." that is not mentioned in the R5 requirement which appears inconsistent since R5 is the Physical Security for the BES Cyber Systems. Provide clarity and make consistent. c) Requirements 5.1, 5.2 and 5.3 appear to be less prescriptive than previous CIP 006 versions. However, is it left up to the Responsible Entity to determine the requirements for controlling access, monitoring access and logging access? Are some of the expectations from previous CIP 006 Rev. 3 still expected, but not documented? d) General Comment: V4 is very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R5.1, R5.2 and R5.3Physical security will be extremely difficult to implement on components located throughout the plant.For 5.9, assuming a key is used to access a system, revoking access within 72 hours maybe impossible. Changing locks may not be able to happen that fast. Face to face terminations may not be the case. Costs associated with card readers to replace locks is extremely high ($5-7k per reader, average 6 readers per hydro station and about 5 hydro stations this will apply to is a minimum of $150,000). Some systems are in cabinets that must be left open to do work. Card readers will set off alarms before work can be completed.For 5.11, should be deleted, as this should be included in the incident response procedures.For 5.2, what does monitoring entail?For 5.8, should be 48 hours.6.3 states "implementing maintenance and testing program....function properly". "Properly" is a vague term open for interpretation.
15.10	SCE&G	Disagree	Again, SDT should allow provisions for entities to leverage existing controls (i.e. Nuclear Facility Physical Security). NPP's have one of the most effective Physical Security

#	Organization	Yes or No	Question 15 Comment
			Programs of all Critical Infrastructures. CIP-011 R5/R5 should acknowledge this progam.5.2 SDT needs to better define what constitues appropriate "Monitoring". 6.3 "physical access control systems" should be defined. Is there an expectation for entities to walk fences around substations/generation facilities every 3 years?
15.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comment.
15.12	Liberty Electric Power, LLC	Disagree	CIP-011 R5 has very short times to revoke access. If an entity gives a contractor a code to enter the a room so he can download data on a Friday night shutdown, the code will have to be changed prior to the next business day -even if he is physically incapable of entering the plant.
15.13	E.ON U.S.	Disagree	CIP-011-1, R5.7, R5.8 and R5.9 does not fairly address the termination of access of contractors and/or service vendors. These types of requirements have generated many self reports to the NERC regions, and it is clear that this will continue so long as registered entities are presumed to have immediate knowledge of a change in the status of each contractor's employees. E ON U.S. proposes the requirements read as follows:R5.7 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for employees terminated for cause. For contractors/service vendors, access shall be revoked within 24 hours from the time of notification from the contracting/service vendor company."R5.8 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 36 hours. For contractors/service vendors, access shall be revoked within 36 hours from the time of notification from the contracting/service vendor company."R5.9 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 72 hours. For contractors/service vendors, access shall be revoked within 72 hours from the time of notification from the contracting/service vendor company."Additionally, CIP-011-1, R5.11 is ambiguous. E ON U.S. requests that the SDT clarify "review" to address is expected.

#	Organization	Yes or No	Question 15 Comment
15.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
15.15	LADWP	Disagree	Commensurate security measures need to be defined. If 6 wall is no longer the standard, what is replacing it?
15.16	Public Service Enterprise Group companies	Disagree	Comments: R5.8 requires physical unescorted access be revoked within 36 hours. This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.Physical protection of assets that are located within a NRC mandated Security Boundary / Perimeter that complies with NRC security regulations for Nuclear plants should be deemed to satisfy NERC CIP physical security requirements. NRC background checks, training, etc. for unescorted access and the physical security provided at Nuclear plants is more than adequate to satisfy NERC reliability physical security needs. Registered entities should not be required to implement duplicative procedures and programs for physical security of BES cyber assets located inside the NERC security Boundary/Perimeter. The drafting team should develop appropriate language to this effect.
15.17	CenterPoint Energy	Disagree	Disagree - For R5.8 and R5.9, CenterPoint Energy recommends increasing the timeframe for revocation of authorized unescorted physical access for personnel who no longer require such access to seven days as is found in the current Standard. CenterPoint Energy also believes physical access methods employed at a control center should differ versus those at a remote substation environment and therefore recommends revisions allowing for such differences.
15.18	FEUS	Disagree	Disagree with comments: 5.5 and 5.6 require authorization and quarterly reviews of unescorted physical access. It is not clear what type of authorization process would be required or what is required to be reviewed.

#	Organization	Yes or No	Question 15 Comment
15.19	Black Hills Corporation	Disagree	In 5.1, do not understand the significance of external connectivity only. Also in 5.1, restrict physical access is not defined (what evidence would be required to prove if we are not required to monitor, log, authorize, etc?) In 5.6, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual. 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
15.20	Constellation Power Source Generation	Disagree	In R5.2, what is meant by the term monitor? Is that continuous, automated monitoring, or can it be an inspection during an operator's round? A suggestion would be to include the phrase "automated or manual" to add clarity. R5.4 defines the action of logging as "manual or automated." This definition should also be used in R5.3 and R5.2. In R5.6, why is the review on a quarterly basis? Other requirements ensure that a terminated employee has access revoked extremely quickly, so the review in R5.6 can be extended out to an annual review without an adverse reliability impact on the BES. In R5.9, why is the term generation lowercase? Is this implying a different meaning? R6.3 is requiring testing and maintenance of all physical security mechanisms on a cycle no longer than 3 calendar years. However, some plants are on a 3 to 5 year maintenance schedule and are otherwise expected to be running. This will force a plant to take an outage it otherwise would not have just to comply with a physical security requirement.
15.21	Luminant	Disagree	It does not make sense to physically protect BES Cyber System for Meduim Impact systems that have external connectivity. The impact of physical access is no different that for systems not externally connected. 5.8 change to 48 hours (2 days) 5.9 1 week. Also remove 5.8 and 5.9 from the Medium impact requirements, as you cannot revoke access since it is not a requirement to restrict or grant unescorted access.
15.22	Emerson Process Management	Disagree	It is unclear about the relevance of physical access control and external connectivity.
15.23	WECC	Disagree	Low and Moderate impact assets must have some baseline physical security. It appears

#	Organization	Yes or No	Question 15 Comment
			that some requirements have differences between the levels for their own sake without the justification of security risk analysis. The standard should be adjusted to provide baseline physical security for all systems regardless of impact and/or method of communication.
15.24	Manitoba Hydro	Disagree	Manitoba Hydro does not agree with the drafting team approach to defer the FERC Order 706 directive for multiple physical security perimeters. Upgrading physical security at facilities is costly and time consuming and deferring the multiple perimeter requirement will require entities to later rework physical security at many facilities. The drafting team should either include the multiple physical security perimeters in version 4 or limit all physical security requirements to those already completed under CIP V1-V3. The reference in Requirement R5.11 to incident response procedures should be cross-referenced to Requirement R27, assuming that these are the procedures being referenced in Requirement R5. Requirement 5.7 could be interpreted as a subset of Requirement 5.8. Requirement 5.8 should explicitly exclude personnel terminated for cause. There are no specifics given with respect to 'restricting' access in Requirement 6.1 so it is assumed to be at the Responsible Entity's discretion in terms of to whom, by what means, etc. It is not clear if the "Required for routable access only" in the impact columns refers to routable BES Cyber Systems or routable physical access control systems.
15.25	Network & Security Technologies Inc	Disagree	Minimum retention period for logs should be specified. 5.11 does not specify a time frame for reviewing and handling unauthorized physical access attempts.
15.26	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R5, but recommends changes as follows: o Regarding Table R5, Minnesota Power recommends changing "areas protecting" to "areas containing BES Cyber Systems" to reduce ambiguity and confusion. o For Section 5.1 of Table 5, for Medium Impact Systems, the inclusion of the term "external connectivity" as a qualifier that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems

#	Organization	Yes or No	Question 15 Comment
			counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that the reference to “external connectivity” be removed from sections 3.2, 4.2, and 5.1 of Tables 3, 4, and 5 respectively. o As currently written, sections 5.3 and 5.4 seem to be similar and could be combined. If it is the Standards Drafting Teams intent that 5.3 apply to those individuals authorized for access, then Minnesota Power recommends the following revision to R5.3:"Log physical access to areas containing BES Cyber Systems for individuals with authorized cyber access and/or authorized physical access. Logging should..." o For sections 5.5, 5.6, 5.7 and 5.10 Minnesota Power recommends that the Medium Impact column match section 5.1. Since 5.1 requires restricted access, that implies that authorization needs to exist for access as well as access review, revocation, and visitor escorting procedures.Minnesota Power generally agrees with the proposed Requirements R6, but recommends changes as follows: o Requirement R6 discusses preventing and/or detecting unauthorized physical access to BES Cyber Systems while the sections of Table 6 discuss “physical access control systems.” This inconsistency creates confusion regarding what should be included in the physical security plan(s). o Regarding Table R6, Minnesota Power recommends changing “areas protecting” to “areas containing BES Cyber Systems” to reduce ambiguity and confusion. o Parts 6.1, 6.2, and 6.3 of Table 6 refer to the “physical access control systems” identified under Requirement R5, Part 5.1, 5.2, 5.3,” but R5 does not identify or use the term “physical access control systems.” Rather, it requires restricting, monitoring and logging physical access and does not require an access control system to do so. Certainly, as a result of its analysis and implementation of Parts 5.1, 5.2 and 5.3, a Registered Entity may implement an electronic system for access control, monitoring and logging, but it is not explicitly required. These parts should be reworded to state that if the Registered Entity has implemented an electronic physical access control system, then these requirements apply.
15.27	NextEra Energy Corporate Compliance	Disagree	NextEra believes it is not specifically clear what relations the different requirements have for the Medium Impact BES systems. For example, 5.1 requires that physical access be restricted, however, it would appear that this access does not need to be logged, authorized, or reviewed in 5.4 through 5.6. Similarly, 5.9 requires revocation of this

#	Organization	Yes or No	Question 15 Comment
			restricted access which may not have been authorized. We believe that R5 needs further clarification.Also, provide clarity regarding 5.1 "External connectivity only" requirement in Medium Impact column. For a site with Medium Impact BES Cyber systems, why would access not be restricted only if the BES Cyber Systems had no external connectivity. Granting access to the site may result in same impact once the individual is at the site as if they had remote connectivityRegarding R5 & R9 - 24 hour revocation requirement “for cause”, technical infrastructure does not support wide scale user administration to revoke cyber access within 24 hours. User administration for site cyber devices is not centralized. NextEra suggests providing specific definition of “revocation of access” to specify physical / cyber access. For example, if an individual has cyber access only and physical access and remote access to the systems is removed, this effectively revokes access. Regarding R5 & R9, what triggers “for cause” termination / no longer requires access?There needs to be consistency of administration in the industry. What starts the 24 hour clock?NextEra believes it should be at the point where the decision is officially entered into the system and/or communicated to the individual no longer requiring access.
15.28	Consultant	Disagree	NOTE: The format of these two requirements and tables is better than that for Requirements R1 through R4. For R5 & R6 the 'requirement' states the objective and the table specifies the required activities.R5 & R6 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R6. A physical security plan does not "prevent or detect unauthorized physical access..."It appears that R6 is misidentified as Physical Security Plans, when it seems to address protection for cyber systems providing physical protection to BES Cyber Systems.Based on the reconfiguration of the requirements in this standard a physical security plan is not necessary to meet the requirements.Suggest this requirement be restated to replace the term "Physical Security Plans" with "Protect Physical Access Control Systems" Table item 6.1 would require protection of cyber systems performing the functions identified in Table R5 items 5.1, 5.2, and 5.3 (See next comment regarding deleting 5.2).Table item

#	Organization	Yes or No	Question 15 Comment
			6.2 would require protection of cyber systems performing logging functions for physical access points.Table item 6.3 would require implementation of a maintenance & testing program for the assets identified in 6.1 & 6.2.A better option would be to include in Attachment 1 a function that relates to physical access control systems as part of the BES Cyber System identification. Such as:Physical Access Controls - activities, actions and conditions necessary to restrict and to log physical access to BES Cyber Systems. This would allow items 6.1 & 6.2 to be deleted, and the protections for "BES Cyber Systems" to apply to the physical access control cyber systems. Should the maintenance and testing requirements apply to BES Cyber Systems identified during the identfication and categorization proces, including those that are used to control physical access?
15.29	Garland Power and Light	Disagree	o Requirement 5.10 - clarify that continuous escort does not include entering bathroom facilities - some bathrooms are small non-partitioned one room facilities and it is inappropriate for escort in such areas.
15.30	PacifiCorp	Disagree	PacifiCorp generally agrees, except R5.9 should be expanded to control centers as well, and R5.8 should be removed. There is not a significant or compelling reason for different deadlines which add to the complexity of the standards and the administrative workload to parse the circumstances of each revocation.Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.31	Progress Energy (non-Nuclear)	Disagree	PE agrees with the 24 hour timeline for access revocation for employees terminated for cause, however it believes this will continue to pose a considerable challenge to many in the industry for its contractor population and would suggest “upon notification” be added to the beginning of the sentence. Thus, Section 5.7 would read, “Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.”PE disagrees with content set forth in R5.8 and R5.9 and believes it will be difficult for many entities to meet and likely result in significant violations throughout the industry. PE suggests language be added to include “upon notification” for both sections and change 36 hours to 48 hours

#	Organization	Yes or No	Question 15 Comment
			for Control Centers so that Section R5.8 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 48 hours," and Section R5.9 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours."5.1 implies that we could have a cyber component without external connectivity. 5.7 revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage. Other requirements appear to be in line with requirements of previous standards.CIP-011 R5.7 thru .9 what is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?Need clarification on period allowed for revocation of access due to expiration of training of background check - recommend that this be included with 5.8, 5.9 (no longer require access - or fail to meet necessary criteria).R5.7 - poor wording "handle...access attempts" Propose: "process such physical..."
15.32	Allegheny Energy Supply	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.33	Allegheny Power	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.

#	Organization	Yes or No	Question 15 Comment
15.34	EEI	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.35	MidAmerican Energy Company	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls. Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.36	Oncor Electric Delivery LLC	Disagree	Physical security at remote substation sites is not cost effective in preventing/detecting cyber attacks. Remote substations with only dial-up communications cannot support the 24-hr time frame of Requirement 5.7 when systems are non-functional (phone line damage, etc). Five to seven days may be required, depending whether some communication system has been installed to the facility. Physical security should only be required at control centers and High impact substations with IP based communications.
15.37	American Electric Power	Disagree	Please see comments as provided in response to Question 15.
15.38	Puget Sound Energy	Disagree	Puget Sound Energy has the following suggested changes:Table 5:5.3 - Suggest changing to “Logging shall record sufficient information to uniquely identify known individuals, or assist in the identification of unknown individuals, and the time of access...”Table 6:6.1/6.2 - Puget Sound Energy would like clarity on how restricting physical access to areas protecting control or monitoring systems for physical access protects the BES Cyber Systems. Physical protection of the BES Cyber Systems (Table 5) is understandable to protect the BES. But, a malicious or inadvertent act solely against the Cyber Systems that provide physical security in no way impact the BES or the Cyber Systems that make

#	Organization	Yes or No	Question 15 Comment
			up the BES unless the physical location of both types of Cyber Systems is the same.6.3 - Puget Sound Energy requests clarity on "...of all physical security mechanisms...". Like many entities, Puget Sound Energy employs physical security measures that are made up of components that do not use routable protocols. Is 6.3 suggesting a full test of all mechanisms (routable protocol or not) involved in restricting, monitoring, and logging? (Ex: card key strikes at doors)
15.39	LCEC	Disagree	R5 - and/or should simply read or. "To prevent and/or detect unauthorized physical access" should read "limit access to authorized personnel through detection and prevention."Medium impact for "external connectivity only" doesn't make sense from a physical security perspective. Change to Control center only.Move 5.8 and 5.9 to 5.7 and base the timings on whether or not it is a control center. CC should be 36 hours and others should be 72 hours.5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9The term "areas protecting" is confusing and should be replaced with "areas containing" BES Cyber Systems.Please consider identifying at what level of access granting must be removed to sufficiently mitigate the personnel risk.R6 Need to clarify "required for routable connectivity only" in regard to physical security controlsMost physical security systems do not require preventive maintenance which makes it difficult for an entity to provide a basis for maintenance performed. Testing is also a challenge because these systems either work or they do not work. What is the intent of the testing and maintenance requirement? Can this requirement be better served by reviewing the configuration of the system and comparison to approved access lists?
15.40	Southwest Power Pool Regional Entity	Disagree	R5 does not address the expectations of FERC Order 706 and subsequent orders. 5.3 needs to include both ingress and egress. 5.4 needs to include identification of the escort staff. 5.3 and 5.4 could be combined. 5.7: The time to revoke physical access can be much faster for control center environments; suggest 2 hours for the control center and 8 hours elsewhere. Ideally, the person's primary access credentials (badge, keys, etc.) should be lifted and access revoked concurrently with the person being notified of the termination for cause. 5.8 and 5.9 can be combined and the timeframe should be

#	Organization	Yes or No	Question 15 Comment
			expressed in business days. 5.10: define "continuous escort" somewhere. R5 overall: consider defining the concept of specifying an "effective date" of a transfer that reflects the reality that often a transferred employee will back fill or support the losing department for a period of time after the HR date of the transfer. 6.3 needs to be much more frequent in a control center environment where the inspection program can be readily performed; weekly is suggested. Additionally, the frequency needs to be commensurate with the impact category regardless of site characteristics.
15.41	ISO New England Inc	Disagree	R5.1 in table 5 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?R5.8 and 5.9 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday.
15.42	Western Area Power Administration	Disagree	R5.2: What is the definition of "monitoring" physical access? Since the concept of the physical security perimeter has been dropped, what specifically is meant by "access to areas protecting BES cyber systems? What constitutes sufficiency in monitoring?R5.3: What constitutes sufficient logging? Is a self-written logbook sufficient? Does logging have to be performed electronically or by a third party if manually logged, or is self-logging sufficient?R5.5: How does 5.5 differ from the requirements of R4?R5.7: Can be very difficult if someone is terminated on a Friday afternoon. Communication is very critical and requires more people knowing in advance, which in itself may cause an additional risk. R5.8: 36 hours could be an issue on 3 day weekends. Suggest 48 hours. Then is will only be an issue at Thanksgiving.R6, 6.3: Needs more guidance on testing and maintenance program what they must cover besides a blanket statement of testing and maintenance of all physical security mechanisms. Shouldn't we follow the installers or manufacturers recommendation on this? Documentation of these tests and maintenance evidence should be kept for how long?R6: what is meant by "routable

#	Organization	Yes or No	Question 15 Comment
			connectivity only"?
15.43	Kansas City Power & Light	Disagree	R5.3: What does "sufficient information" mean? This may encourage too much interpretation and recommend some clarity in the Table R5.R5.10: How do you prove someone who requires an escort was escorted at all times? From an audit perspective this is "proving the negative". It is understood what is intended in this requirement, but this is not measurable or auditable.R6.1 through R6.3: qualification here of "routable connectivity only" is not clear with respect to physical access controls. Routable implies electronic security measures rather than physical.
15.44	Con Edison of New York	Disagree	R5.8 and R5.9 - Add the words "Required for" before "Control Center" or before "Generation or Transmission Facility".R5.1 Need clarification to this item. If I have an enclosure which secures and isolated my cyber system, do I need to restrict access into the enclosure or do I need to restrict access to the area around the enclosure?R5.6 - Quarterly reviews are excessive. Annual or bi-annual would be reasonable.R5.9. - Should be business days, for example 3 business days. Support staff may not be available 24/7 to do this work.R5.10 - Continuous escort access is not practical in the numerous substations. The requirement should be relaxed to say oversight or supervisor, or any other mean which will limit the total escort and allow the operator to perform tasks while people may come to the station.R5.1 Medium Impact; not sure what external connectivity means? R3 clarification may resolve this.R5.8 (and others) - 36 hour requirements for compliance criteria will be a challenge
15.45	San Diego Gas and Electric Co.	Disagree	R5.8 and R5.9 require revoking authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours for medium and high impact control centers and within 72 hours for medium and high impact generation or transmission facilities. CIP-006-2 R1.5, by reference to CIP-004-2 R4, currently requires such revocation within 7 days for all PSPs. Revocation within 36 or 72 hours will be much more difficult to capture, especially for internal personnel reassignments. SDG&E believes that the risk to BES Cyber Systems associated with reassignment of an employee does not justify the effort (and potential non-

#	Organization	Yes or No	Question 15 Comment
			compliance) associated with this change. These time-periods approach the 24-hour limit for personnel terminated for cause in CIP-006, which does carry genuine risk to BES cyber systems.R6.1 and R6.2 in CIP-011-1 concern restricting and monitoring physical access to "areas protecting physical access control systems". Does this mean areas equivalent to PSPs have to be set up around these physical access control systems? Currently, CIP-006-2 R2 and R2.2 concern protection of "cyber assets that authorize and/or log access" to PSPs. Thus, server racks and control panels are locked and monitored, but PSPs are not required around these systems.
15.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R5.8 and R5.9 should be extended to 72 hours or next business day, whichever is longer, to allow for communications for this circumstance. A late Friday occurrence could be addressed early Monday instead of over the weekend.
15.47	Dominion Resources Services, Inc.	Disagree	R5.8 and R5.9. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user, then a shorter time frame to revoke access may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access within the time frames

#	Organization	Yes or No	Question 15 Comment
			specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination should be made at the quarterly review.
15.48	ERCOT ISO	Disagree	Recommend moving requirements 5.5 through 5.9 to a common access management section which addresses cyber access and information access. The remaining parts of Requirements R5 and R6 could be combined.
15.49	US Bureau of Reclamation	Disagree	Requirement R5: Physical security requirements are not adequately addressed in the present Standard. Much of the language from the previous version of the Standard should be re-established in version 4. In addition low and medium systems should include the equivalent of a 6-wall boundary around the cyber systems.Requirement R6: Physical security plans should be required for more than just electronic physical access control systems.
15.50	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
15.51	Xcel Energy	Disagree	The 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not needed. "Restrict physical access" in Requirement 5.1 also needs further definition. Does this mean locks?

#	Organization	Yes or No	Question 15 Comment
			Fencing?There appears to be inconsistencies between R5 and R6. Specifically;1) Table R5, R5.1 applies to Medium impact systems with external connectivity, while Table R6 6.1 applies to Medium impact systems with routable connectivity. 2) Table R6 refers back to 5.1, 5.2, and 5.3 for Medium impact systems, however 5.2 and 5.3 do not apply to Medium impact systems.
15.52	GTC & GSOC	Disagree	The 36 hour requirement for a person who no longer needs access (R5.8) is too stringent. If a transfer or retirement occurs on a Friday there is no reason you cannot wait until Monday. We recommend changing this to "within 36 hours or the next business day, whichever is greater".
15.53	APPA Task Force	Disagree	The APPA Task Force recommends the following edits to R5-R6:R5. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R5. Requirement:Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems." R6. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R6. Requirement: Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in CIP-011-1 Table R6 - Physical Access Control Plans
15.54	Bonneville Power Administration	Disagree	The objective of these requirements ("to prevent and/or detect unauthorized physical access to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.The objective of R5 and R6 should be changed to read "to prevent and detect unauthorized physical access to BES Cyber Systems." They should not say "and/or". Isn't the objective to prevent unauthorized physical access to BES Cyber Systems and to detect unauthorized physical access to BES Cyber Systems?R6: The entries in Table R6 refer to "Part 5.1, 5.2, 5.3". It is unclear whether these refer to subrequirements R5.1, R5.2, and R5.3, which do not exist, or in Table R5, entries 5.1, 5.2, and 5.3.5.7-5.9 refer to timeliness of revocation. Twenty-four hours for terminations for

#	Organization	Yes or No	Question 15 Comment
			cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8-5.9 this should be the same and be reviewed to take place within 3-5 business days. 5.11 is good in that unauthorized physical access is a procedural violation and not necessarily an incident.
15.55	Exelon Corporation	Disagree	The requirement to revoke access (5.8 & 5.9) in 36/72 hours for personnel who no longer require access is far too severe and places unnecessary administrative burden on the entity without technical or risk analysis justification. This would imply that there is little differentiation between an employee terminated for cause and a person who we regard as a solid member of our organization and in turn, we deem as having integrity. This would also become an undue burden to the business as our employees require transition time to ensure there is reliable transfer of information to the new owner of a role or task. This requirement would make that transition period extraordinarily difficult. Also, the ability to capture and store the transfer data to the hour would be impossible with our current human resource data systems. Modifying this system would result in major expense with little to no stated benefit to BES reliability. Exelon's position is that the current 7 day requirement is reasonable from a technical and risk perspective. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
15.56	Ameren	Disagree	The short period of time to remove access for 5.8 does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that this requirement be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred. Also, R6 should be a stand alone requirement, remove circular reference to R5.â€,
15.57	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 15 Comment
	Affiliates		
15.58	Entergy	Disagree	We disagree with 5.1 "Restrict physical access to areas protecting BES Cyber Systems" for Medium Impact BES Cyber Systems with external connectivity only. What difference does it make if the physical security of Medium Impact BES Cyber Systems access is restricted to the Physical Security Perimeters if the access mode to be protected is external, but there is no other requirement to monitor, or log access into or out of the PSP for these cyber systems.How can access be revoked from a Medium Impact BES Cyber Systems if there is no requirement to monitor or log access in and out of the PSP? There seems to be conflict with these requirements. Remove the requirements 5.1, 5.7 and 5.8 for Medium Impact BES Cyber Systems.Instead of having different access revocation time frames for High Impact BES Cyber Systems based on the locations as described in requirements 5.7, 5.8 and 5.9 it would be easier to manage evidence for compliance if all locations was the same. During the Dallas CIP Workshop it was apparent that the SDT was struggling with the interval for access revocation. It is suggested that the revocation of physical access for employees terminated for cause be by the end of the business day the first normal business day after the employee is terminated i.e. if the entities normal business week is Monday - Friday 8:00 - 5:00 and an employee is terminated Friday to Sunday then revocation should be completed prior to 5:00 on Monday for all High Impact BES Cyber Systems regardless were the cyber systems is located, control center, transmission facility or generating station. This would provide a consistent method of tracking the access revocation across the entities facilities and reduce requirements and potential compliance shortcoming and reduce the vulnerability of not taking actions to terminate employees for cause if the 24 hour requirement cannot be achieved on the weekend and the termination be held off until the normal work week when the requirement can be met.
15.59	We Energies	Disagree	We Energies agrees with EEI comment: Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to

#	Organization	Yes or No	Question 15 Comment
			determine the components that may need additional controls.
15.60	PNM Resources, Inc.	Disagree	We would prefer that all accress granting and revocation, for physical and logical access, be identified in a single table. In the current draft, they are scattered through several unrelated requirements.

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Some commenters expressed concern that the electric industry already physically protects its cyber assets from the public for reliability, business, and safety reasons, and that making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden that does not contribute any additional reliability to the Bulk Electric System.

Each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. The SDT has revised CIP-006-5 R1 to define the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

Some commenters also expressed concern that there appears to be a discrepancy in the Medium Impact category, where there could be sites that are not required to restrict access because there is no external connectivity, but they are required to revoke access. The SDT has revised these requirements and has removed the consideration for external connectivity from the applicability portion of this requirement, such that all Medium Impact BES Cyber Systems are required to have a Physical Security Plan. The revocation of access requirements are enumerated in CIP-005-5 R7, and have eliminated the identified potential for conflict.

Some commenters expressed disagreement with the requirements for restricting, monitoring, and maintenance testing for systems that provide physical access control over Medium BES Cyber Systems, when there is no requirement to monitor or log access into a Medium BES Cyber System. This likely is a conflict with the requirements for Medium BES Cyber Systems. The tables need to document basic physical security requirements for all Low and Medium Impact BES Cyber Systems. The SDT has revised the requirements for physical and electronic access for Low, Medium, and High Impact BES Cyber Systems to address these concerns. These requirements are stated in CIP-005-5 and CIP-006-5.

#	Organization	Yes or No	Question 16 Comment
16.1	American Municipal Power		Please provide a little or no impact category.
16.2	Regulatory Compliance	Agree	BUT:5.1 Medium Impact - "Required" only.

#	Organization	Yes or No	Question 16 Comment
16.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Blanks are ambiguous. If Low Impact is “Not Applicable”, then the blanks should be replaced with “NA”FMPA recommends making more clarity to the terms “required for external connectivity only” or “required for routable connectivity only” with: “required for areas containing BES Cyber Systems with routable external connectivity”FMPA believes that even Low Impact BES Cyber Systems should have restricted physical access and believes 5.1 ought to be applicable to Lower Impact “for areas containing BES Cyber Systems with routable external connectivity”R6 assumes card access and a “physical access control system” where the physical access may be restricted through lock and key (especially in substation environments for Medium Impact) and monitored through an alarm signal of a substation control house door opening through a SCADA system. It is unreasonable to require testing of simple padlocks or door-locks in 6.3.Maintenance of such system in 6.3 is unreasonable. Such electronic systems are usually just tested on a periodic basis and maintained as necessary. And, we assume that use of the system is testing the system. If not, what type of testing would be required in 6.3?
16.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
16.5	Manitoba Hydro	Agree	Manitoba Hydro agrees that physical security is not a standard requirement for Low Impact BES Cyber Systems, and should not be auditable. The electric industry already physically protects its cyber assets from the public for reliability, business and safety reasons. Making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden which does not contribute any additional reliability to the Bulk Electric System.
16.6	San Diego Gas and Electric Co.	Agree	Most of the requirements in Tables R5 apply to “high impact” BES cyber systems. Table R6, dealing with physical access control systems, applies to medium impact systems with

#	Organization	Yes or No	Question 16 Comment
			routable connectivity and high impact systems. This seems reasonable, but the scope will depend on what SDG&E determines will fall into these impact levels. Except as noted in the comments for Question no. 15, there are no apparent increases in physical security requirements for covered systems.
16.7	NextEra Energy Corporate Compliance	Agree	NextEra agrees but would like clarification regarding "Required for routable connectivity only" on Medium Impact physical access control systems. Also, as written, the standard does not have consistency in application of the different requirements as noted above.Also, in 5.11, how is the "unathorized physical access attempt" defined? Should this apply to all attempted access card swipes for electronic access systems. We do not believe that application of the incident response plan should apply to attempts such as these at the physical boundary. We believe a tie to suspicious activity threshold or physical boundary damage may be a better definition.NextEra also questions table R6, do training and PRA requirements apply to individuals with access to Physical Access Control Systems for BES Cyber Systems?
16.8	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
16.9	Northeast Utilities	Agree	Suggest merging 5.8 and 5.9 and using 72 hours for the allowable revocation period for all personnel terminated not for cause.
16.10	Minnesota Power	Agree	With the implementation of the changes and clarifications described in Question 15, the impact levels seem reasonable.
16.11	Independent Electricity System Operator	Disagree	- For R 5.8 and 5.9, if restricting physical access is not required for Medium impact assets (R5.1) then why does access need to be revoked?
16.12	PacifiCorp	Disagree	: PacifiCorp agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5

#	Organization	Yes or No	Question 16 Comment
			Row 5.2: There should be additional language describing what “Monitoring” means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.13	Madison Gas and Electric Company	Disagree	: Recommend 5.3 to use the same wording as 5.4 concerning logging access. This would reduce any confusion and provide uniform outcome to each sub requirement. Recommend 5.3 to read:”Log (manual or automated) ...” 5.7 states “Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause”. It may be possible to turn off someone’s electronic access but if there are combination locks, key locks, etc, this may not be possible to accomplish within 24 hours. This also applies to 5.8 and 5.9..
16.14	National Grid	Disagree	1. 5.1 - for Medium Impact BES CS, is it external connectivity with both routable and non-routable protocols? Please specify.2. There appears to be a discrepancy between 5.1 vs 5.7 & 5.8 in the Medium impact category. There could be sites that are not required to restrict access per 5.1 because there is no external connectivity. But, they are required to revoke access per 5.7 & 5.8. Could this be clarified?3. Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9.4. In 5.11, is the SDT considering providing the timeline for reviewing any unauthorized physical access attempts?5. Should the “routable connectivity” be “external connectivity” or “external routable connectivity” for Requirements 6.1, 6.2 and 6.3?
16.15	Consultant	Disagree	5.1 Physical access "Required for External Connectivity Only" is not logical. Suggest rewording to clarify.It is not clear why the change from Physical Security Perimeter to

#	Organization	Yes or No	Question 16 Comment
			the words "areas protecting BES Cyber Systems" makes sense. The new wording is not as clear and removes what was a "bright line". Suggest retaining the Physical Security Perimeter term in this version of the standards. 5.3 As this is currently stated it would appear to require monitoring and logging of both ingress & egress from "areas protecting BES Cyber Systems". Based on the discussion at the workshop, this is not the intent of this requirement. If that is the case then the wording should be modified to reflect the intent. 5.2 and 5.3 The distinction between "logging physical access" and "monitoring physical access" is not clear. If access is logged, then by default it has been monitored. Suggest deleting 5.2, or clarifying the difference between monitoring and logging in this context.5.4 The parenthetical after the word visitors is a definition, and as such should be listed as a definition, rather than being embedded in the requirement statement.5.4 Suggest replacing "to and from" with "entry and exit" or "ingress & egress". A more logical sequence of the requirements list by topic flow would be 5.1, 5.5, 5.3,5.2(see above comment), 5.4, 5.10, 5.7, 5.8, 5.9, 5.6.5.7, 5.8, 5.9 - Personnel transactions are typically measured in days. Setting a requirement in hours for a transaction that is not recorded at that level will create compliance problems. Suggest checking with the nuclear industry about time frames for access revocation. The answers there would be based on over 30 years of regulatory scrutiny.5.8 & 5.9 - There is no difference for personnel transactions based on the facility type, so creating a differential time frame for revocation by facility type would seem to imply that some facilities have less impact than other facilities outside of the impact categorization criteria. Suggest the access revocation time frames should be consistent based on the impact categorization, or adjust the impact categorization criteria to be consistent with the listed revocation time frames. The current table would imply that control center are high impact, and generation and transmission facilities are medium impact.5.11 Suggest deleting the word "any" as the current wording is unnecessarily restrictive. For example, the current wording implies that a single "bad swipe" of an access card should be reviewed, while entities typically have defined 3 to 5 consecutive bad swipes as an adverse event.5.1, 6.1, 6.2 & 6.3 - These table items create another dimension to the impact categorization process. If an asset has been categorized as Medium Impact, it should be afforded the

#	Organization	Yes or No	Question 16 Comment
			same level of protection as any asset categorized as Medium Impact. If the asset does not require the same level of protection then the impact categorization criteria should be adjusted to have it excluded from that impact level.
16.16	US Army Corps of Engineers, Omaha Distirc	Disagree	5.1 unclear why medium impact for "required for external connectivity only." Does this only apply to external connectivity hardware or is it for systems with external connectivity only? 5.8 & 5.9 are inconsistent with 5.5 granting of access is not required for Medium impact BES Cyber Systems.
16.17	Reliability & Compliance Group	Disagree	5.1, 5.5 and 5.8 are contradictory. They make you restrict and revoke access to medium impact systems but how do you do that if you don't have to authorize access to medium impact systems?Also, table R6 contradicts table R5 with regard to medium impact systems.
16.18	ERCOT ISO	Disagree	5.1: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System. 5.2-5.7: Should apply to medium impact BES Cyber System.5.10-5.11: Should apply to medium impact BES Cyber System.6.1-6.3: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System.
16.19	Dairyland Power Cooperative	Disagree	5.11 seems to say that known physical security incidents can be ignored for low and medium impact systems. This seems wrong. If a non-routable protocol terminates at some other facility, it seems there potentially should be physical access controls for that other facility as well-perhaps this would be required for high impact systems.
16.20	LCEC	Disagree	5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9R6 Need to clarify "required for routable connectivity only" in regard to physical security controls
16.21	Duke Energy	Disagree	a) CIP-011-1 Table R6 is identified as applying to "Physical Access Control Systems" but is very confusing to understand as written because the columns describe levels of impact

#	Organization	Yes or No	Question 16 Comment
			to the BES Cyber System but there are no impacts if the Physical Access Control System is operated on a network that is separate and distinct from the SCADA system. Is that the intended interpretation?b) Table R5 Physical Security for BES Cyber Systems state that requirement 5.1 applies only to Medium Impact BES Cyber Systems with "...External Connectivity Only". Does this mean that since 5.1 only requires restricting access to BES Cyber Systems; an acceptable method would be mechanical lock and key control?c) Table R6 Physical Access Control Systems state that Medium Impact BES Cyber Systems requirements R6.1, R6.2 and R6.3 for physical security are "Required for Routable Connectivity Only". Does this mean "Routable Connectivity" of the BES Cyber System or Physical Access Control System?d) Was the access control system intended to be included or intended to be excluded if it is on a separate network and not connected with any BES Cyber Systems? e) General Comment: V4 Tables R5 & R6 are very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R6.1, R6.2 and R6.3For Table R5, we propose the addition of "for external connectivity only" in the high impact column. Same for Table R6. Suggest changing "routable" in the table to "external" in Table R6Remove requirement for Medium impact in 5.1. Remove requirements for Medium Impact Systems in Table R6Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.22	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.5.8 - 5.10 is the first of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any

#	Organization	Yes or No	Question 16 Comment
			distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
16.23	Southwest Power Pool Regional Entity	Disagree	At a minimum, access revocation should extend to all impact categories. Access to a BES Cyber System is an available attack vector. 5.2: Restricting access without monitoring access is an ineffective control; 5.1 is not auditable in the absence of some sort of verification that the control is in place. 5.3 needs to consider that automated logging systems cannot guarantee 100% up time. Consider adding a requirement for recognizing the automated process has failed and responding to the failure (not the same as repairing the failure, which will be situation dependent. 5.11: There should be a clearly defined maximum timeframe for reviewing unauthorized access attempts. Simply leaving it to the discretion of an entity's incident response plan is not an effective control. R6: The Cyber security plan applicability will need to be updated to reflect any changes to the R5 applicability matrix.
16.24	US Bureau of Reclamation	Disagree	At a minimum, physical security controls should be required for low and medium systems, even if it is just a lock on the door.
16.25	FirstEnergy Corporation	Disagree	CIP -011-1 Table R5- Physical Security for BES Cyber SystemsItem 5.1: Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.Item 5.8, 5.9: Why two different revoke authorized unescorted physical access time periods to complete this task? It should be consistent for Control Centers, Generation and Transmission sites to revoke access in one time period to revoke access when no longer required. As stated this is open for confusion and separate corporate polices and procedures for personnel to train, track and manage. If desired to separate time frames it should be based on Low - Medium - High impacts which is not reflected.Additionally, we do not agree with the shortened time frame to revoke access to those who no longer require access -what justifies change? It should remain consistent with current CIP Ver 2 - Certain business processes and day to day operations will cause unrealistic burden in tracking from manual or automated process to revoke

#	Organization	Yes or No	Question 16 Comment
			access for no cause in shortened time frameItem 6.1 Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.
16.26	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
16.27	Ameren	Disagree	Due to the scope of the number of medium facilities it will be burdensome and labor intensive to maintain documentation of R5.1 physical security controls with no added protection to the BES. Suggest removing Medium Impact Systems from R5.1.
16.28	Entergy	Disagree	Entergy disagrees with the requirements 6.1, 6.2 and 6.3 to restricting, monitoring and maintenance testing to the systems and provide physical access control over Medium BES Cyber Systems when there is no requirement to monitor or log access into a Medium BES Cyber System, again there is a conflict with the requirements for Medium BES Cyber Systems. High BES Cyber Systems access for unescorted access and visitors alike logged and monitored for ingress and egress. If a systems is going to put in place to monitor egress for visitors then the same system could monitor unescorted personnel as well, this would reduced the maintenance of logs for visitors verses unescorted should be into and out unescorted and visitor alike for HIGH BES Systems should have a very high degree of control including the security systems providing access and monitoring.
16.29	Southern Company	Disagree	For 5.1, More specificity is probably called for here. What standard of care is called for? What does “protecting BES Cyber Systems” mean? Does it just mean “containing”?In 5.2, what are the boundaries of “monitoring”? Does this require real-time observation, alarm response, or after-the-fact review? What constitutes monitoring?5.5 “Authorize” should be replaced with “Control” or “Place limits on”.5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover employees only, or changed to 72 hours from notification by contracting company.There is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having

#	Organization	Yes or No	Question 16 Comment
			one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.30	MRO's NERC Standards Review Subcommittee	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections. We also believe a two tiered approach would be practical, where personnel specific access devices (manual keys, key cards, etc.) are removed immediately, and then wide scale access changes (shared combination locks, etc.) are allowed more time to be addressed. We believe this approach is similar to that of the NRC.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any

#	Organization	Yes or No	Question 16 Comment
			type of automated physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.
16.31	The Empire District Electric Company	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any type of physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.

#	Organization	Yes or No	Question 16 Comment
16.32	BGE	Disagree	General: What is an "area"? With the elimination of PSP this leaves "area" up for debate. Provide definition for "monitor" (is this manual, automated, 24x7??). 5.1 - Remove the requirement for medium impacted systems (currently says "required for external connectivity only, this requirement is pertaining to physical access). Combine 5.3 & 5.4 and reword to say "Log the entry and exit of all individuals with access to an area protecting BES Cyber Systems." 5.8 & 5.9 should not be restricted to removal from Control Center Only. This should be "areas protecting BES Cyber Systems" to maintain consistency. Define "Generation or Transmission Facility". Define "invalid access". To what extent does physical access mean, does it mean dispatching a guard for every single invalid access attempt? Under 5.8 access is revoked for Medium and High impacted systems but in 5.11 there is no requirement to review access for Medium impacted Systems.6.3 Physical access control systems were not defined in 5.1, 5.2 & 5.3. Should read "Implementing a maintenance and testing program for systems used to comply with 5.1, 5.2 & 5.3)." Define "physical security mechanism".
16.33	Constellation Energy Control and Dispatch, LLC	Disagree	-In 5.1 remove the requirement for medium impacted systems, which is not appropriate for a requirement pertaining to physical access.-Eliminate the timing differences for revoking access between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.
16.34	Bonneville Power Administration	Disagree	In general, Table R5 is acceptable, other than the items discussed below.We understand the impact of FERC requiring immediate revocation. However, it is difficult to see how to achieve that in every case. The standard should be based upon what is achievable and reasonable for both routine revocation and revocation for cause. The table should have a closer resemblance to R9.Section 5.8 and 5.9: 36 or 72 hours seems very short for revoking access for people who, presumably, are still trustworthy, but merely no longer need access or who have left the entity under routine circumstances. They simply no longer require access because of a job change. Such revocation should be a routine, normal business-day action. 72 hours does not allow for business-day action during a long weekend. In fact, for a large organization revocation for field assets in such a short

#	Organization	Yes or No	Question 16 Comment
			time period would often be impossible. Recommend changing this to five business days or five calendar days. We also recommend using the same criteria for all assets: Control Center, generation, or Transmission Facility.Section 5.11 is very good: it makes it clear that unauthorized access is an incident, not a violation.Table R6, 6.1-6.3 require the plans to address Part 5.1-5.3 if identified as "Medium". However, 5.2 and 5.3 do not require physical security under "Medium". How can a plan address elements that are not required?
16.35	Idaho Power Company	Disagree	In R5, if access authorization is not required for medium impact systems then why is there a requirement to revoke authorized access if it was never authorized in the first place.
16.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
16.37	Southern California Edison Company	Disagree	Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present, near a device, to operate it. The boundary protection for this type of role is: (1) the physical security boundary; and (2) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.While this control is easily implemented in a control center or data center environment, field devices that are often located over vast geographic areas pose compliance challenges. This requirement may result in the creation of substantial organization capabilities for compliance without a comparable improvement in reliability of the BES. SCE believes Requirement 5.1 should apply to low impact BES Cyber Systems and Requirement 5.5 should apply across all impact levels. For many field devices, where enforcement of cyber security controls in a timely fashion may be a challenge given the large geographic operational areas, limitation of physical access may be the most

#	Organization	Yes or No	Question 16 Comment
			effective control. Limiting unrestricted access, even to Low impact devices and the ability to control such access, could be a mitigating factor for the inability to perform device by device access revocation where no external access exists.
16.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.39	Oncor Electric Delivery LLC	Disagree	Physical security should only be required at control centers and High impact substations with IP based communications.
16.40	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only' in R5.1. This is an odd mix of physical and electronic access requirements. Please define the stipulations 'Required for external connectivity only' in R6.1, 6.2 and 6.3 for the same reasons.
16.41	WECC	Disagree	Recieved a uniform disagree from all but a vast range of responses to this question depending on the function of the entity reviewin the question.Low levels seem inappropriate as there is veryminimal requiremens for security based on the current tables.andShould apply to all impact levels.
16.42	Hydro One	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements

#	Organization	Yes or No	Question 16 Comment
			5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Please clarify Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.43	ISO New England Inc	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should specify something for BES Medium Impact Cyber System.Request clarification on Requirements 6.1, 6.2 and 6.3 is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.44	Northeast Power Coordinating Council	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Request clarification for Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.45	ReliabilityFirst Staff	Disagree	ReliabilityFirst believes the existing defined term "Physical Security Perimeter" should be retained and used in CIP-011. The current proposed language, "Restrict Physical access to areas protecting BES Cyber Systems", could lead to many questions for an auditor. Further, we believe that all rows of Table R5 (5.1 through 5.11) should be "required" for Medium Impact BES Cyber Systems. For Table R5, row 5.11; what constitutes an unauthorized physical access attempt? If unintended triggering of a magnetic card reader (such as simply walking too close to a reader and unintentionally activating it) indicates "failed attempts", are those to be considered unauthorized access attempts? Also in row 5.11, within what time frame must the review be conducted and we believe

#	Organization	Yes or No	Question 16 Comment
			there should be a requirement to document the review.
16.46	Luminant	Disagree	Remove the requirements for Medium Impact systems
16.47	Nuclear Energy Institute	Disagree	Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.48	Exelon Corporation	Disagree	Requirements 5.8 and 5.9 contain time parameters in hours. Exelon's tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required, it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? It is difficult to understand how the impact levels were determined. The basis of the original CIP Standards addressed the critical sites and took into account the nature of the Critical Cyber Assets that could impact the BES, not the functional/operational parameters of the equipment that is connected to the BES. Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.We are also concerned about the practicality of potentially applying these standards to multiple unmanned locations. Items 5.1, 5.2, 5.3: Requiring this level of physical security for any BES Cyber System that has no external connectivity should be reconsidered. No matter what level of impact, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.

#	Organization	Yes or No	Question 16 Comment
16.49	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
16.50	Xcel Energy	Disagree	See comments on question 15
16.51	Western Area Power Administration	Disagree	See previous comments
16.52	Emerson Process Management	Disagree	Since physical access restriction is not required for low and, maybe, medium impact BES Cyber Systems, according to R2 and R3, everyone in a generation plant will be subject to awareness and training requirements. Further, per R3.1, the training will cover the proper use of BES Cyber Systems, the proper handling of BES Cyber Systems information and storage media, and others. Why do plant's administrative staffs need to know how to use BES Cyber System?
16.53	Detroit Edison	Disagree	Table entries 5.8 and 5.9 require access revocation for Medium Impact access that is not required to be explicitly authorized.Table entries 5.8 and 5.9 should address the concept of expired PRA and/or training requirements. Propose changing 5.8 and 5.9 to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."Table entries 6.1, 6.2, and 6.3 Medium Impact states "Required for routable connectivity only". This term is not defined. We suggest replacing that language with "BES Cyber Systems that use a routable protocol".
16.54	EEI	Disagree	Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Table R5 Row 5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover

#	Organization	Yes or No	Question 16 Comment
			employees only, or changed to 72 hours from notification by contracting company.In general, there is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.55	Allegheny Energy Supply	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.56	Allegheny Power	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.57	American Electric Power	Disagree	Table R5:5.1, Column "Medium Impact BES Cyber System", regarding "Required for external connectivity only", this should be stated "routable external connectivity"?5.8 & 5.9, Column "Medium Impact BES Cyber System", regarding "Control Center only" and "generation or Transmission Facility only". Authorized unescorted physical access is not required for medium impact facilities in row 5.5. If it is not required in 5.5, how can it be revoked in 5.8?5.11, regarding "...unauthorized physical access attempts". Suggested wording: "unauthorized physical access or physical access attempts".Table R6:6.1: Row 5.1 only requires access to areas protecting BES Cyber Systems be protected. It does not say that it needs to be done with a control system. A pad lock can used to restrict physical access. It also requires it for any external connectivity, not just routable.6.2: Monitoring of Medium Impact BES Cyber Systems is not required in section 5.26.3: A physical security control system is not needed to meet row 5.1 on Medium impact

#	Organization	Yes or No	Question 16 Comment
			Facilities since no other requirements from Table 5 are needed.
16.58	Alberta Electric System Operator	Disagree	Tables R5 and R6 do not log, monitor, or control physical security and access to Low Impact BES Cyber Systems. Consider making the requirements in tables R5 and R6 more restrictive. For example, restrict physical access for all impact levels, but make frequency and time horizon of reviews dependent on impact level - Low Impact review semi-annually, Medium Impact quarterly, and High Impact monthly.In table 5.4 - Change to "Log (manual or automated) visitor access (individuals not authorized..." to be consistent with Table 5.3.
16.59	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to include the Low and Medium Impact requirement in 5.1, but as stated in our response to Question 14, we believe the implementation of this requirement must be for a reasonable physical access policy, for example, as required for employee and public safety code compliance. Compliance with this requirement should be straight forward: locked gates, locked control house doors and/or locked fence around BES Cyber systems. Table R5 Item 5.1 should state for Low and Medium Impact; "Required".The APPA Task Force supports the MRO-NSRS proposal For items 5.2 through 5.6; we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We also suggest the following language for the tables noted:R5 Table 5.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR5 Table 5.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.4: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.5: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.6: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force recommends removal of Table Items 5.7 - 5.9, dealing with "revoking authorized unescorted access," since this is covered in Table 9.2-9.5, Access Revocation. We believe there should not be a distinction between the two revocations and the timeframes for the revocation should be the same. There

#	Organization	Yes or No	Question 16 Comment
			should be only one set of revocation requirements.R5 Table 5.10: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR5 Table 5.11: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredThe APPA Task Force supports the MRO-NSRS proposal for items 6.1 - 6.3; hence, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard. The tables would then read:R6 Table 6.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force believes the 3 year maintenance and testing requirement on "all physical security mechanisms" in 6.3 is unreasonable. The term "all" should be replaced with "major" and the timeframe should be based on manufacturer recommendations, not an arbitrary 3 year timeframe.
16.60	Black Hills Corporation	Disagree	The concept makes sense, but 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
16.61	Network & Security Technologies Inc	Disagree	There are a number of inconsistencies in these and other tables related to grant and revocation of access (e.g., 5.1 requires restriction of physical access to areas protecting Medium Impact systems with external connectivity but 5.5 does not indicate such access must be authorized). Recommend a complete "scrub" of all requirements pertaining to authorization of, control of, and revocation of physical and electronic access.
16.62	We Energies	Disagree	We Energies agrees with EEI comment: Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.We Energies agrees with EEI comment: Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? We Energies agrees with EEI: Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a

#	Organization	Yes or No	Question 16 Comment
			particular item or location.We Energies agrees with EEI comment: Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.We Energies agrees with EEI comment: Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.63	Progress Energy (non-Nuclear)	Disagree	Why does Table R6 require access control to systems identified in 5.1, 5.2, 5.3 medium impact with routable connectivity, but 5.1 does not reference routable and 5.2, 5.3 have no requirements for medium impact?See comment 14.

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

Summary Consideration:

Comments concerning the requirement language in Requirement R7 with regard to "acceptable use" and the requests for clarity of the term "account types" indicated that these terms were misunderstood. The term "acceptable use" has been replaced with a requirement to authorize the use of account types, and the associated guidance document has been expanded to include descriptions of account types as used in this requirement.

Many commenters indicated that the format of Requirement R7 was causing confusion, suggesting that consistency in the use of columns and the format of the requirements and other information included in the tables would be helpful. The SDT agreed, and made consistency changes in the format and content of the columns in the tables, including the information required for High, Medium, and Low Impact BES Cyber Systems and BES Cyber Assets.

#	Organization	Yes or No	Question 17 Comment
17.1	ERCOT ISO	Agree	7.1: Please clarify "identification" and "group account".
17.2	Duke Energy	Agree	It's unclear how R7 tasks accomplish the purpose statement for low impact systems.
17.3	Minnesota Power	Agree	Minnesota Power generally agrees with the list of electronic access control requirements included in Table R7. However, it believes that some confusion exists regarding what distinguishes a "group" account from a "shared" account or a "system" account from an "administrative" account as described in Part 7.1.In addition, many types of equipment found in generating facilities or substations do not have typical "accounts," although they may have some type of access control (i.e., configuration password). To add further clarity, Minnesota Power recommends that the following be added to the end of purpose statement for Requirement 7:"...Required for only BES Cyber System

#	Organization	Yes or No	Question 17 Comment
			Components with account management capabilities."
17.4	Puget Sound Energy	Agree	Puget Sound Energy suggests that, because a BES Cyber System is made up of multiple components (hardware, operating system, application) that there should be a little clarity added. For example: "Identification of account types...and administrative accounts, in use for the BES Cyber Systems at the operating system, and applicable application(s) on the BES Cyber System Components."
17.5	Progress Energy - Nuclear Generation	Agree	R7 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
17.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
17.7	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
17.8	Entergy	Agree	This matches the guidance presented in the nuclear industry document NEI-08-09 Rev 6 Section 1.2.
17.9	Green Country Energy	Agree	Would it be possible throughout the standard to footnote sources for guidance such as DHS catalog of control systems or specific NIST documents? Hopefully this would remove some of the ambiguity and lead towards a more results based standard.

#	Organization	Yes or No	Question 17 Comment
17.10	Independent Electricity System Operator	Disagree	- Should R7.1 include anonymous to be consistent with R8.3.- R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy stateme
17.11	Southwest Power Pool Regional Entity	Disagree	7.1 needs to include both local and domain user accounts. Elaborate a bit more on what is meant by "group" account. In many cases, a group account and a shared account are the same account. Very easy to overlook the group categorization the way the requirement is written as it is not defined in the current CIP standards.
17.12	US Army Corps of Engineers, Omaha Distirc	Disagree	7.2 implies that the user agreements would be so detailed as to differentiate the valid uses of individual systems and account types. It should be possible to have user agreements that allow them to work on authorized systems for authorized purposes (ie sysadmin account is authorized for sysadmin work) and restrict use for unlawful and non business purposes.
17.13	BCTC	Disagree	Please provide a definition of Acceptable Use. It is recommended that the term "acceptable use" be replaced (i.e. are we looking to define the roles within the BES Cyber System and define what actions each can take within the system?)
17.14	Idaho Power Company	Disagree	Acceptable use is a broad term when it comes to administrative accounts. As long as acceptable use can be defined in general terms and does not require a definitive list, this requirement will be OK. If it requires a definitive list, then there is risk in trying to define every situation or use of an administrative account.
17.15	Constellation Energy Control and Dispatch, LLC	Disagree	Account types should be defined.
17.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 17 Comment
17.17	The Empire District Electric Company	Disagree	Comments: Many types of equipment found in generating facilities or substations do not have typical “accounts”, although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: “Required for only BES Cyber System Components with account management capabilities.”
17.18	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required based on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not support the ability to demonstrate acceptable use. Also for R7.2, CenterPoint Energy is not sure what is meant by "Acceptable use of each identified account types" and suggests adding specific examples.
17.19	Kansas City Power & Light	Disagree	Do all cyber systems and component that may be identified here have the capability to have an account? Recommend consideration of additional language such as “where equipment capabilities allow” for R7.
17.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be burdensome without preventing malicious activity.
17.21	Dominion Resources Services, Inc.	Disagree	Dominion presumes that the word “acceptable” used in 7.2 will be defined by the Reliability Entity and will not be dictated by an outside group.
17.22	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
17.23	Western Area Power Administration	Disagree	How is the responsible entity to meet this requirement for BES Cyber system components that do not have specific account types? For example...relays, comm equipment, other substation equipment that may now be part of the “affect situational

#	Organization	Yes or No	Question 17 Comment
			awareness of the BES" portion of the requirement.
17.24	Matrikon Inc.	Disagree	I would separate the requirements of creating an "inventory of user accounts" and its application to BES Cyber Systems, from the requirement of assigning "ownership and authorization of user accounts".The key separation is the "inventory" and the "authorization/use" of those accounts. A Cyber system may have 5 user accounts, of which some are disabled, some are shared, and some are actively used by specific individuals.
17.25	Florida Municipal Power Agency	Disagree	Is R7 needed since the real reliability goal is accomplished in R8? "Shall document" is not a strong requirement. The requirement is really account management. FMPA suggests: "Each Responsible Entity shall manage accounts and account permissions in the manner described in CIP-011-1 Table R7 - Account Management Specifications".Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, if R7 is kept, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
17.27	American Transmission Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities."
17.28	MidAmerican Energy Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration

#	Organization	Yes or No	Question 17 Comment
			password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.29	MRO's NERC Standards Review Subcommittee	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.30	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 7.1 within table 7 should provide guidance to identify role based access controls for accounts on the BES Cyber System components. The current way the requirement reads, it is unclear if the specific account types listed are the only ones required for identification. Additionally, the BES Cyber Systems may not have the specific account types listed in requirement 7.1. Furthermore, NextEra believes requirement 7.2 should provide additional guidance related to acceptable use. It is unclear if the acceptable use requirement should be defined per account on each BES Cyber System Component. The requirement should require acceptable use based on role based access controls for categories of accounts. What is the criteria for 7.2 "Acceptable use" of each identified account types? Please add a local definition of "acceptable use" within the standard.Regarding R7, this table seems to apply the CIP electronic account standards to all units. Is this the intent?If so, then for 7.1 - the volume of research and account management, we suggest applying this to high impact only.As for R11.1 does the user restriction for wireless technologies include Blackberries and SmartPhones, NextEra believes this would impact on volume of devices and would be burdensome to manage.NextEra would like to see statement treating personal communication devices the same as company issued laptops since there are internal access controls designed to prevent misuse.

#	Organization	Yes or No	Question 17 Comment
17.31	Indeck Energy Services, Inc	Disagree	Not all Cyber Systems have logins and accounts. [suggestion] “For any Cyber System permitting login access, each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 - Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.”
17.32	Network & Security Technologies Inc	Disagree	Purpose of R7.1 is unclear. Is it intended to require that every type of account a given individual has authorization to use be identified? If so, please clarify.Suggest “acceptable use” be addressed in R1 (policy) rather than here.
17.33	LCEC	Disagree	R7 - “access to its BES Cyber Systems “ should read “Access to a BES Cyber System or its components “Roles should be identified during the creation of accounts.R8 - R7 and R8 should be combined into managing accounts.In CIP 10 there should be an air-gap exclusion for the thousands of relays connected to medium impact or lower systems that would require access revocation.
17.34	Consultant	Disagree	R7 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R7 & Table: In this section there is a change in terminology from the requirement to the table name to the column heading for the requirements. For this requirement:R7: document BES Cyber System accountsTable Name: Account Management Specificationscolumn Heading: Account Management DocumentationThis is confusing, as it is not clear what the topic is being addressed. Suggest consistent terminology for these locations. NOTE: There are multiple requirements where this condition exists and should be addressed.R7 - Account management would not seem to prevent malicious operation of BES Elements. It would seem to maintain control of access to BES Cyber Systems. The grouping of Electronic Access Controls would be more likely to be used to prevent malicious operation. R7 - Suggest deleting the word "maintaining" as account management controls access to BES

#	Organization	Yes or No	Question 17 Comment
			Cuber Systems, and the word maintaining control is unnecessary.7.1 Suggested rewording: For each BES Cyber System identify the account types in use on that system, including individual, group, shared, system, and administrative accounts.7.2 The intent is not clear. Does this mean document the acceptable use of each account type on each system, or document the acceptable use of the account types in use across all BES Cyber Systems? The resulting documentation is significantly different.
17.35	Southern Company	Disagree	R7 creates a workload requirement with very little benefit to overall reliability.
17.36	SCE&G	Disagree	R7 Is every BES Cyber Sytem required to have account types. Will there be provisions for equipment incapable of having an "account type"?R9 When does the timetable start for personnel terminated for cause? Once paperwork is completed?R10 SDT should consider the high volume of TFEs that may be generated for equipment with hardcoded passwords that cannot be changed. The TFE process should be evaluated and revised to make it less burdomesome on entities to document that a password is incapable of being changed every 12 months, or a provision should be added to the requirments. Overall provisions should be added to allow entities to utilize more secure methods of account access control, such as RSA tokens, without burdening the entity with additional adminsitrative work for choosing an access control method which is inherently more secure.R11: The box containing the definition for remote access: is this remote 2-way or 1-way?
17.37	Luminant	Disagree	R7.1 should not be required for low impact.
17.38	ISO New England Inc	Disagree	R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy statement then it should be relocated to R1.
17.39	Ameren	Disagree	R7.2 does not list a monitoring frequency, it implies continual monitoring. Recommend that a monitoring frequency be added to this requirement.

#	Organization	Yes or No	Question 17 Comment
17.40	Powersouth Energy Cooperative	Disagree	R7-14. The required electronic security measures should be limited to the access or gateway point. Strong security measures at the gateway can effectively protect all the cyber assets that are accessed through the gateway. An argument can be made for example that the frequent changing of passwords on tens if not hundreds of devices inside a boundary that has very strong security measures lessens reliability should a qualified employee need to access the device but not be able to do so due to a recently changed password. Little is gained by requiring hundreds of devices inside a secure boundary to have the same level of protection that is provided through a secure gateway. Just because "it can be done" does not mean that "it should or must be done". The objective is to protect the assets. It should be recognized that protecting the assets can be done by focusing on the gateway that allows access to the devices. This allows entities to keenly focus on managing the security of those points of access rather than spending time, capital and other resources that provide limited if any added security. Prior to the workshop it was felt that strong gateway protection would meet the objectives of the standard. However, that is no longer clear. For example, it was felt that at a substation strong security measures at the gateway that allowed access to the cyber devices would meet the objective of standard with the cyber system (a collection of protective relays or other devices) being protected by the secure gateway. It appears that may not be the case. This results, for example, in the failure to change a password in a single device on a secured network being non-complaint with the standard for a situation where the BES reliability was never jeopardized. That type approach will likely result in numerous non-compliances that will on serve wasted resources even though the BES was never jeopardized. If it is intended that protecting only the gateway meets the objective that needs to be made clear.
17.41	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms. What is the difference between group and shared? What is the definition of "Acceptable use"?
17.42	San Diego Gas and Electric	Disagree	SDG&E recommends separating Wireless concepts from Access Concepts. Wireless is a

#	Organization	Yes or No	Question 17 Comment
	Co.		method of access, as is VPN, Citrix, dial-up, etc..., while Access implies a physical and logical service provided to a client.
17.43	Garland Power and Light	Disagree	Shared & group accounts should not be created or allowed because there is no accountability for these accounts
17.44	APPA Task Force	Disagree	The APPA Task Force does not believe the description of R7 follows the intent of the requirement. The following are recommended edits:R7. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R7. Requirement:Each Responsible Entity shall document manage BES Cyber System accounts Components with account management capabilities by incorporating the criteria specified in CIP-011-1 Table R7- Account Management Specifications R8. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R8. Requirement: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 - Account Management Implementation R9. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R9. Requirement: Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation R10. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber SystemsR10. Requirement:Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 - Account Access Control Specifications The drafting team uses the word "any" in the description in R11 and R12. This appears to require the all BES Cyber Systems be included in the requirement, even if the wireless functionality is disabled. The APPA Task Force believes the description should read: R11. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R11. Requirement: Each Responsible Entity that allows remote or wireless electronic access to a BES Cyber System shall apply the criteria specified in CIP-011-1 Table R11- Wireless and Remote Electronic Access Documentation for that specific BES Cyber System R12. Objective:To ensure that only authorized access is allowed to BES

#	Organization	Yes or No	Question 17 Comment
			Cyber Systems that have remote or wireless electronic access.R12. Requirement:Each Responsible Entity that allows wireless and remote electronic access to a BES Cyber System shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 - Wireless and Remote Electronic Access Management for that specific BES Cyber System. R13. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R13. Requirement:Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems [it owns and operates?] by implementing the criteria specified in CIP-011-1 Table R13 - Remote Access Revocation R14. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R14. Requirement:Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to the BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 - Wireless and Remote Electronic Access Controls.
17.45	Southern California Edison Company	Disagree	The drafting team should clarify mapping of controls, as identified in CIP-005 R1.5, and unbundle these requirements for access control devices. This would be in agreement with the drafting team's stated objective to leverage the financial and organizational capital invested by registered entities in providing cyber security through compliance with current versions of the CIP standards. SCE believes that all instances of electronic access, whether to the boundary or a system/device within the boundary, should be in one requirement. A new standard for access may include these account related controls in addition to others.The drafting team should provide guidance for R7.2. As written, R7.2 suggests that the acceptable use for each identified account type is required across all impact levels. It is not clear whether the intent here is to document business justification(s) for the acceptable use, the posting of signage describing acceptable use, or both. SCE recommends that the drafting team explicitly state the intent of this requirement.

#	Organization	Yes or No	Question 17 Comment
17.46	US Bureau of Reclamation	Disagree	The use of terminology is a problem in this standard. It is suggested that the term "electronic access" should be used instead of the term "account";or, a definition should be developed to clearly differentiate the difference, if there is one. The term electronic access is more precise.
17.47	Public Service Enterprise Group companies	Disagree	This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.
17.48	Pepco Holdings, Inc. - Affiliates	Disagree	What is a Cyber System account? Does this exclude Cyber System Component accounts? Would microprocessor relays passwords be in scope? Please reference comments on BES Cyber System Components and BES Cyber System definitions.
17.49	Manitoba Hydro	Disagree	What is the definition of “Acceptable use” for Requirement R7.1?

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011 R7 was moved to CIP-007-5 R5.

Several commenters expressed concern that the documentation requirements for Low Impact BES Cyber Systems would be burdensome and would not prevent malicious activity. In response, most documentation and technical requirements applying to Low Impact BES Cyber Systems have been removed. However, the requirement for changing the default password remains, because this addresses a significant vulnerability and does not require periodic maintenance.

Some commenters suggested the standards need to be more explicit as to whether the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components. In response, the SDT provided additional clarity as to when a requirement applies to individual Cyber Assets. However, the requirements are written to allow flexibility in implementation.

In addition, commenters suggested adding "Required for routable connectivity only" to the applicability for Low and Medium Impact BES Cyber Systems. In response, the applicability for this requirement has been modified to High and Medium Impact BES Cyber Systems. For Medium Impact BES Cyber Systems, the SDT does not believe that the communication attributes of the BES Cyber System adequately mitigate the vulnerability this requirement addresses.

#	Organization	Yes or No	Question 18 Comment
18.1	Idaho Power Company	Agree	Account types will not vary by BES impact.
18.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
18.3	The Empire District Electric Company	Agree	Comments: We agree, assuming the suggested statement under question 17 is included.
18.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 18 Comment
18.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
18.6	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels of R7 if the drafting team accepts our edits proposed in response to question 17.
18.7	Duke Energy	Agree	This is a lot of work to do for low impact systems. We suggest the requirement be removed from R7. Please provide insight as to how these tasks accomplish the purpose for low impact systems.
18.8	MRO's NERC Standards Review Subcommittee	Agree	We agree, assuming the suggested statement under question 17 is included.
18.9	BGE	Disagree	7.1 and 7.2 remove the requirement for low and medium since we do not need to log and monitor those systems per R8.
18.10	The United Illuminating Co	Disagree	7.1 and 7.2 should not apply to Low Impact devices.
18.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
18.12	LCEC	Disagree	Clarify if 7.1 & 7.2 are for account types only or if this includes specific accounts.
18.13	Indeck Energy Services, Inc	Disagree	Cyber Systems without login access need to be excluded.
18.14	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be particularly burdensome for low impact BES cyber systems.

#	Organization	Yes or No	Question 18 Comment
18.15	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
18.16	Minnesota Power	Disagree	It appears inconsistent with the other Requirements of CIP-011-1 to apply the criteria specified in Parts 7.1 and 7.2 to Low Impact BES Cyber Systems. If those using accounts on Low Impact Systems are not required to have Training, as required in R3, how are they to know the acceptable use of these accounts and therefore, why inventory and document it?
18.17	LADWP	Disagree	Low impact BES Cyber Systems should not be required.
18.18	National Grid	Disagree	National Grid suggests removing controls for Low Impact BES CS in table R8 to be consistent with table R7.7.2 - Elaborate on “acceptable use” and documentation required for acceptable use
18.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirement to identify and document acceptable use of accounts on Low Impact BES Cyber systems should not be required. The exercise of complying to that requirement for Low Impact BES Cyber systems will take considerable effort but will provide little if any security value or improve the reliability or security of the BES Infrastructure. It is recommended to have the requirement apply to both Medium and High Impact BES Cyber Systems.
18.20	American Municipal Power	Disagree	Please provide a little or no impact category.
18.21	Hydro One	Disagree	Presently, R7.1 specifies identification of account types. We suggest that the requirement R7.1 is modified to delete the word “types”.
18.22	Puget Sound Energy	Disagree	Puget Sound Energy notes that physical security measures are only applicable to High Impact and some Medium Impact BES Cyber Systems. Puget Sound Energy suggests aligning Table 7 to Tables 5 and 6, or clarifying “Required for routable connectivity only”

#	Organization	Yes or No	Question 18 Comment
			for Low and Medium Impact BES Cyber Systems. At the very least, Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management.
18.23	Progress Energy (non-Nuclear)	Disagree	R7.1 - account management for "low" assets may be significant when you consider all of the intelligent programmable field instrumentation they will likely be categorized this way.Acceptable use is too broad a requirement. If someone is deemed competent to have access this requirement is not needed.Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.24	Constellation Energy Control and Dispatch, LLC	Disagree	Remove Required status for low and medium BES Cyber Systems, since R8 does not require logging or monitoring of those systems.
18.25	Garland Power and Light	Disagree	Requirement 7.1 & 7.2 should not be required for Low Impact BES Cyber Systems
18.26	Network & Security Technologies Inc	Disagree	See response to 17, previous.
18.27	Constellation Energy Commodities Group Inc.	Disagree	Should not be required for low impact systems.
18.28	Ameren	Disagree	Suggest removing R7.1 and R7.2 for Low Impact Systems. Creating and maintaining recordkeeping for all BES Systems will be a massive undertaking with no added protection to the BES.
18.29	Entergy	Disagree	The requirements should apply across the board for sites where routable protocols and dial-up communications are employed.

#	Organization	Yes or No	Question 18 Comment
18.30	Allegheny Energy Supply	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.31	Allegheny Power	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.32	EEI	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.33	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments. Please also reference comments on BES Cyber System Components and BES Cyber System definitions.
18.34	American Transmission Company	Disagree	We agree, assuming the suggested statement under question 17 is included.
18.35	We Energies	Disagree	We Energies agrees with EEI use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT

#	Organization	Yes or No	Question 18 Comment
			needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.36	FirstEnergy Corporation	Disagree	We feel there could be limited value in maintaining account type information for low impact BES Cyber Systems. Suggest removing 'required' for that column of table for R7.
18.37	Manitoba Hydro	Disagree	What is the purpose of Requirement 7.1 for Low Impact BES Cyber Systems? It is not clear that this information is needed for other requirements. Requirement 7.2 is inconsistent with Requirement R3, where no training is required for Low and Medium Impact BES Cyber Systems. Defining acceptable use of account types serves no purpose if it is not provided in training. The meaning of the references in Requirement R7.1 to "account types" and in Requirement R10.8 to "non-privileged accounts" is unclear. The reference in Requirement R7.2 to "Acceptable use of each identified account types" is incomplete. What is it that the Responsible Entity is required to do - develop criteria related to acceptable use, monitor for compliance with such criteria, etc? There are no specifics given with respect to "restrictions" in Requirement R11.1 or "allowed methods" in Requirement R11.2 1, so it is assumed to be at the Responsible Entity's discretion. It is unclear whether Requirement R11.3 requires a written policy to be in place - one would assume no written policy was required by the opening language of Requirement R11.

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

Summary Consideration:

Some commenters expressed concern that physical and electronic access controls may use the same terms, but they can actually mean different things, so there is a need to keep the requirements separate. In response, the terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters expressed the need to combine requirements so that all "revoke" requirements are in one place. The SDT agrees with this suggestion, and the requirements to revoke access have been combined.

Some commenters expressed the need to combine the physical and electronic access control requirements based on the concern that being in separate requirements might lead to an entity missing something. The SDT agrees with this suggestion. The terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters suggested continuing the use of ESP and PSP terminology, since it is now well understood. Upon further review, the SDT decided to continue use of the term Electronic Security Perimeter (ESP), but PSP has been modified to Defined Physical Boundary (DPB) to focus the requirements on controlling access rather than creating a perimeter.

#	Organization	Yes or No	Question 19 Comment
19.1	Duke Energy	Agree with proposed method	Access control for physical and electronic should continue to be separate.
19.2	Dairyland Power Cooperative	Agree with proposed method	Access to a physical area is different than access to an account that provides access to system(s) or application(s). Separate handling is appropriate.

#	Organization	Yes or No	Question 19 Comment
19.3	City Utilities of Springfield, Missouri	Agree with proposed method	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
19.4	Platte River Power Authority	Agree with proposed method	Electronic security and physical security are different disciplines and should be kept separate.
19.5	LCEC	Agree with proposed method	I agree that these should be separate but think that the retired terminology like Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) are well understood and should not be retired for the sake of change. A lower level of controls does not make sense for physical access in some areas like data centers or control centers but may make sense in areas like substations.
19.6	Southwest Power Pool Regional Entity	Agree with proposed method	Physical access control includes certain requirements, such as escort, that are not applicable to electronic access. If combined, the standard will need to carefully make the appropriate distinction between physical and electronic access controls as necessary.
19.7	Bonneville Power Administration	Agree with proposed method	Physical and Electronic access controls may sometimes use the same terminology, and appear similar, but they are very different disciplines. Physical security may use electronic tools are part of its tool kit. However, it is still primarily a physical and geographical control methodology. Electronic access controls are more amorphous, with boundaries being at once more difficult to define, but more easily and absolutely controlled. Combining them would only lead to confusion and probably to failure in the end.
19.8	FirstEnergy Corporation	Agree with proposed method	Preference is to keep all electronic access requirements together, all physical access requirements together, and all informational access requirements together, but keep the three separate from each other.

#	Organization	Yes or No	Question 19 Comment
19.9	San Diego Gas and Electric Co.	Agree with proposed method	SDG&E recommends separation of the concepts of Logical (electronic) and Physical access.
19.10	APPA Task Force	Agree with proposed method	The APPA Task Force agrees with the SDT's proposal to separate requirements for Physical Access and Electronic Access. We do want to point out that both are interdependent. If a BES Facility has physical access control and does not have external routable connectivity, you do not need cyber system access control. This is covered in our comments for a number of the requirements where we recommend changing the impact level from "Required" to "Required for Routable External Connectivity Only."
19.11	Madison Gas and Electric Company	Agree with proposed method	The separation allows for clarity in these two distinct areas.
19.12	Progress Energy - Nuclear Generation	Agree with proposed method	To improve this Requirement, see attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
19.13	Xcel Energy	Agree with proposed method	We believe the separation is beneficial because it recognizes cases where physical access is needed but electronic access is not required, such as in the case for a mechanical maintenance vendor who performs no duties requiring electronic access.
19.14	Regulatory Compliance	Agree with proposed method	Would not want the controls for Physical Access and Electonic Access to be mixed.
19.15	US Bureau of Reclamation	Combine Access	Agree, but physical, logical, and information access control requirements should all be

#	Organization	Yes or No	Question 19 Comment
		Control requirements	included under a single set of requirements.
19.16	ERCOT ISO	Combine Access Control requirements	All access control areas should be combined (i.e., electronic access, physical access, information access). This will enable ease of use of the standard and a clearer understanding of the requirements. The current practice of having to go from standard to standard to find the requirements makes it more likely to miss a requirement and risk potential violations.
19.17	Puget Sound Energy	Combine Access Control requirements	As stated in the comments for question 18, Puget Sound Energy would prefer to see consistency (or an explanation of the differentiation of physical and logical controls).
19.18	Detroit Edison	Combine Access Control requirements	Combine all access control and revocation requirements into one requirement and one table.
19.19	Garland Power and Light	Combine Access Control requirements	Combine Tables R5, R9, R13, and R24.4 into one table so one can look at one table and see all the “revoke” requirements in one place - for most companies, the same people are going to be involved with “revoking” regardless of the Requirement #.
19.20	Consultant	Combine Access Control requirements	If the requirements for access control are the same, then combining them is better.Consideration should be given to combining information protection access and wireless access as well.It will also be clearer if there are any differences in access requirements for different types of access to have them combined so differences are obvious.
19.21	Idaho Power Company	Combine	It makes sense to combine some of them such as authorization, PRA and training,

#	Organization	Yes or No	Question 19 Comment
		Access Control requirements	revocation. Others are more specific to the type of access and may not lend themselves to combining.
19.22	USACE - Omaha Anchor	Combine Access Control requirements	Makes it easier to know which access must be terminated without looking through the entire document.
19.23	Southern California Edison Company	Combine Access Control requirements	The drafting team may not have adequately addressed the intent of Order 706 with respect to system security controls. Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present near a device to operate it. The boundary protection for this type of role is (a) the physical security boundary and (b) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.
19.24	Reliability & Compliance Group	Combine Access Control requirements	Tracking is easier if they are combined. We suggest that information access control be also included.
19.25	American Municipal Power	Combine Access Control requirements	Whenever possible, please eliminate redundancy in the requirements.
19.26	Progress Energy (non-	Combine	Will these be two distinct groups or will many have both accesses? Many people with

#	Organization	Yes or No	Question 19 Comment
	Nuclear)	Access Control requirements	physical access to transmission facilities will also need electronic access, suggesting that a single group/list may be easier to maintain.
19.27	Florida Municipal Power Agency	Combine Access Control requirements	Without a change in the definition of BES Cyber System to include an exclusion similar to the existing CIP-002-2 R3.1, R3.2 and R3.3, then there can be thousands of digital relays covered by this standard. A relay technical could have electronic access to thousands of such relays. It would be impossible to change all of those accounts within the time limits proposed in R9. We need to be careful in developing the standards that we do not cause unintended consequences of changing behavior that would reduce the reliability of the BES. This requirement R9 (and others within the standard) may have an unintended consequence of causing entities to revert to electro-mechanical relays to avoid onerous requirements in the standards. Reverting to electromechanical relays would likely increase costs as far as increased maintenance and testing requirements, but, would save costs of having to change accounts at numerous remote locations every time an employee changed positions.FMPA suggests combining physical and electronic (including wireless) access requirements to develop more reasonable requirements for situations such as these, e.g., revoking physical access to BES Cyber Systems with no external routable protocol should be enough. Thinking through these combinations is important to developing reasonable requirements.

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R7 and R8 have been moved to CIP-004-5 and CIP-007-5.

Some commenters expressed confusion regarding the definition of "monitor" with respect to shared and guest account access privileges. In response, the specific term "monitor" has been removed from these account access requirements in favor of clearly defining the functions and actions associated with monitoring. Requirements to monitor access control have been moved to the Security Event Monitoring requirements in CIP-007-5.

Some commenters expressed a belief that the requirement for quarterly review of accounts and access privileges is excessive. The SDT notes that the quarterly review is required for Medium and High Impact BES Cyber Systems. The drafting team has clarified that it is not necessary to perform a detailed quarterly review of entitlements at the individual asset level.

Some commenters expressed a need to make the requirements for Account Management Specifications (CIP-011-1 R7) and for Account Management Implementation (CIP-011-1 R8) more consistent. In response, the drafting team has attempted to supply consistency as suggested by the commenters and has included these requirements in CIP-007-5.

Some commenters suggested removal of allowance of "guest" accounts. The drafting team believes there are reasons to retain "guest" accounts, and that complete removal would cause a hardship to some entities or may not be possible. Those using such accounts should be identified as required in the modified requirement.

Some commenters suggested combining Account Management Implementation (CIP-011-1 R8) with Access Revocation (CIP-011-1 R9). The drafting team has combined requirements in all cases where it seems feasible. However, what was formerly R9 concerned revocation, which carries a different VRF than most other access control requirements, and the subject matter concerns personnel actions. The Access Revocation requirements are now defined in CIP-004-5 R7.

Some commenters suggested changing R8.3 to "maintain a list of those who have access to guest/shared accounts." After review, the SDT determined that this part of the requirement was unnecessary and has removed it.

#	Organization	Yes or No	Question 20 Comment
20.1	National Rural Electric Cooperative Association (NRECA)		In R8.3, how do your demonstrate "monitor" to an auditor? This should be reworded such that both the auditor and the utility understand this the same way.
20.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.3	The Empire District Electric Company	Agree	Comments: Note impact level comments under question 21.
20.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."Apply criteria" is not a strong requirement. The activity is account management, so, the requirement ought to be account management and R7 and R8 can be combined.Quarterly reviews of all accounts and privileges could be an onerous activity, and could actually decrease the reliability of the BES due to the higher rate of human error. FMPA suggests annual review of accounts and associated access privileges.
20.5	Puget Sound Energy	Agree	Puget Sound Energy suggests that R8.1 include wording regarding the removal of accounts. Example: "Establish and implement a process for authorizing the addition of account(s) and associated access. This process shall include necessary steps for the removal of accounts when no longer necessary."
20.6	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
20.7	APPA Task Force	Agree	The APPA Task Force Agrees with the criteria. See our response to Question #21 for

#	Organization	Yes or No	Question 20 Comment
			the Impact Levels discussion.
20.8	FEUS	Agree	The drafting team should clarify 8.3 what is intended to 'monitor' the use of shared and guest accounts.
20.9	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Item 8.2 in Table R8 states "Conduct a quarterly review and verification of accounts and associated access privileges." It does not indicate what type of documentation is required to demonstrate compliance. Is an attestation sufficient documentation? Or is the Responsible Entity required to have specific documentation of its quarterly review by account types, etc?
20.10	Reliability & Compliance Group	Agree	The requirements in table 8 really should apply to medium impact systems as well.
20.11	Independent Electricity System Operator	Disagree	- R8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session.
20.12	Southwest Power Pool Regional Entity	Disagree	8.1: Authorization should be required for both the addition and the modification of a user account. 8.3: Define what is meant by "monitoring" the use of the shared and guest/anonymous accounts. Is it sufficient to know that someone used the account or must their activities with the account be monitored? Is monitoring required in real-time or after the fact? Is there a requirement to review account activity after the fact?
20.13	Con Edison of New York	Disagree	8.2 Quarterly reviews are excessive, suggest annual reviews and a documented

#	Organization	Yes or No	Question 20 Comment
			process for adding, removing or modifying access8.3 Need clarification on what monitoring means outside of annual review of if it is still required
20.14	Progress Energy (non-Nuclear)	Disagree	8.2 Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
20.15	American Electric Power	Disagree	8.3, regarding "Monitor the use of shared and guest/anonymous accounts". This is not technically feasible on all systems. What level of detail is required to monitor the use? Does this need to be an automated electronic process? Is it even feasible to believe this can be done manually? How long must this monitoring data be kept?This should be removed.
20.16	Michigan Public Power Agency	Disagree	A quarterly review and verification of accounts would be overly burdensome and would not improve the electronic security of the system compared to a defined "annual" review.
20.17	BCTC	Disagree	Â Suggest removing “guest” from the language; guest accounts should not be permitted to be used in a secure systemÂ R 8.3 why single out monitoring of shared and guest accounts; should we not monitor all accounts?; unsure what the objective of this requirement is
20.18	Entergy	Disagree	Again, this is similar to NEI-08-09 Rev 6 Section 1.2. However, we question the advantage of having Account Management Implementation separate from Access Revocation. Please consider combining R9 with R8 by adding requirements 8.4 and 8.5 (below) and modifying the language in 8.1, as well as adding ‘required’ to low and medium impact BES Cyber Systems for 8.2 and 8.3.
20.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required base on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not

#	Organization	Yes or No	Question 20 Comment
			support the ability to demonstrate acceptable use.
20.20	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the wording of R8.3 to read:"Maintain a list of who has access to shared and guest/anonymous accounts."
20.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
20.22	LCEC	Disagree	In 8.1, changes to existing accounts that grant additional access should be authorized as well.
20.23	Black Hills Corporation	Disagree	In 8.2, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual.
20.24	Minnesota Power	Disagree	In Part 8.3 of Table 8 the Standards Drafting Team needs to clarify what is meant by the term "monitor." Does this mean that Registered Entities need to be able to review who (named individual) accessed a shared account, and when this access occurred, or does this require logging their actions while utilizing the shared account? In addition, does this include system/admin accounts (as they are listed above as being different than shared accounts)? These measures seem to be appropriate, but implementation and providing auditable evidence could be difficult.
20.25	Idaho Power Company	Disagree	Monitor in 8.3 is vague. Would it require just that we know who used the account when or more detail about what the user did while using the account.
20.26	National Grid	Disagree	National Grid recommends changing Requirement 8.2 from "quarterly review" to "annual review" since the extra work is noticeably less than the benefit. Request clarification on 8.3 "monitor"
20.27	NextEra Energy	Disagree	NextEra believes the standard requirement 8.3 needs to be clarified regarding the

#	Organization	Yes or No	Question 20 Comment
	Corporate Compliance		ability to "Monitor" the use of shared and guest/anonymous accounts. What is the extent of this monitoring? If allowed by the standard, we do not believe effective monitoring of the use of these generic accounts is feasible due to their generic nature. This may be better stated as maintaining logging information and ensuring that quarterly reviews ensure access is documented to individuals with valid business need and credentials.The impact levels are appropriate for the requirement. However, for Requirement 8.2 it is unclear what an acceptable verification method is. Clarification regarding recommended methods for verifying accounts and privileges especially for legacy BES Cyber System components should be included in the requirement.Additionally, Requirement 8.3 is concerning because it is unclear what monitor means in the context of the requirement, the word should be clearly defined. Multiple users can use shared accounts at the same time and that would be something impossible to monitor. If monitor means who has approval to use shared accounts and who is has access to the password for shared accounts that should be defined in the requirement. Likewise, it is unclear how to monitor anonymous access. Clarification should be provided regarding the definition, intent, and appropriate evidence to demonstrate monitoring.
20.28	Oncor Electric Delivery LLC	Disagree	Not all BES Elements can monitor the use of shared and guest/anonymous accounts. TFE should be applicable. Requirement 8.3 should only apply to remote routable communications.
20.29	American Municipal Power	Disagree	Please provide a little or no impact level category
20.30	Pepco Holdings, Inc. - Affiliates	Disagree	Please reference to question 17.
20.31	Ameren	Disagree	R8.2 - Exhaustive review of all accounts quarterly will be time consuming with no added protection to the BES; this requirement should be changed to annually.

#	Organization	Yes or No	Question 20 Comment
20.32	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R8.2. Due to the requirements of R9 the review and verification time should be extended to an annual time frame.
20.33	Western Area Power Administration	Disagree	R8.3 - What constitutes “monitoring” of the use of shared and guest/anonymous accounts?
20.34	EEI	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account.
20.35	Southern Company	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account. In addition, . this requirement could require a large number of TFE’s for systems which do not support multiple passwords.
20.36	Kansas City Power & Light	Disagree	R8.3: What does the “Monitor” represent?
20.37	Hydro One	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.38	ISO New England Inc	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review” since the extra work is noticeably less than the benefitR8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session. clarification on monitoring use of shared accounts.

#	Organization	Yes or No	Question 20 Comment
			"use" not provisioning. login/logout, all activity while logged in? commands used?
20.39	Northeast Power Coordinating Council	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.40	BGE	Disagree	Replace the word “elements” with Cyber System Component to maintain consistency with the defined terms. R7 & R8 requirements need to be synchronized. What is the definition of “monitor” (track actions, how much detail, will sudo suffice?)
20.41	Northeast Utilities	Disagree	Request clarification:- Are shared accounts included in 8.2 and required to be reviewed quarterly?- What does monitor mean in 8.3?
20.42	Garland Power and Light	Disagree	Requirement 8.3 - Do not believe that shared and guest/anonymous accounts should be allowed.
20.43	Network & Security Technologies Inc	Disagree	SDT should clarify intent of 8.3 (monitor use of shared and guest/anonymous accounts).
20.44	GE Energy	Disagree	Some type of account and privilege review should be required for Medium Impact systems, but not on a quarterly basis. These systems may well be used to validate software before promoting it to High Impact systems, and thus should have some account management due diligence.
20.45	Platte River Power Authority	Disagree	Suggested Revision:8.3 Track individuals that have been granted access to shared and guest/anonymous accounts.
20.46	Duke Energy	Disagree	Table 8: 8.2 quarterly reviews are too frequent. Suggest annually8.3 explain what is meant by “Monitor”What are the expectations for monitoring use of shared and guest/anonymous accounts? Is that up to the Responsible Entity? If the RE provides a procedure/policy and follows the policy, is that sufficient to pass audit?What is the

#	Organization	Yes or No	Question 20 Comment
			acceptable practice? 24/7?
20.47	ReliabilityFirst Staff	Disagree	Table R8; row 8.1 - suggest adding the word “document”, row 8.2 - what constitutes “review” and suggest the review should be documented, row 8.3 - what does “monitor” mean?
20.48	Constellation Energy Control and Dispatch, LLC	Disagree	The phrase "monitoring the use" of accounts is too vague.
20.49	ERCOT ISO	Disagree	The requirements of R7 and R8 can be combined. The purpose of each requirement is so similar that there appears to be no reason to separate them.
20.50	WECC	Disagree	The table lists three procedures for account management. Suggest this requirement be written to state: “Each Responsible Entity shall have implemented and documented procedures as described in Table...”The requirements should mandate additional rigor around access management, including the maintenance of access lists or automated provisioning systems. Additional specificity should be added to clarify the level of detail at which access must be tracked.
20.51	Consultant	Disagree	The word 'criteria' should be changed to requirements, as the table is listing requirements.Suggest replacing the words "to prevent malicious operation of BES Elements by maintaining..." with to maintain control..."Table R8-8.3 Not clear why this only applies to shared and guest accounts? And the difference between 'monitoring' and 'logging' is not clear.Suggest requirement is to "Log electronic access to BES Cyber Systems." and keep as required for High Impact Systems.
20.52	Dairyland Power Cooperative	Disagree	Validating whether users are assigned to appropriate roles or accounts should follow this timing. A detailed review to insure that the roles (or account groups) have proper permission settings can be a very time consuming and complex task depending on the complexity of a system. The detailed role definition review should be no more frequent than annually. The language used is not clear as to whether a distinction is

#	Organization	Yes or No	Question 20 Comment
			intended.
20.53	GTC & GSOC	Disagree	We recommend in R8.3 the term "Monitor" be replaced by "Review monthly". The term "monitor" could be taken to imply real time monitoring. Many entitities do not have the communication links required to meet such a real time requirement.
20.54	Alliant Energy	Disagree	We recommend retaining the annual requirement for 8.2 account review while retaining a quarterly requirement for personnel access review.8.3 needs more clarification regarding the activities included in the term “use” so as to provide specific guidance as to what constitutes a sufficient audit record.
20.55	The United Illuminating Co	Disagree	What is the intent of 8.3? It is difficult to discern what Monitor means in this requirement.
20.56	Manitoba Hydro	Disagree	word “Monitor” in Requirement 8.3 is unclear.

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R8 has been moved to CIP-007-5 R5.

Some commenters expressed concern CIP-011-1 R8.1 (Account Authorization) should apply to all three impact levels. In response, the SDT notes that authorization also implicitly carries with it requirements for account review, revocation, and training. The SDT did not believe that the effort required to comply with these requirements for all three impact was appropriate given the risk posed to the Bulk Electric System.

Other commenters expressed concern that only Medium Impact BES Cyber Systems with routable external connectivity should be subject to the Table R8 requirements. The SDT disagrees and believes regardless of a BES Cyber System's communication characteristics, it is important to ensure that access to BES Cyber System is properly authorized and subject to periodic review.

Other commenters also expressed concern that the requirements in Table R8 should be aligned with those in Table R7. In response, the Table 7 and Table 8 requirements have been combined into CIP-007.

Some commenters expressed that the impact levels in R8.2 should have different review periods. The SDT believes a quarterly review period for access authorization and an annual review period for access privileges are appropriate for both High and Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 21 Comment
21.1	Florida Municipal Power Agency	Agree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections.
21.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 21 Comment
21.3	Puget Sound Energy	Agree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management. If account management is not required for Low Impact BES Cyber Systems then it is unclear what benefit is there in identification of those accounts.
21.4	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
21.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
21.6	FirstEnergy Corporation	Agree	While the proposal provides flexibility based on Impact Categorization from a practicality viewpoint it will be easier to administer if all are treated equally. FE would likely take a conservative approach and treat all the same to simplify administration of this requirement.
21.7	ReliabilityFirst Staff	Disagree	8.1 should apply to all BES Cyber Systems. 8.2 should provide different periods of review for different levels of impact. Suggest making these annual for Low Impact, semi-annual for Medium Impact, and quarterly for High Impact.Suggest “required” Medium Impact for row 8.3.
21.8	ERCOT ISO	Disagree	8.1: Should be required for all. 8.2: Could be documented temporally. Low Impact required annually. Medium Impact required quarterly. High Impact required quarterly. 8.3: Please clarify meaning of “monitor”. Should be revised to address who has access to the accounts.
21.9	US Army Corps of Engineers, Omaha Distirc	Disagree	8.3 "monitor the use of" is somewhat vague. What would the measure be? Please define

#	Organization	Yes or No	Question 21 Comment
21.10	Southwest Power Pool Regional Entity	Disagree	Account authorization is a basic security control and should be applicable at all impact levels. Periodic review is also important and should be done for at least Medium impact systems as well, albeit more frequently for High impact than lesser impact.
21.11	Alliant Energy	Disagree	Alliant Energy agrees with EEI's comments relative to 8.3 and the consideration of capabilities and connectivity.
21.12	USACE HQ	Disagree	At a minimum, 8.2 should be required for all impact levels. Requirement 7 creates a document of every account type and its acceptable use, but for low and medium impact systems it is not required to update the same as per requirement 8.2.
21.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
21.14	The Empire District Electric Company	Disagree	Comments: For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.15	FEUS	Disagree	Disagree: The drafting team should consider 8.1 be applicable to LOW BES Cyber Systems for consistency with 7.1, 7.2, and 9.1. Without a process for authorizing new accounts it is difficult to review approved accounts and to revoke access that was not authorized.
21.16	WECC	Disagree	Even "Low Impact" systems have the capability of impacting operation of the BES within 15 minutes, thus these requirements should be required for all impact levels. Again, this requirement could then be rewritten without the table to provide more clarity.These requirements should apply to all impact levels

#	Organization	Yes or No	Question 21 Comment
21.17	San Diego Gas and Electric Co.	Disagree	For entities that own both Medium & High impact assets, they will likely perform all of the requirements contained in Table 8 for both classes of assets instead of maintaining separate procedures and mechanisms that will have a higher risk of compliance errors. SDG&E believes it just adds potential confusion to the process to have different requirements for Medium and High impact assets in this instance.
21.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.19	American Transmission Company	Disagree	For R8.1 through R8.3 suggest adding "Required for routable external connectivity only." At the present there is no practical method to monitor the use of devices such as relays and IMUXs when accessed from inside a substation. They may be able to be front-ended, but as yet it has not proven viable.
21.20	Consultant	Disagree	If 8.1 requires authorizing accounts for Medium Impact Systems, then quarterly review of 8.2, and the logging access of 8.3 (see previous comment) should be required for those systems.Or, remove the requirement in 8.1 for Medium Impact Systems.
21.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
21.22	Black Hills Corporation	Disagree	In 8.3, do not understand why guest/anonymous accounts would be allowed. Should be limited to shared accounts only.
21.23	E.ON U.S.	Disagree	It is not clear what is meant by the term "monitor." Does monitor in 5.2 mean active

#	Organization	Yes or No	Question 21 Comment
			monitoring, e.g., video" Does it mean log?
21.24	Emerson Process Management	Disagree	It is prudent that account and privilage can only be created and granted with proper authorization. This principal should be applied to any BES Cyber System.
21.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
21.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comments below:Regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.27	Con Edison of New York	Disagree	Modified 8.2 should be required for medium (annual review)
21.28	American Municipal Power	Disagree	Please provide a little or no impact category
21.29	BGE	Disagree	R7 & R8 requirements are not synchronized.
21.30	Ameren	Disagree	R8.3 - should be required for Medium Impact Systems.
21.31	Allegheny Energy Supply	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

#	Organization	Yes or No	Question 21 Comment
21.32	Allegheny Power	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.33	EEI	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.34	Southern California Edison Company	Disagree	SCE believes it may be possible to leverage the NERC PRC standards to effect compliance. In R8.2, an additional control with a timeframe longer than a quarter may be added for low and medium impact systems. It seems that access to low and medium impact systems never has to be verified. Although monitoring under R8.3 is not required for low and medium, which SCE is in agreement with, SCE believes that R8.2 should be modified where list of accounts and access privileges are tracked on a time bound basis.[MVL-HOW?] This may be an opportunity for the drafting team to review the appropriate NERC PRC standard on protection relay maintenance schedules and leverage the compliance requirements stated there.
21.35	GE Energy	Disagree	See question 20 comments
21.36	Entergy	Disagree	Suggest 8.2 apply to medium assets as 8.1 required a process for authorization. There is value in reviewing access lists from a security perspective.
21.37	Network & Security Technologies Inc	Disagree	Suggest adding a periodic review of access privileges to Medium Impact systems (8.2), perhaps every 12 months in lieu of quarterly.

#	Organization	Yes or No	Question 21 Comment
21.38	Alberta Electric System Operator	Disagree	The AESO believes that reviews should also be performed for Low and Medium Impact levels. Consider creating additional rows in the table to perform annual reviews for Low and Medium Impact BES Cyber Systems.For Table 8.1 - A process should be required for all impact levels.For Table 8.3 - Monitoring should be performed for all impact levels, however frequency of monitoring can be dependent on the impact level.
21.39	APPA Task Force	Disagree	The APPA Task Force supports the proposal by the MRO-NSRS to change 8.1 - 8.3 under Medium Impact to read "Required for routable external connectivity only." As stated in our response to Question #19, the physical security is covered in requirement R5 so only routable external connected devices are vulnerable. The tables should therefore read:R8 Table 8.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
21.40	Constellation Power Source Generation	Disagree	The impact levels mapped out in R8 should be changed to mimic those in R7. Why identify all account types for every BES Cyber System, but then require processes for authorization and quarterly reviews of privileges for some of the impacts?
21.41	Reliability & Compliance Group	Disagree	The requirements in table 8 really should apply to medium impact systems as well.
21.42	Southern Company	Disagree	The scoping levels of R7-R14 are vastly expanded when compared to R5 and R6. Each requirement should be examined to determine the correct scope to best support overall reliability. The lack of differentiation based on connectivity and BES component type, in conjunction with the inclusion of requirements that have a per-low-system-component impact, mean that the vast majority of the effort involved in CIP compliance will have to be spent on low-impact, relatively unimportant assets,

#	Organization	Yes or No	Question 21 Comment
			often at the expense of overall reliability.
21.43	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to systems with routable communications.
21.44	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Table R8 Row 8.3.
21.45	We Energies	Disagree	We Energies agrees with EEI regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.We Energies agrees with EEI regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6 and R7.

A number of commenters requested that the Standards make a distinction between "primary" access and "secondary" access, based on an understanding that an individual would need primary access to be able to use any secondary access (such as a database account). The SDT has revised the access revocation requirements (CIP-004 R7) to state that revocation of access includes remote, electronic, and physical access to the BES Cyber Systems. The requirements also address the revocation of "the ability to access" BES Cyber Systems and BES Cyber System Information as well as the resulting follow up actions related to additional assets (such as applications and databases). The SDT believes this best captures the concept of primary and secondary access.

Other commenters suggested revocation "with cause" should remain at 24 hours, and revocation "without cause" should remain at 7 days. This timing would keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer. In response, the SDT notes the FERC Order directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Given that organizations usually have termination procedures to return company property and perform exit interviews, the SDT believes the processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

Some commenters expressed concern that the revocation timeframe requirements based on combinations of BES Cyber System type and Impact Level are overly complex, and add confusion and undue administrative overhead in situations of job changes. To address this, commenters recommended more consistent timeframes. In response, the requirement has been modified to simply revoke access when a person no longer needs it. Evidence showing termination down to the hour is not practical in many cases. In the revised requirements, entities will show revocation of access as part of their termination procedures and demonstrate they follow these procedures (i.e., through dated sign-off records, system logs or actual system access control databases).

#	Organization	Yes or No	Question 22 Comment
22.1	Green Country Energy	Agree	Additionally addressing the transfer of responsibilities to another individual shpould be addressed if the terminated employee is a system administrator or such. If a "key" individual is terminated it may be quite a process to remove them from the system within 24 hours,leaving a system vulnerable or a backup plan unable to be executed. In summary termination with cause of a high security level employee could be very difficult to accomplish in 24 hours.
22.2	Oncor Electric Delivery LLC	Agree	One of the few examples where “Control Center” is separated from Transmission and Generation.
22.3	FEUS	Agree	The drafting team should consider revising the wording for revocation as ‘immediately but not to exceed XX hours’
22.4	Progress Energy - Nuclear Generation	Agree	To improve implementation of this requirement incorporate information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
22.5	Regulatory Compliance	Disagree	9.1 - clarify for service vendor that the clock should start upon notification to the entity.9.2-9.4 - 7 day revocation across the board
22.6	American Electric Power	Disagree	9.2 - 9.4: Recommend rewording 9.2-9.4 to match 5.7-5.9 or vice versa.Recommend removing physical access and external connectivity within a short-time window, and application rights later.
22.7	ISO New England Inc	Disagree	9.2, 9.3, 9.4 - all should be within the same time frame 72 hours. Same level of security issues or concerns across all (control center, trans, gen). Remove Requirements 9.3 and 9.4R9.2, R9.3 a d R9.4 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the

#	Organization	Yes or No	Question 22 Comment
			change."The purpose of the requirement is so that personnel have the least amount of access that is needed to do their jobs and so that they don't accumulate access as they move around. Also this is to limit possible segregation of duty violations and to require that authorized access permissions are the minimum necessary to perform work functions. (R10.6)
22.8	Dominion Resources Services, Inc.	Disagree	9.2, 9.3, and 9.4. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user then a shorter time frame may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes. And 24 hours is only possible if Revoking System Access is limited to controls that prevent the user from physically and electronically accessing the system. For example, if the user must either have physical access to the device or authenticate through a corporate system (e.g., active directory) before being allowed to access a BES Cyber System, then removal of physical access rights and of the ability to authenticate in the corporate system meets the Requirement for revoking system access, even though an account may still exist on the BES Cyber System. The account on the BES Cyber System would be removed within 7 days since many BES Cyber Systems are not administered 24x7.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access

#	Organization	Yes or No	Question 22 Comment
			within the time frames specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination can be made at the quarterly review.
22.9	Con Edison of New York	Disagree	9.2,3,4 - may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
22.10	US Bureau of Reclamation	Disagree	A requirement for revocation needs to be included for all impact levels. Suggest the timeframes for Requirements 9.2 through 9.4 be established on the basis of business days (for example 2 business days) or that the number of hours be increased cover long weekends.
22.11	MidAmerican Energy Company	Disagree	Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems. Also see MidAmerican Energy's response to question 54.
22.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also, 9.2 - 9.4 is the second of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations

#	Organization	Yes or No	Question 22 Comment
			for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
22.13	Kansas City Power & Light	Disagree	Are these requirements applicable for electronic and physical access? 36 and 72 hours are too short a time frame for considering personnel who have changed access status other than that of termination when consideration of weekends and holidays. 5 to 7 business days would be an appropriate time frame. For personnel terminated for cause, 24 hours is acceptable.
22.14	Xcel Energy	Disagree	As noted in our response to a previous question, the 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
22.15	E.ON U.S.	Disagree	CIP-011-1, R9 references "system access." Does this mean physical or electronic access? For requirements 9.3 an d 9.4 it can be difficult to determine the exact time a person no longer needs access if, for example, the person has not required access for an extended period of time.E.ON U.S. does not believe compliance requirements are necessary for the low impact category.
22.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
22.17	The Empire District Electric Company	Disagree	Comments: If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose

#	Organization	Yes or No	Question 22 Comment
			that the period for removing electronic access be lengthened.
22.18	BGE	Disagree	Define “immediate”. The table does not specify that the revocation is for personnel with electronic access. Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent.
22.19	USACE HQ	Disagree	Does not make sense to create “for cause” requirement in any environment but a “no longer require” for only three (3) specific environment. I suggest to only have a two requirements, one (1) “for cause” and one (1) “no longer require”.
22.20	Duke Energy	Disagree	For 9.2, change 36 hours to 48 hours. Is the FERC mandate for ALL BES systems? Is there any room for loosening the requirement for low impact system?
22.21	Reliability & Compliance Group	Disagree	For personnel transferring to new positions where access is no longer available, 36 hours seems unduly burdensome. Recommend that this be changed to 72 hours for personnel no longer needing access to control center BES Cyber Systems.Also, this contradicts R5. Why do you need to revoke physical access at all for medium impact systems if you did not authorize it in the first place?
22.22	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
22.23	MRO's NERC Standards Review Subcommittee	Disagree	If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose that the period for removing electronic access be lengthened.

#	Organization	Yes or No	Question 22 Comment
22.24	WECC	Disagree	If the goal is to revoke access at termination (“immediate”) then the requirement should state simply, “The Responsible Entity will remove electronic and physical access at the time of termination.” This should be possible for any entity that has use physical tokens for physical or electronic access (such as RSA SecurID, keys, RFID badges), however it would NOT be possible for entities that are still using access control systems with passwords, combination locks, or other access methods where revoking access requires reprogramming of devices. Note- this could indirectly require token based authentications for perimeter access which is not necessarily a bad requirement for medium and high impact systems.Terminations for cause should require immediate revocation of access - performed in conjunction with the termination notification to the employee. This is already standard practice at many entities. Additional criteria regarding employee suspensions should be added.
22.25	Consultant	Disagree	Immediate revocation is not achievable as indicated by the fact that there is a time frame for each identified revocation condition. Suggest using rules similar to the nuclear plants for access revocation, as those rules have over 30 years of regulatory basis for being adequate to control access revocation.R9. - Suggest deleting the words "...by maintaining control of access to its BES Cyber Systems," Revoking access does prevent malicious operation.9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.9.2, 9.3, & 9.4 - the word "such" in the statement is unnecessary. Suggest deleting the word "such".Similar to combining access requirements, the revocation requirements should be combined. This makes both

#	Organization	Yes or No	Question 22 Comment
			similarities and differences easier to understand.
22.26	Minnesota Power	Disagree	In extreme circumstances, it may not be possible to adhere to proposed the 24 and 36 hour revocation timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule.Are we to interpret “revoke system access” to mean access to individual accounts, or does it also include shared/group/system/admin accounts known by the person who no longer requires access?
22.27	LADWP	Disagree	It is infeasible to revoke access to Medium and High BES systems within the max 72-hour requirement. a. Revocation of Hard-Copy information should not be considered under the standard. b. The current 7 day window for revocation of access for individuals no longer needing access is reasonable and should remain a part of the standard.
22.28	Allegheny Energy Supply	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Another example is if the BES Cyber System has no electronic communications outside of its physical boundary, then revoking physical access is effectively revoking access. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.29	Allegheny Power	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System.

#	Organization	Yes or No	Question 22 Comment
			Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.30	EEI	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.31	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
22.32	Southwest Power Pool Regional Entity	Disagree	Make a distinction between "primary" access and "secondary" access. Primary access includes the domain user account, remote access (e.g., VPN, dial-up) credentials, and physical access (badge, keys) credentials. The idea is that the individual would need to gain access using the primary access in order to be able to use any secondary access such as a database account. Revoke primary access in much less than 24 hours for termination for cause, especially for control center systems access. Ideally, primary access should be revoked at the same time the individual is being terminated. Express revocation timeframes for terminations other than for cause in terms of business days. Provide for a negotiated "effective transfer date" other than the HR effective date; transferred personnel often back fill or otherwise continue to provide assistance to the losing department for some period of time.
22.33	National Grid	Disagree	National Grid recommends that Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems (transmission, generation, and control centers)

#	Organization	Yes or No	Question 22 Comment
			and remove Requirements 9.3 and 9.4.
22.34	Manitoba Hydro	Disagree	NERC should request from FERC a clarification on their meaning of “immediate”. “Remote access” in Requirements R11 - R14 could be considered a subset of “system access” in Requirement R9. Is the intent for Requirement R9 to refer to local, electronic access?
22.35	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirements for access revocation for personnel who are still employed by the responsible entity but no longer in a job function that requires access to BES Cyber Systems are too restrictive. The responsible entity should be able to develop timelines and processes to support the removal of access for a person who transfers, since a transfer is not an indication that the employee is a security risk or threat to the BES Cyber System.For personnel terminated for cause, the access should be removed before notification to the impacted personnel. The access that is revoked would be considered global access, as in the terminated personnel’s physical access to the BES Cyber Systems as well as network access. The responsible entities could then create a process, which gives them additional time up to two weeks, to remove individual system access to each BES Cyber system component. For personnel who separate from a responsible entity due to retirement or resignation should go thru a deprovisioning process based on the responsible entities internal processes. The risk posed by normal termination or transfer is extremely small and if malicious behavior or intent is planned, then the actions will happen before the scheduled termination. The recommendation is to revoke network and corporate cyber access and physical access, which would be considered global access within a 2-week timeframe. The responsible entities could then create a process, which gives them additional time up to thirty days, to remove individual system access to each BES Cyber system component. NextEra would also like to establish what is meant by revoking System Access? Is this revocation time frame applicable to removal of access rights at the Boundary Level, BES Cyber System level, or BES Cyber System Component Level?â€,Access is given to individuals on different levels beginning with access to entity networks and facilities, and flowing to access to individual BES Cyber System

#	Organization	Yes or No	Question 22 Comment
			components. The revocation of the individual's access to entity networks and facilities should be referenced or defined as accomplishing the desired result. This effectively removes the individual's ability to access any BES Cyber Systems and allows for the timely execution to approach the "immediate" completion as defined in Table R9.â€,This item should also reference upstream requirements to grant access at either the BES Cyber System level or the BES Cyber System Component level. What level of documentation is required for access rights?â€,Transmission Faciltities' IEDs (such as protective relays) utilitze shared passwords as the method of access control. What are the expectations regarding R9 - Access Revocations for those BES Cyber System Components? Are the expectations to change every IED shared password the user being revoked had access to in every High and Medium BES Transmission Facilities within 72hrs? This task of changing hundreds of protective relay passwords within 72hrs is currently not operationally feasible.R9 - indicates that NERC CIP password schemes will be applied to all units. Many systems with passwords have never had a password change.Large volume to manage. Control systems were not designed to have password changed regularly.When we implemented the NERC rules on the Load Control Computers in December, we found that they wouldn't run properly without the administrator password from when the software was originally installed. On one machine, we ended up having to reload the software to get it to work againThe OPC connections between the Toshiba ST and Ovation systems are the same way, they will only work with the logon credentials from the original software loading and configuration.NextEra suggests not requiring changes for legacy systems with embedded passwords.
22.36	PacifiCorp	Disagree	Per question 15 above, PacifiCorp believes revocation when access is no longer needed should be consistent among the different types of facilities. Specifically, R9.2 should be merged with both R9.3 and R9.4 resulting in a consistent 72-hour requirement.Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems.

#	Organization	Yes or No	Question 22 Comment
22.37	American Transmission Company	Disagree	Propose maintaining time frame in 24 hour increments. Revocation for Medium impact should be revised from 36 hours to 48 hours.
22.38	Southern Company	Disagree	R9 should be modified to make it clear that the goal is effective removal of access - for example, that can be accomplished through revocation of physical access and revocation of network access without action at the individual BES Cyber System Component level.Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.An unachievably short time limit for revocation due to dismissal for cause will actually result in damaging security as Entities are forced to delay dismissal until revocation can be accomplished in order to maintain compliance.Requiring that an Entity monitor the employment status of its contracting companies' employees creates an impossible burden. The requirement should be modified to require removal of access within a given number of hours after notification by the contracting company, combined with requirements that communication requirements are to be given to the contracting company.
22.39	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
22.40	Detroit Edison	Disagree	R9 uses the term "system access" while in other places the term is "authorized electronic access". Table entries 9.2, 9.3 and 9.4 should address the concept of expired PRA and/or training requirements. Propose changing to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."
22.41	Ameren	Disagree	R9.2, R9.3, and R9.4 - The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.

#	Organization	Yes or No	Question 22 Comment
22.42	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
22.43	ERCOT ISO	Disagree	Recommend: "Each Responsible Entity shall revoke the ability to access its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Requirements should be revised to address primary and secondary access. Primary access being access to electronic and physical security perimeters (i.e., domain, remote access, badge access). Secondary access being access to assets within the protection of the primary access means (i.e., applications, databases, internal doors within facilities). The timelines listed in 9.1 - 9.4 are acceptable for primary access. Secondary access should allow a more reasonable timeframe. This also needs to address situations where a person may have access to a shared account that would require an outage to change the password. Doing this in a rushed manner would pose a risk to the BES Cyber System and to reliability. Access revocation should be consistent with R5. Recommend SDT consider language addressing access for system administrators and others with high risk access privileges.
22.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.

#	Organization	Yes or No	Question 22 Comment
22.45	Hydro One	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. We suggest removing requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.46	Northeast Power Coordinating Council	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.47	Exelon Corporation	Disagree	Requirements 9.2, 9.3 and 9.4 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? Exelon’s position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
22.48	Progress Energy (non-Nuclear)	Disagree	Revoking access within 24 hours will most likely require a special procedure. Revocation of access within a ‘hours’ timeframe implies that the access would be controlled through a security group with 24/7 coverage.Generation subsystems are much less sensitive than any of the control center subsystems. Leave this at 168 hours revocation other than for cause.
22.49	Southern California Edison Company	Disagree	SCE does not feel that reliability is served by imposing a 36 hour revocation for medium impact systems in a control center, and does not see any great distinction

#	Organization	Yes or No	Question 22 Comment
			between medium impact in transmission, generation, or a control center - these should all use a 72 hour timeframe. The timeframe for revocation of access to servers, applications, systems, sensitive information, relays, and equipment, etc. within a physically controlled area should be longer (e.g. 7 days). SCE also requests clarification on what devices must be revoked. The standard does not clarify what immediate revocation of access is - be it access to the "front gate" of an electronic and/or physical boundary versus the revocation of access to each "door" to every system and or component. As such, the potential scope of system access under R9.1 is unclear. SCE Recommends the drafting team revise this so that there is a single requirement for access revocation that and have it sub-divided into sections for physical, electronic, and information artifacts.
22.50	SCE&G	Disagree	SDT needs to consider utilizing the layers of access control leveraged by the exisiting standards here to meet the FERC mandate. Consider allowing entities to revoke access at the firewall level or password level within the timeframes suggested, and then give entites additional time to remove access at all of the other access control layers.
22.51	Florida Municipal Power Agency	Disagree	See comments to Question 19.In 9.2, 9.3 and 9.4 "who no longer require" is an ambiguous term separate from a more defined process of "granting" or "authorizing" access. FMPA suggests: "For personnel who have changed job responsibilities such that authorized access ... is no longer justified".9.3 and 9.4 can be combined into "non-Control Center BES Cyber Systems"
22.52	Liberty Electric Power, LLC	Disagree	See R5 comments on the short times to revoke access. It should be "next business day", not 24 hours in most cases. Further, it should be clear that revoking physical access to an entire facility would serve to revoke physical access to a secure are within the facility.
22.53	Constellation Power	Disagree	Some systems have a single username and password (shared), so when an employee is terminated, is the expectation that every component (such as a similar relay used

#	Organization	Yes or No	Question 22 Comment
	Source Generation		all over the system) have their shared passwords changed? A suggestion would be to allow physical revocation of access in these instances to trump cyber access. R9.4 should state “Generation” with a capital ‘G’ instead of “generation.”
22.54	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
22.55	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	The 24 hour requirement of 9.1 will be particularly burdensome for small entities that do not have 24/7 dispatch. While terminations can and should happen after hours when the situation calls for it, those who can revoke access may not necessarily be available. The unintended consequence may be a needed termination being delayed. Another fix would be to increase the number of those able to revoke access, but this may create more problems than it solves.
22.56	San Diego Gas and Electric Co.	Disagree	The access revocation timeframes listed for R9.2 - R9.4 should be consistent, since there is not a significant enough difference in risk between the three requirements warranting different time-periods. R9.4 is contradictory with R9.2 if, by the proposed definition of Control Center, a BES Cyber System controls two or more generation facilities or transmission facilities.SDG&E believes that the requirements in Table R9 should include language clarifying that contractors and service vendors that have access shall have that access revoked (within whatever time frame is appropriate) once the RE is notified by the contactor/service vendor of a contractor/service vendor’s termination. The RE cannot and should not be held responsible for the lack of timely notifications of termination of contractor/service vendor personnel from a contractor/service vendor company. In other words if a contractor were to terminate someone on 1/1/XX and they do not notify the RE until 1/3/XX, the RE should not have to be held to a revocation time period that ends sometime on 1/2/XX.
22.57	Seattle City Light	Disagree	The most mature user provisioning systems with effective processes would unlikely meet the parameters in this requirement. As a result, utilities will modify their

#	Organization	Yes or No	Question 22 Comment
			organizational processes to redefine when "access is no longer needed." For example, rather than submitting a request to remove user access after termination, utilities will await completion of the revocation request before officially terminating employment. This would make the requirement ineffective in accomplishing it's intent.
22.58	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The requirement should refer to electronic access, not just system access. The 36/72 hour requirement to remove access for routine changes is overly confining, as detailed in the answer to Question 16. Table 5 Part 5.7-5.9 also refer to timeliness of revocation. Twenty-four hours for terminations for cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8, 5.9, 9.2, 9.3 and 9.4, the 36/72 hour requirement to remove access for routine changes is overly confining. We suggest that routine revocation be accomplished within 5 business or 5 calendar days.
22.59	Northeast Utilities	Disagree	The table must be simplified; making a distinction by type of asset only increases risk of non-compliance. For personnel terminated not for cause why not make them all the same?
22.60	FirstEnergy Corporation	Disagree	There is much emphasis in properly categorizing facilities in Attachment II but that information seems to disregarded in information presented in Table 9 of CIP-011. If different timeframes for revoking access is warranted then it should be bases on Low-Medium-High impact - its unclear why a control center and generation/transmission facility is treated differently if each are deemed High Impact. This seems to be an issue in multiple tables dealing with revocation of access privileges - logical and

#	Organization	Yes or No	Question 22 Comment
			physical.Consider replacing 9.2, 9.3 and 9.4 with one row that say 'BES Cyber Systems' with appropriate timeframes for Low, Medium and High impact if needed. However, FE believes the R9.2, R9.3, R9.4, 36 and 72 hours is too restrictive and would like it to remain at the Version 2/3 timeframe of 7 days. To simplify, we recommend consistent revocation of all employees regardless of impact level. In practice most entities will likely implement consistently throughout their organization to the most restrictive requirement. Therefore, not sure the H/M/L levels has a practical use in this situation due to an administrative burden to implement and track differing time periods.
22.61	Powersouth Energy Cooperative	Disagree	This will be greatly affected by the ability to revoke access by account management at the gateway to the cyber system versus the changing of each component that makes up the system. Password/account management on systems such as relays that don't allow individual user accounts will be extremely complicated and time consuming. Consideration should be given to clarifying if managing access at the gateway and revoking physical access is sufficient, especially for low impact systems.
22.62	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Time frames for 9.2 to 9.4 should be extended to 72 hours or next business day, whichever is longer.
22.63	USACE - Omaha Anchor	Disagree	Timelines are unreasonable for removal of electronic access - we do not have 24/7 coverage for revocation of electronic access. Revocation of physical access should be allowed for this section. If they don't have physical access - they can't access the electronic access. Electronic access removal should then be changed to two business days or next business day.
22.64	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 22 Comment
22.65	We Energies	Disagree	We Energies agrees with EEI. It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.66	GTC & GSOC	Disagree	We recommend changing this to "36 hours or 1 business day, whichever is greater".
22.67	GE Energy	Disagree	Why introduce a time interval not based on a day? 36 hours may as well be 48 hours.Time periods should be specific to business days and take into account weekends.
22.68	APPA Task Force	Disagree	With physical access control as covered in R5 and remote access control as covered in R13, the greatest risk to the BES is presented by employees and contractors who have been terminated for cause. We therefore recommend the following conforming changes should be made to R9 Table 9.2 - 9.4: R9 Table 9.1: For personnel terminated for cause. Low, Medium and High Impact: "24 hours".APPA recommends elsewhere in these comments that (i) all impact levels have physical access controls in R5 Table 5.1, (ii) requirements in R5 Table 5.7-5.9 be removed, and (iii) requirement R10 Table 10.2 be edited to require passwords to be changed annually, If these comments to the drafting are accepted, the risk of malicious operations is minimal. We therefore recommend the following conforming changes be made to R9 Table 9.2-9.4:R9 Table 9.2: For personnel and others previously granted unescorted access who no longer require such access to Control Center BES Cyber Systems. R9 Table 9.3: For personnel and others previously granted unescorted access who no longer require such access to Transmission BES Cyber Systems. R9 Table 9.4: For personnel and others previously granted unescorted access who no longer require such access to Generation BES

#	Organization	Yes or No	Question 22 Comment
			Cyber Systems.

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6.

Commenters expressed concern that Table R9 is inconsistent with Table R8 for Low Impact BES Cyber Systems, as there should be no requirement to revoke access if there is no requirement to authorize it. In addition, many commenters raised concerns about entities being able to meet proposed revocation times, especially for Low Impact BES Cyber Systems due to the expected large numbers of such systems. The SDT agrees with these concerns, and the requirements for revocation of access for Low Impact BES Cyber Systems have been removed.

#	Organization	Yes or No	Question 23 Comment
23.1	BCTC		Â Recommend collapsing requirements 9.1 to 9.3 into one requirement.Â The time requirements for the one requirement are recommended to be:Â Medium Impact - within 72 hoursÂ High Impact - within 24 hours
23.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
23.3	Florida Municipal Power Agency	Agree	See comments to Questions 19 and 22. Also consider adding “Required for remote access or routable external connectivity only” to Medium and Lower Impact. Lower Impact should be not applicable for 9.1 to be consistent with 5.7. Also, for Medium Impact, 9.1 and 5.7 ought to be consistent.
23.4	Bonneville Power Administration	Agree	The table should refer to electronic access, not system access. The revocation time frames should be adjusted, as discussed above.
23.5	E.ON U.S.	Disagree	: CIP-011-1, R9 has stringent commitments for Low Impact and Medium Impact BES Cyber Systems. E ON U.S. proposes that these time requirements be extended. It is

#	Organization	Yes or No	Question 23 Comment
			not a hard and fast rule as to when employees no longer requires access to 9.4 cyber systems. This is particularly true when an employee is moving to another position within the Company and a certain amount of training is required to backfill their position. Three days does not allow time for that situation. A monthly or quarterly time frame would be adequate in most instances.
23.6	Network & Security Technologies Inc	Disagree	9.1 - Access to Low Impact systems needs to have been explicitly granted (8.1) or at least documented (7.1??) in order to be revoked (consistency issue - also see comments on Question 16).
23.7	Consultant	Disagree	9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.
23.8	Detroit Edison	Disagree	9.1 requires access revocation for Low Impact but there is no requirement to specifically authorize access for Low Impact.
23.9	American Electric Power	Disagree	9.1, Column "Low Impact BES Cyber System", regarding "Within 24 hours". There is no requirement to formally request, authorize, or review access to low impact BES Cyber Systems. How would it be possible to effectively remove that access?
23.10	Constellation Energy Commodities Group Inc.	Disagree	Align time requirement for 9.2 with the other 9.3 and 9.4 (all at 72 hours) to eliminate confusion.
23.11	Oncor Electric Delivery	Disagree	As stated earlier, depending on the type of communication to Cyber Systems, it may

#	Organization	Yes or No	Question 23 Comment
	LLC		not be possible to comply with these requirements due to communication failures. This requirement is particularly burdensome as it applies to contractors and service vendors. Many entities have resorted to weekly verification with their contractors/vendors to verify this requirement. A 24-36 hour requirement, other than "for cause", is not practical.
23.12	Northeast Power Coordinating Council	Disagree	Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.13	USACE - Omaha Anchor	Disagree	Believe revocation of physical access should be adequate for this standard - if that were so timelines and impact levels would be acceptable.
23.14	ReliabilityFirst Staff	Disagree	By not specifying a time for revocation of access for low impact assets, the requirement will not be enforceable for these assets. Suggest something like 30 or 90 calendar days for Low Impact BES Cyber System for 9.2, 9.3 and 9.4.
23.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
23.16	BGE	Disagree	Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent. Can the drafting team declare why the time elements were changed from 1 week to 36 or 72 hours?
23.17	The Empire District Electric Company	Disagree	Comments: For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement

#	Organization	Yes or No	Question 23 Comment
			should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.18	Exelon Corporation	Disagree	Does this apply to protective relays, even if there is no external access? If so, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
23.19	Allegheny Energy Supply	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.20	Allegheny Power	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.21	San Diego Gas and Electric Co.	Disagree	Even though the compliance timeframes are reasonable in Table R9, two versus three timeframes are preferred. SDG&E believes that the control center timeframe (36 hours) should also be 72 hours, like R9.3 and R9.4.
23.22	USACE HQ	Disagree	First, requirements 9.1, 9.2, 9.3, and 9.4 should be required for every level of impact. Second, to avoid the "Friday 5PM termination with cause" scenario, the language should be change as follow: 9.1, from "within 24 hours" to "Close of Business Day (COB) of the following day after the termination", 9.2 from "within 36 hours" to "Close of Business Day (COB) of the second day after access is no longer required", and 9.3 and 9.4 from "within 72 hours" to "Close of Business Day (COB) of the third day after access is no longer required", OR if requirements 9.2 - 9.4 are collapsed into one requirement (please refer to my answer to previous question) from "within XX

#	Organization	Yes or No	Question 23 Comment
			hours" to "Close of Business Day (COB) of the third day after access is no longer required".
23.23	MRO's NERC Standards Review Subcommittee	Disagree	For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.24	American Transmission Company	Disagree	For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.25	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
23.26	APPA Task Force	Disagree	If our comments in response to Question #22 are accepted, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access). We feel for remote and unmanned BES facilities ensuring and demonstrating compliance with this requirement will be difficult if not impossible to comply with from a logistical standpoint. We also recommend the drafting team allow more time to comply with 9.3 and 9.4. We know there are pressures to have access restricted as soon as

#	Organization	Yes or No	Question 23 Comment
			possible. But there are substantial difficulties in doing so, as many systems have multiple owners, are in remote locations and have numerous devices to access. The drafting team appears to be basing its timetable on a control center environment where the cyber systems are more IT focused and have controls that can be turned on and off easily. We therefore recommend the following changes be made to the impact levels: R9 Table 9.1: Low Impact: For remote access or routable external connectivity only, 24 hoursMedium Impact: For remote access or routable external connectivity only, 24 hoursHigh Impact: 24 hours.R9 Table 9.2: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 36 hoursHigh Impact: 36 hoursR9 Table 9.3: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 weekR9 Table 9.4: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 week
23.27	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, the account revocation requirements should be required for the same levels
23.28	Manitoba Hydro	Disagree	Is 24 hours a reasonable and achievable time interval to revoke electronic access to Low Impact BES Cyber Systems? This is too short in consideration of the large number of Low Impact BES Cyber Systems.
23.29	Progress Energy (non-Nuclear)	Disagree	It seems reasonable that access for all impact levels, even low, should be revoked if and whenever it is no longer needed.The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
23.30	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
23.31	MidAmerican Energy Company	Disagree	MidAmerican Energy does not agree with the timelines specified in Table R9. See the response to question 54.

#	Organization	Yes or No	Question 23 Comment
23.32	Tenaska	Disagree	Most of these are doable on SCADA and EMS hosts only and/or ingress/egress of perimeters/boundaries.10.1 Some DCSes will not allow this for some processes to work.10.2 Same as 10.110.3 must have a way of handling old equipment.10.4 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries .10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.6 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.7 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.8 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.
23.33	National Grid	Disagree	o Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? National Grid recommends removal of this combination. o The text in 9.2/9.3/9.4 - “who no longer require such access” is vague and should be specific such as transfers, suspensions, or change in job duties.
23.34	American Municipal Power	Disagree	Please provide a little or no impact category
23.35	NextEra Energy Corporate Compliance	Disagree	Please see response to item 22. NextEra believes while it is appropriate to require access revocation requirements for Medium and High Impact BES Cyber Systems, the periods are too restrictive for personnel who transfer, or who separated from the responsible entity via normal means not for cause. NextEra does not believe that 9.1 should apply to Low Impact or No Impact BES Cyber System. In previous section, 8.1 (Authorizing Access) is not required for Low Impact BES Cyber System and the standards should be consistent.
23.36	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management and Table 9 Access Revocation. If account management is not

#	Organization	Yes or No	Question 23 Comment
			required for Low Impact BES Cyber Systems how can account access be revoked within 24 hours? Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: "Required for routable connectivity only".
23.37	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
23.38	Ameren	Disagree	R9.1 - Without accounting for who has access this will be a difficult requirement to maintain documentation for Low Impact Systems.
23.39	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
23.40	Minnesota Power	Disagree	Regarding Part 9.1, Low Impact BES Cyber Systems cannot require revocation, because creation of accounts for these was not tracked in Requirement R8.
23.41	EEI	Disagree	Regarding Table 9 Row 9.1, Effective Access to low impact systems should be removed within 24 hours for the "termination for cause" requirements See question 22 for definition of Effective Access.
23.42	Idaho Power Company	Disagree	Registered Entities will potentially have a large number of low impact systems. One individual may have access to many of the low impact systems. It may not be possible to remove the access from all of them individually within 24 hours.
23.43	Southern Company	Disagree	Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.
23.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all

#	Organization	Yes or No	Question 23 Comment
			substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.
23.45	Alberta Electric System Operator	Disagree	Revocation criteria should be specified for Low Impact BES Cyber Systems as well. The AESO suggests the following timelines in Table R9:9.1 Low, Medium, and High all Within 24 Hours9.2, 9.3 and 9.4 Low, Within 120 Hours, Medium and High, Within 72 Hours
23.46	Southern California Edison Company	Disagree	SCE does not agree with 36 hour revocation for medium impact systems in a control center, and does not see any great distinction between medium impact in transmission, generation, or a control center. These should all use 72 hour timeframe.Table R9 is that Requirements R9.3 and R9.4 are identical and can be combined. The time constraint for access revocation for low impact system as written is identical across impact levels. This does not reflect the intent of Order 706 where controls are commensurate with impact to BES reliability. The drafting team has selectively interpreted Order 706's directive for "immediate" revocation but has not given adequate consideration to the impact on BES reliability.
23.47	Alliant Energy	Disagree	See response for Question 22.
23.48	ISO New England Inc	Disagree	Since the Low Impact do not have an access control requirement, how can Low Impact have Requirement 9.1? Recommending removal of this combination.Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4

#	Organization	Yes or No	Question 23 Comment
23.49	Northeast Utilities	Disagree	Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? Recommend removal of this combination (i.e., Low Impact / For Cause).Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.50	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
23.51	Southwest Power Pool Regional Entity	Disagree	Termination of access, whether or not for cause, is a basic security control and needs to be applicable to all impact categories.
23.52	The United Illuminating Co	Disagree	The time frames should specify what T=0 is. For example, for termination for cause does the clock start with the termination, or with the notice from Human Resources.
23.53	Dairyland Power Cooperative	Disagree	There should be some time frame for revoking access to low impact systems. 30 days?
23.54	Reliability & Compliance Group	Disagree	They contradict R5.
23.55	FirstEnergy Corporation	Disagree	Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities. In practice we would likely enforce the most restrictive. As stated in our response to Question 22 the revocation times for a high or medium impact facility should not be different for control centers and other facilities - otherwise why is it "high impact"?Why is Low Impact not covered? This implies a need for a "no impact" category which we believe is warranted.

#	Organization	Yes or No	Question 23 Comment
23.56	ERCOT ISO	Disagree	Timelines should be identified for low impact systems on 9.2, 9.3, and 9.4. The current timeline of 7 days would be appropriate.
23.57	Con Edison of New York	Disagree	Timeliness of access removal is important. This criteria can be interpreted to mean (R9.1 for example) as access needs to be revoked within 24 hours of the actual time of termination for cause. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the termination within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 24 hours from notification of the termination for cause.
23.58	US Army Corps of Engineers, Omaha Distirc	Disagree	Times will be near impossible to meet for 9.1. Particularly when they cover high medium and low impact systems. Recommend that the emphasis be placed on removing remote electronic access and physical access to facilities. Time frames in terms of business days would be an improvement. 9.1 could be remove remote and physical access by next business day. 9.2 could be remove remote and physical assess within 2 business days. 9.3 & 9.4 within 3 business days. Also have concerns about meaning of "when no longer required" and how this would be tracked and audited. Example would be of an employee that leaves a job but retains system rights in order to train new person.
23.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
23.60	Hydro One	Disagree	We believe that changing passwords on non-routable devices isn't realistic and depending on final version of BES CSC list, this may even be unachievable. The standard should allow for other methods of revocation and permit appropriate implementation time.Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for

#	Organization	Yes or No	Question 23 Comment
			all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.61	We Energies	Disagree	We Energies agrees with EEI recommendation: Effective Access to low impact systems should be removed within seven calendar days.
23.62	PacifiCorp	Disagree	While we PacifiCorp agrees that terminations for cause require more immediate action to remove access than other terminations; we do not believe that normal terminations and transfers require such timeframes and believe that the current timeframes are more than adequate to ensure the safe operation of the BES. If these timeframes are unavoidable, business days should be considered as opposed to the currently proposed number of hours as this imposes significant risk to our ability todifficulty comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R10 has been moved to CIP-007-5 R5.

Some commenters expressed concern that password criteria should be provided as guidance, and that entities can increase password strength and meet security requirements without meeting all criteria for password complexity. The drafting team believes that moving all password criteria to guidance would create a significant challenge in auditing this requirement, and would lead to the continued use of Technical Feasibility Exceptions, as entities and auditors may not agree on the most appropriate password policy. However, flexibility in the periodicity of changing passwords has been incorporated in the standards, and the requirement for password complexity was modified to allow more equally effective complexity requirements to be attainable.

Other commenters expressed that Table R10 focuses only on passwords, when there are other mechanisms for authentication (such as tokens). A more flexible requirement has been added to validate credentials before granting access to BES Cyber Systems. This requirement is intended to allow for other types of authenticators.

Some commenters expressed the need to have certain password changes occur during outages, and not necessarily be time based. In response, revisions were made to the password requirements to allow an entity to consider system characteristics when developing a password policy dealing with periodicity of change.

Some commenters suggested combining the requirements R10.6 to R10.8, and they also have concerns about having multiple IDs for different systems and permission levels. In response, the requirement for administrators to have an account for privileged functions was removed because it was too prescriptive. This requirement would not be reasonable to apply on all systems.

Some commenters expressed general concern about being able to enforce the Account Access Control requirements in R10.1 to R10.5. In response, the requirements have been modified to allow for procedural enforcement mechanisms. However, the measure makes clear the challenge in auditing procedural enforcement: entities may be required to divulge their passwords prior to immediately changing them to show compliance.

Some commenters expressed that in R10.7 "explicit authorization" is not defined, and questioned how this differs from R10.8. In response, the term "explicit authorization" has been removed from the requirement. Authorization requirements have been combined

into CIP-004-5, and CIP-003-5 now addresses the delegation of authorization responsibility.. Anywhere authorization is needed in the Standards, the requirement states the authorization occurs by the "CIP Senior Manager or Delegate".

Some commenters requested that the SDT define “privileged” and “other system functions” as used in R10.8. The SDT has removed these terms from the requirements.

#	Organization	Yes or No	Question 24 Comment
24.1	National Rural Electric Cooperative Association (NRECA)		In R10.1, the wording appears to permit changing vendor passwords "anytime" after installation. Do we mean prior to installation or within some specific time after installation. Please clarigy so there is not auditor confusion on what is required here.In R10.7, what what "explicit autorization" mean? Is this different from "authorization?" If yes, please ensure the requirement is clear on what is required.
24.2	WECC		SDT should reevaluate the password complexity requirements as many systems do not support special characters but could still have strong passwords by increasing lengths or changing more frequently. Consider replacing with a requirement that passwords have a minimum bit length (which is what requiring certain lengths, and character sets is prescribing).The password requirements are too weak to be effective. Strong password construction should be required at all levels.
24.3	FEUS	Agree	Agree with comments: The drafting team should clarify when default vendor passwords must be changed after installation (10.1)
24.4	RRI Energy	Agree	Could possibly need a TFE for field installed intelligent electronic devices - meters, monitors, plcs, rtus
24.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Passwords or equivalent should not be so prescriptive and such requirements can result in many TFEs. Also, by creating onerous password requirements, it is more likely to create reliability issues in the BES by having to keep track of complicated passwords; passwords should be both reasonable and functional.The focus of the requirement should be on user accounts. “System”

#	Organization	Yes or No	Question 24 Comment
			accounts should be excluded from many of these requirements (possibly considering new requirements concerning the security of system passwords) to avoid numerous TFEs while maintaining security.User accounts should focus on the password entropy, not on the specifics of number of characters and types of characters. Password entropy is the term used in the computer industry and a much better metric for defining password complexity vs. having to give a specific length or number of characters. For instance, there are 94 ASCII printable characters as described in 10.3, 10.4 and 10.5, so, a 6 character password can have about 36 bits of password entropy. An 8 character password consisting of non-case sensitive alpha-numeric characters (36 characters) has 40 bits of entropy; more than what is described in the standard. FMPA suggests using a metric of 36 bits of entropy for medium-impact password requirements. Such a step will avoid numerous TFEs for older equipment that cannot handle special characters, but can handle longer passwords for instance. FMPA suggests using the NIST's Electronic Authentication Guideline as a baseline for the standard. A copy can be found at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdfA password's information entropy can be expressed by the formula: where N is the number of possible symbols and L is the number of symbols in the password. The function log2 is the base-2 logarithm. H is measured in bits. (See Appendix A in NIST Electronic Authentication Guide referenced above for more detailed information).Even these simple requirements will not pose much of a threat to automated attack which is why these requirements must work together in order to best secure the BES. If securing the BES is the objective, passwords alone are not enough to secure devices; they must be accompanied by logging and alerting systems to ensure industry best practices. For example, a 56-bit password could be cracked in under a day with specialized hardware. A 72-bit password would take over 1,000 years to crack, while 128 bit passwords are currently considered uncrackable by brute force. A 22-character alpha-numeric password has entropy of 128 bits.Footnote 1 is unnecessarily onerous, e.g, if a device cannot support special characters or case sensitivity, but does support 32 character passwords, then the footnote would require use of all 32 characters with around 180 bits of entropy.Also, the focus on passwords

#	Organization	Yes or No	Question 24 Comment
			excludes other, even more secure tools, such as multifactor authentication, that ought to be accounted for.10.1 and 10.2 can be combined “Passwords much be changed upon installation and at least once every twelve months”On bullet 10.6 the wording “the minimum necessary to perform work functions.” is subjective and difficult to measure. We propose this be replaced with “in accordance with the policy required in R1.” In addition, 10.6 is account management and should be in R8, not R10.10.7 is duplicative of 8.1 and should be removed.10.8 is duplicative of requirements in R7 and R8 and should be removed or embedded within that requirement.
24.6	Green Country Energy	Agree	Guidance?
24.7	Emerson Process Management	Agree	In the popular Windows Active Directory, there is no enforcement of complying with password complexity policy. So, the policy can be set for password complexity, the user can still implement weak password without rejection.
24.8	Puget Sound Energy	Agree	Puget Sound Energy suggests including “Where Technically Feasible” to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.
24.9	Progress Energy - Nuclear Generation	Agree	R10 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
24.10	National Grid	Agree	Requirements 10.3, 10.4, and 10.5 indicate the “how” which NERC wants to move away from. Suggest moving this to the guidance document.
24.11	US Bureau of Reclamation	Agree	Row 10.4 and 10.5 would be easily reworded into a specific requirement for password construction. Also refer to question #54, comment 2.
24.12	PNGC-Cowtitz-Central	Agree	See comment for question 6.

#	Organization	Yes or No	Question 24 Comment
	Lincoln-Benton-Clallam Group		
24.13	Network & Security Technologies Inc	Agree	Suggestion offered at recent workshop to substitute “ensure authenticity” for “use passwords” has merit and should be considered.
24.14	Alberta Electric System Operator	Agree	The AESO thinks that it is impossible to guarantee a RE can “prevent malicious operation,” however the RE can “mitigate malicious operation.”Please define the term "BES Elements".We agree with the list of criteria that are included in Requirements Table R10.
24.15	Independent Electricity System Operator	Disagree	- R10.2 broaden the scope of passwords and allow for certificates, keys, etc. Some vendors deliver default certificates. In addition, keys may be used for authentication and should be changed. If using two factor or multi factor authentication it techn
24.16	LADWP	Disagree	1. The footnote [1] for CIP-011-1 R10 appears to allow entities to assess TFEs for Account Access Control / Passwords within their own judgment. I would recommend that for 10.3, 10.4, and 10.5 be replaced by footnote [1]. a. The current FERC-Approved TFE process is inefficient; the incorporation of all TFEs into their appropriate requirements should suffice the standard.
24.17	Progress Energy (non-Nuclear)	Disagree	10.1 may be better to indicate ‘upon commissioning’10.7 and 10.8 are too broadly defined to effectively control.It needs to be clarified that it is not required that each device be capable of being configured to automatically enforce authentication requirements (forcing password change, password length, password sophistication, etc.).R10.6 - Recommend clarification of language to indicate that ‘access permission are the minimum necessary to perform work functions’ means normal work functions for each particular individual. There should be no intention to require a single individual to maintain multiple logins for each function for which they are responsible (beyond an administrative login and a ‘normal functions’ login).Consider combining 10.6 and 10.8. If you meet the intent of 10.6 then you should be meeting 10.8.

#	Organization	Yes or No	Question 24 Comment
24.18	LCEC	Disagree	10.1 should be changed passwords prior to production as opposed to after installation.10.1-10.5 lead back to TFE issues. Consider applying only to interactive users.Must address current compliance challenge of requiring technical enforcement of password policies. 10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
24.19	Idaho Power Company	Disagree	10.1 should specify a period of time after installation or require it before putting it in production. As long as default passwords are changed, low impact systems should have a longer password change cycle
24.20	American Electric Power	Disagree	10.1: Regarding "Change default vendor passwords after installation", suggest using "Default vendor password shall be changed before or during commissioning", or "Change default vendor passwords". The word "after" fails to establish a time frame for the change.10.3: Regarding "Implement a password scheme that has the following attributes:[1]Minimum of six characters", and its footnote. While the footnote potentially allows for some exceptions, this could still be subject to a Technical Feasibility Exception (TFE) process. The TFE process is very cumbersome and provides little value. Based on the direction of CIP-010, the number of TFEs could grow exponentially.10.7: Regarding "Require explicit authorization of access to system and security administrative functions within the BES Cyber System". This seems redundant to 10.6. Would these not be granted based on job function? If not, how is it different than 10.6?10.8: Regarding "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions". What security benefit does this provide? This defeats any single sign-on functionality. To what level do you limit each account? Why are users required to have more than one account? Will they need more than 2 accounts? What is the limit?

#	Organization	Yes or No	Question 24 Comment
24.21	Dominion Resources Services, Inc.	Disagree	10.8. Some equipment does not support non-privileged accounts. A footnote similar to the one added for 10.3 to eliminate the need for a TFE should be added to 10.8.
24.22	BCTC	Disagree	Â BCTC can see the need for a TFE with requirement 10.2, 10.3, and 10.4Â Requirement 10.7 - we are uncertain as to the objective of this requirement. Does this simply require System Owner, or delegate, approval fro personnel assigned Admin accounts?Requirement 10.8 - we would appreciate some guidance on what type of evidence would be required to demonstrate compliance to this requirement. This seems very difficult to enforce.
24.23	Public Service Enterprise Group companies	Disagree	A rework of the language is needed to address the following questions to avoid confusion and misunderstanding. Please define for 10.7 what is meant by “security administrative functions” and for 10.8 what is meant by “other system functions”. Does the Operating System need automatically to check a user account against a list of “security administrative functions” before allowing access? What needs to be done if the Operating System does not have this capability? Meeting this requirement may not be technically feasible.
24.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also 10.3 - 10.8 seem to suggest technical authentication enforcement capability for all systems. Suggest softening the language to allow for administrative controls to compensate where technical controls are not possible. Also recommend verbiage that provides consideration for said technical limitations to eliminate the requirement for TFEs.
24.25	FirstEnergy Corporation	Disagree	As written, it appears that this would eliminate many TFEs and we like this change.10.4, 10.5 - Make text in table more generic - ‘implement a password scheme that utilizes as many of the four attributes as possible for the device to which the password applies’. As written, 10.5 would still mean TFE’s for any Microsoft-based authentication systems.Need to provide guidance for 2nd factor authentication (which is typically all numeric) and non-password authentication sources (e.g. smart

#	Organization	Yes or No	Question 24 Comment
			cards)
24.26	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level. Either choose a standard that is compatible with MS Windows, or explicitly state that implementing the maximum password complexity that the device supports is sufficient to meet the requirement without requiring documentation of an exception.
24.27	Liberty Electric Power, LLC	Disagree	CIP-011 R10 changing passwords every 12 months. This is a “feel good” requirement which does not advance security, but rather degrades is as the new passwords are more likely to be written down than the old passwords. The number one method of password theft is reading off a written document.The better method for password security is requiring changes "for cause".
24.28	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
24.29	GTC & GSOC	Disagree	Dictating password attributes requires a specific technology, one that is rapidly becoming obsolete. We recommend the standard should require adequate authentication measures to prevent unauthorized access to systems without specifying passwords as the method for doing so.
24.30	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned for entities without routable connectivity this requirement is overly burdensome and would require the manual resetting of passwords on thousands of remotely distributed programmable electronic devices. Emergency response would be hampered with the resulting manual password modification and management process. An unintended consequence of not excluding unconnected devices from this requirement may cause an entity to establish connectivity to meet this requirement. This potentially exposes BES cyber system to additional unnecessary security risks which should not be the intention of this requirement. Additionally, password protection may not be available on all BES Cyber

#	Organization	Yes or No	Question 24 Comment
			Systems since some may use other authentication schemes, such as digital certificates or encryption keys. TFEs may be necessary for this requirement.
24.31	Exelon Corporation	Disagree	Exelon is concerned that this will require unique identifiers and passwords for each BES Component despite the ambiguity resulting from the use of the term BES Element which could be read to mean group of components. Exelon suggests that this be limited to only those BES Components which can be remotely accessed via routable or dial-up protocol.
24.32	Constellation Power Source Generation	Disagree	For R10.1, instead of changing passwords "after installation," it should state "upon installation" in case the password is changed before physical installation. R10.2 requires passwords to be changed every 12 months, but in the case of relays for a base loaded generation facility that has planned outages every 3-5 years, this is not possible. The verbiage should add flexibility for planned outages. For R10.4, passwords are not the only way to authenticate, so requiring a password scheme is troublesome.
24.33	Southwest Power Pool Regional Entity	Disagree	Ideally, require user authentication before granting access without prescribing any particular technology. For the requirements specific to password management, add "if used" to the requirement. As written, R10 can be read to mandate the use of passwords. 10.3: Longer is better, especially for administratively privileged accounts. Require 10 or more characters for administratively privileged accounts and at least 8 characters for less-privileged accounts. Where the BES Cyber System Component cannot support the defined length, mandate the maximum password length supported. 10.4 and 10.5: Instead of defining the complexity characteristic, require complex passwords as enforced by the BES Cyber System Component's operating system. 10.7: Define what "explicit authorization" means and clarify if for all types of access or only interactive access. 10.8: Consider rewording the requirement to read "Require users of security administrative accounts to use non-privileged accounts when performing non-administrative functions on BES Cyber Systems."

#	Organization	Yes or No	Question 24 Comment
24.34	Detroit Edison	Disagree	In 10.1 the term “after installation” is vague. Change the sentence to “Change default vendor passwords prior to putting any BES Cyber System Component in service”.In 10.2 change 12 months to “at least once per calendar year, not to exceed 14 months between instances”
24.35	San Diego Gas and Electric Co.	Disagree	In Table R10, Requirement 10.5, SDG&E believes that passwords for high impact systems should be longer, not necessarily more complex. We recommend that high impact system passwords be a minimum of 10 characters. Complexity requirements should be the same for high and medium systems (SDG&E recommends 10.4).Certain legacy devices won’t be able to comply with these password requirements as listed (such as substation serially connected relays), so TFEs may be required for some of these Requirements in CIP-011.The drafting team also may want to consider changing R10 to include other technologies for controlling access besides passwords, such as special locks, biometric devices, etc.
24.36	Hydro One	Disagree	In the case of R10.2 we believe that the change of passwords every 12 months for all three categories would be very difficult to implement and would not provide increased benefit to the overall reliability of the BES. Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the “minimum” will make 10.6 difficult to audit (refer to the response to Question 54).
24.37	Minnesota Power	Disagree	Is it the Standards Drafting Teams intent that Part 10.7 of Table R10 requires explicit approval for every login to system or security administrative accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power believes that the intent of authorizing access privileges is adequately covered by Requirement R8, subject to the comments made in Question 20.
24.38	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 24 Comment
24.39	Pacific Gas & Electric Company	Disagree	Need to consider physical security interaction with “cyber” security. An example is a substation control panel (handles, etc, which you can physically operate various devices in a sub) that is physically co-located with electronic devices that perform the same functions. In this case “electronic access control” for local access to should not be required.
24.40	NextEra Energy Corporate Compliance	Disagree	NextEra comments that in reference to the footnote regarding the situation where the "device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support", isn’t this better presented for the Responsible Entitiy to have a mechanism to file for a TFE or any other exception process proscribed by the Standards?Regarding 10.8, what is the expected documentation and/or account management access control actions to demonstrate requiring users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions?Regarding R10.2, how are BES Cyber Systems not capable of technically enforcing password changes handled? Are procedural controls sufficient to meet this requirement?Additionally, how could one demonstrate compliance with R10.2 if the BES Cyber System Component is not capable of logging when the password was last changed (e.g. protective relays)?Requirement 10.2 time requirement for changing passwords at least once every 12 months does not take into account or include verbiage for legacy systems that do not have the functionality to change passwords, Is there an opportunity for an exception with evidence from the BES Cyber System component manufacturer? There should also be verbiage included in the requirement for exceptions related to BES Cyber system components that passwords cannot be changed due to operational and reliability impacts to the BES. For requirements 10.3 - 10.5, it is unclear how responsible entities document implementing the password scheme requirements. Does the responsible entity comply with having a policy that indicates the necessary requirements or is it necessary that these requirements are enforced technically by the BES Cyber System component? It is recommended that these requirements are satisfied by policies

#	Organization	Yes or No	Question 24 Comment
			instituted by the Responsible Entities and the verbiage indicates that the requirements do not have to be technically enforced. Another recommendation is that there are allowable exceptions to this requirement if a BES Cyber System component cannot technically enforce the requirements, since there are a number of legacy systems that cannot enforce this requirement.For requirement 10.6, there needs to be direction on documenting how access permissions are the minimum necessary to perform work functions. A recommended approach should indicate that the responsible entities administer policies requiring the concept of least privilege concerning their role-based access control administration. Lastly, it is unclear how requirements 10.7 and 10.8 differ from requirement 8.1, since authorization of adding account and subsequent access has to be included in a process based on the requirement. Requirements 10.7 and 10.8 should be moved to 8.X requirements section and clarification should be made as to what explicit authorization means. Is this authorization required each time a user has to access system and security administrative functions? In addition, how is the Responsible Entity supposed to demonstrate compliance to 10.7 and 10.8?
24.41	Southern Company	Disagree	Password requirements written to the level specified in R10.3 through R10.5 have proven unworkable in past versions of the standard. What should be included is only a requirement for strong authentication measures so that alternative, possibly superior, technology is not disallowed.
24.42	Platte River Power Authority	Disagree	Question:Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions What is meant by “other system functions”? What if the “other system functions” require a privileged account?
24.43	Consultant	Disagree	R10 (and others) Suggest the wording "to prevent malicious operation of BES Elements by maintaining control of access to its ES Cyber Systems." be modified to remove the phrase "to maintain control of access to its ES Cyber Systems." Account management and access control do not prevent malicious operation. The objective of

#	Organization	Yes or No	Question 24 Comment
			the standard is to prevent malicious operation, but the requirements control access (in this group), which is only one of the actions required by the standards "to prevent malicious operation."Table R10 - Items 10.3, 10.4, and 10.5 - These are statements of "How To" regarding technical implementation and should be changed to be a "What" requirement by using the words from the footnote: "implement the maximum password complexity that the device can support."Suggest items 10.6 & 10.7 be moved to the table R8, as these statements regard account management rather than access control.Item 10.8 This item should be removed. "Non-privileged account" is not an account type required by R7, and is a subjective term. "other system functions" is not defined and is also a subjective term. "security administrative accounts" is not a defined term. This statement uses multiple undefined and subjective terms and does not establish a requirement that can be implemented or audited.
24.44	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R10. System functionality and capabilities may not allow an entity to meet this requirement. Will there be language added to relieve this requirement if the system is not capable? R10.8 should contain language specifying that it applies to other system functions that do not require system level access.
24.45	Con Edison of New York	Disagree	R10.1 Changing passwords on equipment that are not networked, such as relays, is very labor intense. This activity and will be a year-long job because by the time you finish, you will need to go back to the first relays and start changing those again. The requirement to change these passwords on a yearly basis should be on systems that are networked. There must be a lower level requirement on the non-networked equipment.R10.6 Some system may not technically have the ability to perform this function.R10.8 The purpose of this requirement is not clear.R10.7 requires “explicit” authorization. This requirement should allow for specific personnel designation to be authorized for access and not require it be by name. For example LAN administrators by job definition should be able to be authorized for a specific level of access.R10.8 requires LAN administrators to log in differently if they do not need full access for the current task. This can be enforced procedurally although there should be no expectation that this can be documented to show that in each case the correct login

#	Organization	Yes or No	Question 24 Comment
			was used.R10.8 - Impossible to verify compliance or audit this, should be removed
24.46	Kansas City Power & Light	Disagree	R10.8 is unmanageable in the “windows” world. These requirements are too prescriptive and consideration should be given toward what needs to be accomplished and less on how to accomplish it.
24.47	Western Area Power Administration	Disagree	R10: Biometric and token-based factors not addressed. They need to be. R10.3 - Suggest combining 10.3 & 10.5 to number 10.3 with a 10.3.1 & 10.3.2. R10.4 - Delete 10.4 & just use 10.5 for both Medium & High.R10.4 - Are there exceptions for any equipment that doesn’t handle special characters?R10.5 - Are there exceptions for any equipment that doesn’t handle special characters?
24.48	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2Concerned that 10.6 will be hard to audit, should be a policy statement and included in R1. There is no clear way to audit this requirement and is open to auditor interpretation. This can be easy to audit if an administrator has admin access everywhere or a dispatcher has admin access in the application as well as components. But really an auditor’s opinion may differ from BES cyber system’s owner.R10.8 Should be a policy statement and included in R1. There is no clear way to audit this requirement. How is this going to be audited? Whether a user has two accounts?R10.7 Please explain “explicit” authorization, versus authorization? They seem to be the same why the emphasis.
24.49	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the “minimum” will make 10.6 difficult to audit (refer to the response to Question 54).
24.50	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value.

#	Organization	Yes or No	Question 24 Comment
24.51	Northeast Utilities	Disagree	Regarding 10.4 and 10.5 - Most, if not all, security software can not make the distinction to this level of detail nor can it be effectively monitored manually. Recommend that the criteria MS Windows defines today for password complexity is used. Additionally, trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
24.52	EEI	Disagree	Regarding Table R10 Row 10.1:Default vendor passwords should be changed before or during commissioning for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.53	Allegheny Energy Supply	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)This should also include the ability to provide alternatives such as 2 factor authentication where all the types of characters for a single password may not be possible.Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.54	Allegheny Power	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative

#	Organization	Yes or No	Question 24 Comment
			functions" means. Moreover, it appears duplicative of requirement 10.6.
24.55	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms.
24.56	Duke Energy	Disagree	Requirement 10.1: Passwords should be changed BEFORE making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Nuclear plants are on an 18 month fuel cycle. Some are moving to a 24 months. Ideally, systems would be started up at the end of a refueling outage and not touched, save for required maintenance activities until the beginning of the next refueling outage. If the maintenance activity didn't require electronic access, then having each technician/engineer/operator go to the device and change their user specific password on a 12 month basis is actually adding more risk to the BES. Alternate controls can be just as effective with less risk - for instance, installing a stand-alone (e.g. not network/serial/wireless connected) device located in a locked/alarmed cabinet. Is there any allowance for such an alternate control? Also, can this requirement be lessened for low impact systems?10.3 State that multi factor token may be used in place of password.Requirement 10.6: Require that authorized access permissions are the minimum necessary to perform work functions. This applies to user permissions as opposed to administrator functions, correct? Administrator privileges typically include all permissions.
24.57	Nuclear Energy Institute	Disagree	Requirement 10.1: Passwords should be changed before making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Frequencies for all requirements should be defined by the Entity, and not defined in these Standards. If a time must be specified in the Standard, then a process must exist for the frequency to be tailored to meet operational requirements.
24.58	USACE HQ	Disagree	Requirement 10.3 should include the language in the footnote to make it clear that

#	Organization	Yes or No	Question 24 Comment
			that is an option under the standard.
24.59	Garland Power and Light	Disagree	Requirement R10 - Paragraph needs to state that a policy or procedure requiring password length, complexity, and password changes are adequate and do not need to be technically enforced by the device.
24.60	Oncor Electric Delivery LLC	Disagree	Requirements 10.5 and 10.7 cannot be applied to all legacy systems currently in-service as they do not support account management. These should allow for TFE. Mandated password change should only be on High impact systems with routable/dial-up communications.
24.61	Xcel Energy	Disagree	Since not all deices are capable of supporting these password requirements, this is an area where TFE need to be allowed. We are concerned with Requirement 10.2 to change passwords every 12 months. For substation devices this would a significant burden, especially for low and medium impact systems.
24.62	ERCOT ISO	Disagree	Since the purpose of this is basically the same as the previous requirements, these could all be combined into a single requirement. 10.1: Recommend specifying a time-frame for changing passwords. 10.2-10.5: Recommend that the requirements address the use of alternate authentication means, such as biometrics and RSA SecurID. TFEs should be allowed for the requirements under this section.
24.63	MidAmerican Energy Company	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
24.64	Ameren	Disagree	Suggest changing R10.1, R10.2, and R10.3 for Low Impact BES Cyber System requirement to “Required, unless system is behind a firewall or other protective measures.” Giving password strength criteria is too specific when entities may use

#	Organization	Yes or No	Question 24 Comment
			other ways to implement security that meet or exceed this requirement. The manpower necessity for changing passwords yearly and maintaining a protected/immediately accessible database to store passwords so that those who need to access relays can when needed for Low Impact Systems is not needed. If all the High Impact System relays have firewall protection that should be enough. The industry needs to be able to access relays to keep the BES system functional and respond to operational issues. Also, for R10.1 need to clarify how long after installation should a vendor password be changed.â€,â€,R10.4 and R10.5 - These requirements will be difficult to prove in an audit. Should be changed to provide a documented process should be sufficient and should be less trouble in dealing with an audit on these requirements. However, some systems may not be able to adhere to these policies, and TFE's may be required.R10.6 - Documentation of the permission check will be volumes of data that will have to be performed in the audit. This requirement needs a periodic review time associated with it.R10.7 - What is the intention of this requirement? If all access is already accounted for in R10.6 isn't this requirement duplicate effort?
24.65	Entergy	Disagree	Suggest simplifying requirements 10.4 and 10.5 by combining and rewriting into: “Implement a password scheme that cannot be found in the dictionary and has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)”Requirement 10.8 should be reviewed from a technology perspective. While use of a “normal” user account and gaining “root” access through “sudo” is robust in the UNIX variant operating systems, performing the same function in the Windows operating system can be problematic with logging in as a different user all together. Suggest possibly relaxing this requirement.
24.66	ReliabilityFirst Staff	Disagree	Table R10; row 10.2 - High Impact BES Cyber Systems should have the password changed at least every 6 months. Regarding footnote 1, for devices that are not capable of meeting the password threshold, the entity should be required to

#	Organization	Yes or No	Question 24 Comment
			document this situation, including compensating measures, for audit review.
24.67	Southern California Edison Company	Disagree	Technical capability is not a homogenous quantity in a system with diverse classes of devices and thus the ability to implement generic controls over a heterogeneous system does not always exist. A means to seek exception from the "word" of the standard, while still complying with the intent which is to clearly identify technical situations where a prescribed control, is not implementable while maintaining cyber security protections is needed. Requirements R10.4 and R10.5 are too prescriptive and do not allow registered entities to seek out alternative access authentication mechanisms. For instance, biometrics or 2-factor authentication based on numerical passwords generated by a key-based security architecture may not meet the word of the standard but go above and beyond the intent of the standard.
24.68	USACE - Omaha Anchor	Disagree	TFE will be required for this section if verbiage isn't added to address lower level machines where some items (10.7, 10.5) are not possible.
24.69	Manitoba Hydro	Disagree	The account access control requirements should be more generic and technology independent, allowing the entity to apply a variety of account access controls. If passwords are needed, Requirement R10.3 should also require some "special" characters, to the extent that the device is capable. The standard should also allow protection by layers of security, which may be provided by other methods or cyber systems.
24.70	APPA Task Force	Disagree	The APPA Task Force supports the proposal by MRO-NSRS to be more generic in the wording of the requirements in R10, to account for innovations such as biometric controls used in lieu or in conjunction with password controls.We propose the following edits to R10:R10 Table 10.1: Restrict electronic access to BES Cyber Systems through use of an electronic access control that does not use/rely on the vendor defaut password.R10 Table 10.2: Electronic access controls must be updated/modified at least once annually.Since numerous devices would be exempt from this requirement due to their inability to support password protection, the term

#	Organization	Yes or No	Question 24 Comment
			"Electronic Access Controls" should replace "Passwords". This is non-limiting and will not lock into the standard a current technology, for example, keyboard-based "password access."APPA proposes that items 10.3 - 10.5 be removed from this requirement and be submitted to the "guideline in support of the standard" drafting team to be included as a best practice for account access control. If 10.3-10.5 must remain in the requirement we recommend they be less technology-specific. We propose the following language:R10 Table 10.3: Implement a password scheme that has a minimum of six characters, or an electronic access control with an equivalent or superior technology option.R10 Table 10.4: Implement a password scheme that has at least two of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option. R10 Table 10.5: Implement a password scheme that has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option.In Table 10.6 the wording "the minimum necessary to perform work functions" is subjective and will be difficult to measure. We propose this be replaced with "Require that access permissions are in accordance with the entity access authorization policy required in R1."
24.71	Constellation Energy Control and Dispatch, LLC	Disagree	The appropraite account access control mechanisms should not be specifically defined in the Table R10.
24.72	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In today's electronic world there are many methodologies for electronic access control. Many systems now make use of multi-factor passwords, and/or biometrics. They use passwords or

#	Organization	Yes or No	Question 24 Comment
			pass-codes are randomly generated, encrypted and time sensitive. Access codes or passwords may be one time, expiring after one use, and/or after a specified time (usually 60 seconds). The systems implemented may also provide checks to insure that the passwords are not captured and hijacked. These modern methodologies are far more effective and secure than the stated requirements. This requirement is prescriptive and too specific. The way it is written it would preclude the use of modern and stronger tools because they may technically not meet one or more of the specifications, even though they are bigger, better and stronger. If the requirements must remain this prescriptive, then the following changes should be made:- There should be a second footnote, "Stronger methods, such as multi-factor authentication of one-time passwords, may be used in lieu of username/password combinations."- 10.1: A time frame for "after installation" needs to be specified.- 10.3: Given the efficacy and availability of Rainbow Tables, a 6-character password is woefully inadequate. The minimum should be at least 10, and 14 would be better. - 10.6: There's a difference between "minimum necessary" and "minimum practical and necessary". Strict interpretation would require that access grants would change depending on the task being performed, which is probably not the intent. Suggest the wording be changed as described. An alternative would be to use the NIST definition of "Least Privileges - The security objective of granting users only those accesses they need to perform their official duties" (NIST IR 7298 - NIST Glossary of Key Information Security Terms) and then require the use of Least Privileges.Item 10.2 in Table R10 states that “/p/asswords must be changed at least once every 12 months”. Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently passwords must be changed.
24.73	Reliability & Compliance Group	Disagree	This requirement does not consider the use of biometric access systems such as finger print readers that could be used in place of password verification.Also, it should include the word “electronic” when it talks about “maintaining control of access to its BES Cyber Systems.”

#	Organization	Yes or No	Question 24 Comment
24.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding footnote 1 and Table R10 Row 10.7.
24.75	American Transmission Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.We would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here. Finally, the standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
24.76	MRO's NERC Standards Review Subcommittee	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12

#	Organization	Yes or No	Question 24 Comment
			months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.77	The Empire District Electric Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.78	We Energies	Disagree	We Energies agrees with EEI: Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.We Energies agrees with EEI: Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)We Energies agrees with EEI: Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.

#	Organization	Yes or No	Question 24 Comment
24.79	PacifiCorp	Disagree	While the criteria themselves are not onerous for the long term/future development of the systems, the fact is that current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.The standard needs to allow for non-password based authentication systems or one time passwords. Modify 10.2 through 10.5 with “or equivalent or greater authentication methods”The current password requirements in table 10 are too burdensome and unnecessary. The requirements as written are also confusing. Passwords should not be the only acceptable way to authenticate a user prior to granting access.
24.80	Luminant	Disagree	Will require TFE for some systems

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R10 moved to CIP-007-5 – Cyber Security - Systems Security Management - Requirement R5.

Commenters indicated that passwords on Low Impact BES Cyber Systems should not be subject to any periodic change as stated in Table R10 (10.2). In response, the SDT revised the password requirements, and they are not applicable for Low Impact BES Cyber Systems.

Commenters suggested a single criterion for password complexity. In other words, do not differentiate by risk level. The SDT agreed and reduced the password complexity requirement to be the same regardless of applicable risk or impact level.

#	Organization	Yes or No	Question 25 Comment
25.1	US Army Corps of Engineers	Agree	Agree with impact levels, but disagree on item Table R10, 10.8: "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions." Add to the end of the statement, if the system function does not require the use of using a privileged account.
25.2	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
25.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
25.4	US Bureau of Reclamation	Agree	Recommend we establish Requirement 10.6 for all impact levels. Also, please refer to question #54, comment 2
25.5	Southern California	Agree	Requirement 10.7 may be interpreted that access need not be denied as a default

#	Organization	Yes or No	Question 25 Comment
	Edison Company		setting. If the intent of the drafting team is a different control, the team should consider rephrasing this requirement.
25.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
25.7	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels for R10 if it is understood that a blank in the table means N/A. The APPA Task Force agrees with the MRO-NSRS proposal:"If the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems."
25.8	GTC & GSOC	Agree	We recommend 10.8 to be changed to: "Require persons to use non-privileged accounts when accessing system functions that do not require privileged accounts"
25.9	Exelon Corporation	Agree	We would suggest the password items begin with "Where passwords are utilized they must ...." These requirements should allow entities the flexibility to use other user authentication methods besides just passwords such as two factor tokens or other methods that provide even better protection than just passwords. Exelon appreciates the clarification provided in footnote #1 which has the potential to limit the number of TFEs that would be required.
25.10	Regulatory Compliance	Disagree	10.1 - 10.3 STRIKE "Required" for Low Impact10.6 - STRIKE "Required for medium impact - inconsistent with level.
25.11	LCEC	Disagree	10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
25.12	BGE	Disagree	10.2 maintain consistency for timeframes (i.e. use 12 months or annual). 10.3, 10.4

#	Organization	Yes or No	Question 25 Comment
			and 10.5 should be combined.10.6 needs a definition for “minimum”. 10.8 needs clarification for the meaning of “other system functions”.
25.13	Dominion Resources Services, Inc.	Disagree	10.2. It is anticipated that there will be thousands of Low Impact devices geographically spread across a utility’s system. By definition these devices provide little risk to the BES. It is impractical from a resource perspective and unnecessary from a reliability perspective to change the passwords of low impact components every 12 months. The requirement should be removed from Low Impact.
25.14	ERCOT ISO	Disagree	10.7-10.8: Should apply to Medium Impact BES Cyber System.
25.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
25.16	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. For example, a reasonable estimate is that our Entity will have approximately 2,500 low-impact substations with an estimated 100 programmable devices in scope per substation. Without any other consideration of work required, that represents 250,000 password changes each year to be performed, tracked, and communicated. The majority of those devices have hardware override switches which disable password protection for anyone who has physical access to the device, so no reliability advantage is gained by performing the password change. This is just one example of the scope of work with little or no benefit to the BES that is required as long as there are per-component low-impact requirements.The standards should be modified so that requirements for low-impact cyber systems include only program-wide efforts such as policy, governance, incident response planning, and disaster recovery planning.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.In addition, vendor contracts with sole suppliers of necessary equipment may conflict

#	Organization	Yes or No	Question 25 Comment
			with 10.1. At the least, this creates the necessity for a large, cumbersome TFE program.In 10.1, the phrase "after installation" should be replaced by "before, during, or immediately after installation".10.4 and 10.5 create a TFE burden without any substantial benefit and disallow advanced technology that provides stronger authentication but does not meet the literal wording. Instead, the requirement should be modified to require authentication.
25.17	Tenaska	Disagree	At the end of R11 just add "identify restrictions and uses for accesses". And remove table.
25.18	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level.
25.19	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
25.20	The Empire District Electric Company	Disagree	Comments: With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, it the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.21	Southwest Power Pool	Disagree	Complex passwords and minimum password lengths are a basic security control and

#	Organization	Yes or No	Question 25 Comment
	Regional Entity		should be applicable to all impact categories.
25.22	E.ON U.S.	Disagree	E.ON U.S. does not believe a requirement is necessary for low impact items.
25.23	Consultant	Disagree	Item 10.2 - There is no requirement for account management for Low Impact assets, and it is illogical to require password controls where there are no account controls.
25.24	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
25.25	Progress Energy (non-Nuclear)	Disagree	Low impact BES systems should not have this requirement. By virtue of their definition they do not need this requirement.CIP-011 R10 - Would like to compliment the SDT for constructing a realistic and reasonable approach with regard to effective use of complex passwords. The SDT has recognized that there may be password complexity limitations with older existing electronic gear that is in operational service and rather than try to mandate a standard that is technically not feasible to implement, they have provided the footnote to require that practical password complexity should be set to the maximum that the device is capable of supporting.CIP-011 R10 - Account management access control & passwords is this meant to include BIOS or only interactive logins to devices?10.2 - “Passwords must be changed at least once every 12 months”, If this is referring to cyber system components, this represents unreasonable costs to utilities. Password changes for relays with no remote capability will be cost prohibitive, and password changes for individual relays with remote capability will require excessive time.
25.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes for Low Impact BES Cyber Systems, requiring passwords to be changed at least once every 12 months should be changed at least every 24 months; for Medium Impact BES Cyber Systems, we suggest changing passwordsat least every eighteen months.
25.27	Alberta Electric System	Disagree	Please consider the following changes to increase security and make the

#	Organization	Yes or No	Question 25 Comment
	Operator		requirements more restrictive:Table 10.2 - passwords changes at least once every three months.Table 10.3 - minimum eight character password (with same footnote)Table 10.4 - change to “three of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.5 - change to “four of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.6 - required for Low, Medium, and High impact levelsTable 10.7 - required for Medium and High impact levelsTable 10.8 - required for Medium and High impact levels
25.28	American Municipal Power	Disagree	Please provide a little or no impact category
25.29	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management, Table 9 Access Revocation, and Table 10 Account Access Controls. Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: “Required for routable connectivity only”.
25.30	Con Edison of New York	Disagree	R10.6 should not be required for medium impact
25.31	Ameren	Disagree	R10.8 - Should be added for Medium Impact Systems.
25.32	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2
25.33	Hydro One	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.We’d like to know the full meaning of “explicit authorization”. If possible please add the definition in the glossary.
25.34	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.

#	Organization	Yes or No	Question 25 Comment
25.35	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value. Similarly, 10.7 & 10.8 should also apply to medium impact systems.
25.36	Northeast Utilities	Disagree	Recommend that the 10.4 scheme (use 2 of 4) is used for both medium and high impact and that the 10.5 scheme (use 3 of 4) is eliminated. Trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
25.37	Minnesota Power	Disagree	Regarding Part 10.2, Minnesota Power believes that the requirement to change passwords for Low Impact Systems at least once every 12 months is excessive. The requirement that a Registered Entity change passwords within this time frame for all BES Cyber Systems is unnecessarily cumbersome and time consuming. In addition, the coordination that would go into making these changes is infeasible and could result in an inability to access the system. In addition, Minnesota Power recommends that the Standards Drafting Team consider adding the following qualifier to Parts 10.1 through 10.5 of Table R10:"...where passwords are used for access control."
25.38	MidAmerican Energy Company	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.39	PacifiCorp	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.40	SCE&G	Disagree	SDT should consider not requiring Low Imapct systems to have passwords changed annually. This could potentially generate a high volume of TFEs for hardcoded passwords as previously described.

#	Organization	Yes or No	Question 25 Comment
25.41	Constellation Energy Control and Dispatch, LLC	Disagree	See comment provided to question 24
25.42	LADWP	Disagree	See previous
25.43	Western Area Power Administration	Disagree	See previous
25.44	WECC	Disagree	Several of the actions should be done for low impact assets, such as “Require that authorized access permissions are the minimum necessary to perform work functions”. Consider relooking at the impact levels.The password requirements should apply to all impact levels.
25.45	Allegheny Energy Supply	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.46	Allegheny Power	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.47	EEI	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for

#	Organization	Yes or No	Question 25 Comment
			components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.
25.48	Duke Energy	Disagree	Table 10: o All of Table 10 will potentially require a TFE o 10.1 change 'after installation' to "prior to being placed in service" o Suggest all password verbiage be replaced with 'authentication method' and remove specified attributes. Otherwise TFEs will be required for 10.3-10.5. o For 10.2 change 'at least every 12 months' to 'when security conditions require' o Requirement 10.2: Can this requirement be lessened for low impact systems? o 10.8 requires multiple accounts for individuals with admin rights on individual accounts. Suggest making this applicable only for shared admin accounts or removing for Windows based systems.
25.49	ReliabilityFirst Staff	Disagree	Table R10; rows 10.7 and 10.8, should be "required" for medium Impact BES Cyber Systems.
25.50	Dairyland Power Cooperative	Disagree	The focus is entirely on passwords, but other forms of credentials can be used. For example there are certificate or key based authentication to many systems. Many vendors use default keys that need to be changed, just as default passwords. The password rules are very weak compared to common practices. This seems to be an attempt to encourage the strongest possible password on legacy components/systems, but the by-product is that this weakens the requirements for modern systems. There should be a better way to deal with legacy systems while requiring new systems to use stronger passwords.
25.51	FirstEnergy Corporation	Disagree	The impact levels are agreeable assuming the changes suggested in Q24.10.1 Vendor default passwords should be changed based upon a clear definition of "installation." Non-password authentication sources need to be addressed. Possibly combine 10.4 and 10.5, but keep the note on implementing the maximum password complexity.FE request that the "Required" shown in the Low Impact column of rows 10.2 and 10.3 be removed. Password changes to Low Impact items should not be a requirement in the standard but left as a "best practice" guideline. A requirement to annually change

#	Organization	Yes or No	Question 25 Comment
			passwords to multiple digital protection relays associated with Low Impact facilities would be extremely burdensome with little reliability improvement. Each relay would require individual attention as there is no method of globally changing all digital relay passwords. If retained, consider allowing entities to synch up the changing of passwords on these devices with their normal PRC-005 maintenance cycles.
25.52	Southwestern Power Administration	Disagree	The language in this requirement should be changed to include a broader scope of technology or to be technologically neutral so that new or emerging technology (such as biometrics) which may be more secure than passwords will still be considered as in compliance.
25.53	Entergy	Disagree	The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly “low impact” BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Suggest making password requirements for all assets meet the requirements for high assets and let foot note as written take care of the assets that are unable to meet the requirement.
25.54	American Transmission Company	Disagree	The standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
25.55	Florida Municipal Power Agency	Disagree	The table should have different levels of password entropy required for the different impact areas. For example, medium impact systems should have 40-bits of required entropy, while high impact systems should require 64-bits of entropy. Low impact may be able to get by with 32-bits of entropy.
25.56	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to Control Center Cyber Systems.
25.57	We Energies	Disagree	We Energies agrees with EEI: Sufficient Password security can be accomplished by

#	Organization	Yes or No	Question 25 Comment
			combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.58	MRO's NERC Standards Review Subcommittee	Disagree	With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, if the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.59	Emerson Process Management	Disagree	With the latest Windows OS, there is really no great difficulty of asking for complex password. This requirement can be easily applied. The only thing is enforcement. This enforcement may be retuired for high or medium impact BES Cyber Systems.

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electrnic Security Perimeters – Requirement R2. The wireless requirements have been removed.

Commenters suggested more clarity was needed in the terms "remote access" and "external connections" and "wireless". The SDT proposed the following formal definitions for additional clarity on "remote access" and "external connectivity," and removed wireless access requirements from the revised Standard.

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter*.

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: *Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.*

Commenters suggested that wireless and remote access be broken out into separate requirements. In response, the SDT notes that wireless access requirements have been removed from the Standard. There is a single requirement for Remote Access in CIP-005-5 R2.

Commenters stated that given the local definition of Remote Access, the requirements of Table 11 Row 11.2 are extremely unclear. In response, a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3.

#	Organization	Yes or No	Question 26 Comment
26.1	Regulatory Compliance	Agree	BUT:11.1 Please clarify whether these are wireless technologies within the electronic boundary or wireless technologies originating outside the electronic boundary.
26.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."shall implement the requirements ..." makes the bullets individual requirements, which FMPA does not believe what the intent of the drafting team. FMPA suggests "shall implement the security controls ..." as an alternative.Consider combining R7, R8, R11 and R12. FMPA believes the standard should be more clear as to if this is wireless connection that is under the complete control (end-to-end) of the Responsible Entity or not. There is no way an individual can ensure that their data path, once outside of their control, routes over a wireless device or not. For access that is not under the control of the RE, the standard should refer to it just as it might for any other remote access control, demanding that the data is encrypted and the end point is protected.
26.4	Progress Energy - Nuclear Generation	Agree	R11 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
26.5	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
26.6	APPA Task Force	Agree	The APPA Task Force believes disabling the wireless functionality should be an option. If the description is not changed as proposed in Question #17 then we recommend that R11 Table 11.1 should include "and/or document that the wireless functionality is disabled."

#	Organization	Yes or No	Question 26 Comment
26.7	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.It it not clear that wireless needs to be specifically addressed. It is one of many access methods that may be use. If it is to be specifically addressed, then it should be treated separately, but as a sub-class of remote access. (Even if wireless access is intended to be used for access by Entity personnel, its very nature means that access could be gained from other locations.)If it is addressed at all it should be limited to requiring adequate protection for Wireless Access Points, but not to the level of specifically prescribing the methods that need to be taken.Finally, "Wireless Access" needs to be defined. The most common usage refers to wireless local area networks under one of the 802.11 standards. But, technologies such as point-to-point communications using microwave or laser are also wireless technologies. We offer no suggestions for the definition, since we do not know the intent of the team.
26.8	Progress Energy (non-Nuclear)	Agree	We like the clarity provided by the use of the term "interactive" remote access.
26.9	Independent Electricity System Operator	Disagree	- R11 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.- R11.1 - Is this just a policy stat
26.10	BGE	Disagree	11.1 Define "wireless technology" (i.e. could implicate a cell phone). Throughout the table when "external connectivity only" is stated this can be interpreted as a connection from the DMZ or other company network.
26.11	Black Hills Corporation	Disagree	All BES systems should have should have access controls regardless of hard line /

#	Organization	Yes or No	Question 26 Comment
			remote / wireless connection.
26.12	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
26.13	Southwest Power Pool Regional Entity	Disagree	An important aspect of wireless access was overlooked. Prescribe the use of available security features on all wireless access points. If possible word the requirement to not prescribe specific characteristics of configurations (WEP versus WPA, SSID broadcast, MAC address filtering, etc.) in order to not preclude next generation technology.
26.14	Southern Company	Disagree	Better specificity is needed as to what constitutes wireless access. Is the intent limited to 802.11x access or is the intent to include all communication done without wired connectivity?R11.1 This requirement could be interpreted to include all wireless, including voice. Insert “network” prior to “technologies”.
26.15	Luminant	Disagree	Combine 11 and 12? Does this apply to a remote user that may be connected via a wireless network connection at a remote location?
26.16	CenterPoint Energy	Disagree	Disagree - For R11.1, CenterPoint Energy is not clear as to what is meant by "use restrictions". Table R11 is titled "Wireless AND Remote Electronic Assess..." but R11 states "Each Responsible Entity that allows remote OR wireless electronic access..." CenterPoint Energy suggests separating remote and wireless access requirements. CenterPoint Energy also suggests adding clarification as to type of wireless protocols that should be included.
26.17	Exelon Corporation	Disagree	Exelon feels that definition of access needs clarity. Is this meant to include “view only” access or is it limited to administrative access that allows for maintenance, trouble shooting or modification of BES Cyber Systems?
26.18	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote

#	Organization	Yes or No	Question 26 Comment
			connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.Distinction between "remote access" and "external connectivity" is not clear. More clear definitions may need to be provided. Such as, external connectivity allows for direct Internet access vs. remote connectivity allows for access from the enterprise WAN.Table 11: suggest removing 11.3 for low impact systems. No need to authorize remote access when physical or electronic access is not authorized.
26.19	Allegheny Energy Supply	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.20	Allegheny Power	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.21	EEI	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.22	Constellation Power Source Generation	Disagree	In general, Constellation Power Generation believes that wireless controls should be combined with network controls, as the same controls will be applied.
26.23	Minnesota Power	Disagree	In reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. In addition, by definition all wireless access is also remote access and this should be stated or otherwise clarified.Regarding Part 11.3 of Table

#	Organization	Yes or No	Question 26 Comment
			R11, does this require explicit approval for every remote login to BES Cyber System accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power recommends changing the language to clarify that Part 11.3 requires that a Registered Entity determine who has authorized remote access privileges.
26.24	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.
26.25	Dairyland Power Cooperative	Disagree	It is unclear if the standard wants to make a distinction between wireless and remote access, or an equivalence.
26.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
26.27	FirstEnergy Corporation	Disagree	Need clarification wireless technology (does it include Wi-Fi, Bluetooth, Routable Protocol).

#	Organization	Yes or No	Question 26 Comment
26.28	National Grid	Disagree	o National Grid recommends changing 11.1 to “Identify the use and security restrictions for wireless technologies”. Are smart phones which have wireless capabilities considered as wireless technologies? Suggest providing examples of wireless technologies in the guidance document. o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access”
26.29	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.30	Puget Sound Energy	Disagree	Puget Sound Energy requests clarity to NERC’s definition of “wireless”. If NERC means the 802.1x protocol, then it should specify that so as not to confuse entities with radio telecommunication networks and other wireless technologies.
26.31	LCEC	Disagree	R11 - Any wireless portion of a control or administrative session should be included. Remove the term remote and replace with non-console.Many issues surrounding wireless including encryption and open transport, relay communication, PLCs. Need to clearly define scope and expectations.
26.32	ISO New England Inc	Disagree	R11.1 - Is this just a policy statement and belong in R1 or does it need to be enforced and detect violations of the restrictions? How can this be audited? If there are no restrictions is this a violation?For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
26.33	Ameren	Disagree	R11.1 what is meant by "use Restrictions" does this apply to the type of device allowed to be used on wireless, of the type of use allowed on wireless technology. Please add more detail on this requirement.R11.2 and R11.3 - Does this include Serial communications such as RTU connectivity or other non-routable protocols? Please

#	Organization	Yes or No	Question 26 Comment
			add more description in these requirements.
26.34	Northeast Power Coordinating Council	Disagree	Recommend changing 11.1 to “Identify the use and security restrictions for wireless technologies”.For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
26.35	Detroit Edison	Disagree	Remove requirement 11.1. Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.
26.36	WECC	Disagree	Requirements R11 and R12 could be combined into a requirement to produce and implement a Remote Access Plan.There are no specific requirements regarding use restrictions on wireless technologies. This criterion cannot be audited.”Wireless” and “remote electronic access” are two different things and should be addressed in separate requirements.There are no specific requirements regarding remote access. These criteria cannot be audited.
26.37	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
26.38	Network & Security Technologies Inc	Disagree	Section is unclear. Is wireless an example of a technology that might be employed for remote access, or is the SDT positing other uses? Please clarify. In addition, beyond 11.3, section does not contain any explicit requirements for controlling remote access. 11.1 and, possibly, 11.2 as written would more appropriately be included in a policy (R1). Requirements in R11 should be more aimed towards enforcement of “use restrictions” and exclusion of access methods that are not explicitly allowed.

#	Organization	Yes or No	Question 26 Comment
26.39	American Electric Power	Disagree	Security controls for wireless access seem out of place in the remote access area. Wireless Access controls is a form of boundary protection for the network and should be moved to R20-R22.
26.40	Manitoba Hydro	Disagree	Since Requirement R11 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Requirement 11.3 is unclear if it refers to authorizing remote access as a design, or operational requirement, or does it refer to the authorization of user access and privileges? Please clarify.
26.41	Entergy	Disagree	Suggest breaking out wireless access from other remote access. These are two distinct technology types, and breaking out within this document the use restrictions and minimum security countermeasures (e.g., WPA, WPA2) for wireless technologies is appropriate.
26.42	Alberta Electric System Operator	Disagree	The AESO believes that wireless access and remote access should be two separate concepts.
26.43	E.ON U.S.	Disagree	The definition of remote access includes the criteria “...from a device external to the BES Cyber System . . . “ With the removal of the concepts of an electronic security perimeter, the boundaries to these systems are not clearly defined, and “external” becomes difficult to determine. It is unclear, for example, whether accessing a BES Cyber System from an internal workstation (though external to the BES Cyber System) constitutes remote access. The definitions for BES Cyber System and BES Cyber Component also do not address the concept of a perimeter.
26.44	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
26.45	Consultant	Disagree	There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic

#	Organization	Yes or No	Question 26 Comment
			access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R11. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems." Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"
26.46	Northeast Utilities	Disagree	There is not enough information provided - please specify minimum acceptable security standard allowed (i.e., two-factor, level of encryption, etc.) associated with the use of wireless technologies.
26.47	Emerson Process Management	Disagree	This is a very confusing requirement. Remote does not equal to wireless.The requirement states "allows remote OR wireless electronic access.." The table title is "Wireless AND Remote..."If a remote access is carried out through wired VPN, doesn't this table apply?Does this "remote access" only emphasize on "interactive user session?" If so, this requirement is not applicable to wireless I/O when only data are transmitted to and from BES Cyber System via wireless communications.
26.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
26.49	Hydro One	Disagree	We don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.Recommend changing 11.1 to "Identify the use and security restrictions for wireless technologies".For 11.2 and 11.3 recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to

#	Organization	Yes or No	Question 26 Comment
			"remote access".
26.50	We Energies	Disagree	We Energies agrees with EEI: Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.We Energies agrees with EEI: The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.51	RRI Energy	Disagree	While the statement 'an interactive user session with a BES Cyber System" is clear to me, examples of "interactive non-user" should be clarified so that the users of this standard know when R11 does not apply. The most common non-user interaction, I would term as "interactive application session". One prevalent wireless "interactive application session" would be a GPS antenna to time synch a cyber asset. Another example would be a wireless serial data IO application. Since these are non-user sessions, R11 does not apply.
26.52	US Army Corps of Engineers, Omaha Distirc	Disagree	Wireless and remote access should be separated.
26.53	NextEra Energy Corporate Compliance	Disagree	Wireless and remote electronic access should be two distinct and separate categories of requirements. Wireless should be defined and it should be established that the term wireless in the context of the requirements is a technology based on 802.1X. As it stands right now, wireless could additionally be considered both blue tooth and radio technologies.Moreover, interactive user session needs to be defined and clarified. It should explain if interactive includes a user session where the user only has read capabilities or if an interactive user session is only applicable when the end user had modification capabilities to the BES Cyber System component. It is unclear how requirement 11.1 adds to the reliability or security of the BES Cyber system. Are the use restrictions per user or are these network restrictions? Moreover, if a Responsible Entity's documented use restrictions are overly broad and insecure, they still comply with the requirement as is. The recommended approach should provide guidelines on acceptable means of securing wireless access to BES Cyber System

#	Organization	Yes or No	Question 26 Comment
			components.Requirement 11.2 should be modified to include the requirement for strong technical and procedural controls for remote access. Requirement 11.3 is vague and unclear as it is currently stated. A responsible entity could misinterpret the requirement for establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges to approve the initial remote access infrastructure and not approving each individual that has remote access capabilities.Requirement 11.3 should be worded to state the following, “If remote access is used and/or implemented, establish, and implement a defined process for authorizing the establishment of remote access infrastructure”NextEra suggests an additional requirement be added and stated as follows:”If remote access is used and/or implemented, establish a defined process for authorizing users to utilize remote access for unescorted interactive cyber access to BES Cyber Systems.”There are not any requirements related to logging or monitoring of remote electronic access and the current requirements within Boundary Protection (R20-R22) requirements do not address this issue either.Finally in 11.2 and 11.3, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
26.54	Platte River Power Authority	Disagree	Wireless technology shouldn’t be specifically called out in the standards. Security controls should be broad enough to cover all technologies including wireless and should be handled in their respective sections.

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electronic Security Perimeters – Requirement R2.

Commenters expressed concern that the Standards need better definitions to clarify remote access vs. external access. In response, a new requirement for Remote Access Management (CIP-005-5 R2) for Interactive Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters expressed that there should be some governance of automated data exchange with remote systems. In response, the SDT noted that automated data exchange (or data in motion) requirements are not considered within scope of this Standard.

The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.*

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 27 Comment
27.1	WECC		Consider renaming to Remote User Access since it is specific to user not other systems or machines. Move to the beginning of the standard. Don't like box in the middle of requirement.Additional language should be added to clarify what constitutes a remote interactive session.

#	Organization	Yes or No	Question 27 Comment
27.2	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
27.3	Exelon Corporation	Agree	Exelon would like clarity on whether “view only” access would be included in the definition of “interactive user session”? If the answer is no, this should be explicitly stated in the definition of remote access.
27.4	Dairyland Power Cooperative	Agree	However, there should be some governance of automated data exchange with remote systems, perhaps in another section. Also, there is no governance as to how wireless technology can be used for non-interactive data communications.
27.5	Alliant Energy	Agree	However, we recommend consideration of adding clarity to the use of the term “external” in the definition or the replacement of the word “external” with “geographically or logically separate”.
27.6	Consultant	Agree	If "wireless access" has to be specifically stated it should be included in the definition as a method of remote access.
27.7	Southern California Edison Company	Agree	Remote Access is defined without reference to boundaries, logical or physical. For example, access from any device residing in the same local area network, but not part of the BES Cyber System, can be interpreted as Remote Access.
27.8	Florida Municipal Power Agency	Agree	The review periods of the access may need to change with the different levels (12 months for low, 6 for medium, and 4 for high). The standard should require end-to-end encryption between the BES Access Point and the endpoint. Wireless should require minimum standards for 802.11 access points, such as WPA/AES encryption.
27.9	Progress Energy (non-Nuclear)	Agree	This can imply a non routable protocol since a command to open a breaker does result in an operation and provides a subsequent indication that the breaker actually

#	Organization	Yes or No	Question 27 Comment
			did open.
27.10	FirstEnergy Corporation	Agree	We agree fundamentally with the definition, but are concerned about impact to areas outside the BES Cyber System (e.g. Remote access to corporate networks bordering the BES Cyber Systems). Need clarity of "interactive user session".
27.11	Xcel Energy	Agree	We feel it would be beneficial to define the remote access point. For example, a case where a user uses a desktop VPN access to dial-up access a substation relay.
27.12	Independent Electricity System Operator	Disagree	- For 11.2 and R11.3 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
27.13	PacifiCorp	Disagree	(See comments on #13) The problem is conflicting definitions. The BES Cyber System Component definition requires that any device providing "control" of the BES Cyber System is to be considered a component of the BES Cyber System. (pg 2, Standard CIP-010-1) Yet, remote access is defined as an "interactive user session with a BES Cyber System from a device external to the BES Cyber System". (pg 12, Standard CIP-011-1)In short, all devices providing 'control' must be considered "BES Cyber System Components", which corresponds to 'internal access'. This definition eliminates remote access that provides control, because the provided function of 'control' requires reclassification as 'internal'.
27.14	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined. Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.

#	Organization	Yes or No	Question 27 Comment
27.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
27.17	The Empire District Electric Company	Disagree	Comments: As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.18	Luminant	Disagree	Controls for Remote access should include only the machines that have direct acces.
27.19	Network & Security Technologies Inc	Disagree	Current definition suffers from inadequacy of the definition of "external connectivity." As suggested in our response to Question 13, we think the definition might be helped by recasting it as meaning interactive access to a BES Cyber System from "outside" an electronic boundary such as an ESP.
27.20	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned this definition would apply to laptop computers used to perform maintenance on programmable electronic devices and believes that a temporary laptop connection to perform maintenance on an on-site programmable electronic device does not involve the same process as a typical interactive user session through remote access. Therefore CenterPoint Energy believes this requirement should not apply to temporary laptop connections which are otherwise in compliance with section R26 and recommends an exception be included.

#	Organization	Yes or No	Question 27 Comment
27.21	E.ON U.S.	Disagree	E.ON U.S. suggests that the standard specify access is through an “access point”.
27.22	RRI Energy	Disagree	Give more clarity on non-user sessions so that it is well understood that application data sessions are not a part of the “remote access” terminology of R11.
27.23	San Diego Gas and Electric Co.	Disagree	If a device can establish an interactive user session with a BES Cyber System and thus either respond to a BES condition or disturbance or enable control and operation, this “external device” should be named a “BES Cyber System Component.SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
27.24	US Bureau of Reclamation	Disagree	In addition, however, a mechanism needs to needs to be established to deal with devices locally connected for the purpose of "testing" and "configuration" so that these devices can be periodically connected for a specified and limited purposes. Per discussions during the recent Grapevine, TX, meeting, the drafting teams indicated that they would address this issue during their revision process.
27.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
27.26	National Grid	Disagree	National Grid recommends this definition be consistent with the “external connectivity” definition -recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
27.27	Black Hills Corporation	Disagree	Need a better definition to clarify remote access vs. external access. This creates policy issues for entities with respect to their definitions of these terms.
27.28	Northeast Utilities	Disagree	Need to clarify external connectivity (i.e., from other security domains within the company’s internal network or directly from the public internet). Level of authentication required should differ.

#	Organization	Yes or No	Question 27 Comment
27.29	LADWP	Disagree	Needs more clarification
27.30	NextEra Energy Corporate Compliance	Disagree	NextEra suggests defining external connectivity should be defined and clarified. It is unclear if external connectivity means external to the network the BES Cyber System resides or if it means connectivity from any device to any BES Cyber System component whether it is on the same network. External connectivity should be defined as any remote connection established through the BES Cyber System network access point devices, which includes examples of access point devices, such as dial-up connections, firewalls, SSL VPN connections, etc to a BES Cyber System component. As a point of clarification, since remote access is defined as "an interactive user session with a BES Cyber System from a device external to the BES Cyber System", is the device external to the BES Cyber System now considered a BES Cyber System with the same BES Impact Level as the BES Cyber System in which the device is remotely connecting to? For example, if we have a High Impact BES Cyber System which is an Energy Management System (EMS) within a Control Center, a laptop is used to remotely connect to this EMS, is the laptop now considered a High Impact BES Cyber System?
27.31	Tenaska	Disagree	not needed
27.32	USACE - Omaha Anchor	Disagree	Per your definition one cyber system talking to another cyber system that are side by side would be considered remote access - there seems to be no way to mitigate this. Remote access would be better served defined as communication from outside of the “physical security perimeter” or outside the plant.
27.33	Con Edison of New York	Disagree	R11 dialog box refers to Remote access as an interactive session with a BES Cyber System from a device “external” to a BES Cyber System. It is expected that external means from outside the electronic boundary.
27.34	Hydro One	Disagree	Recommend this definition be consistent with the “external connectivity” definition - recommend changing from “from a device external to the BES Cyber System” to “from

#	Organization	Yes or No	Question 27 Comment
			a device external to the BES Cyber System Boundary".
27.35	ISO New England Inc	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from <<from a device external to the BES Cyber System >> to << from a device external to the BES Cyber System Boundary>>
27.36	Northeast Power Coordinating Council	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
27.37	American Electric Power	Disagree	Regarding "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System", should this be "Remote electronic access"? Table R11 refers to "Wireless and Remote Electronic Access Documentation". Adding "electronic" to the definition would maintain consistency.
27.38	Regulatory Compliance	Disagree	Remote access - access originating from outside the eletronic boundary.
27.39	Southwest Power Pool Regional Entity	Disagree	Remote access can be application-to-application and should not be limited to just interactive access. For example, an FTP file transfer works the same way whether invoked interactively by a human user or programmatically by an application. It makes no sense to establish requirements for interactive access only.
27.40	Duke Energy	Disagree	See above, external to station. For generation stations in particular, external connectivity (R3) and remote connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.The definition may need to state "a device external to the BES Cyber System and outside the BES Cyber System electronic boundary".

#	Organization	Yes or No	Question 27 Comment
27.41	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
27.42	Allegheny Energy Supply	Disagree	Suggest clarifying similar to the following: Remote access should be interactive access of a BES Cyber System from a device external to the electronic and physical protection boundaries of that BES Cyber system.
27.43	Platte River Power Authority	Disagree	Suggested Revision:Remote access for the purpose of this standard means an interactive user session with a BES Cyber System Component from a device external to the BES Cyber System.That would better match the definition of external connectivity.
27.44	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal to add the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.45	Minnesota Power	Disagree	The current definition of "remote access," along with definition of "external connectivity," leaves open to interpretation whether Requirement R11 applies to host-based controls, or if it mandates network-based controls even within isolated or protected networks. It would appear that any interactive network access to a BES Cyber System is by definition remote access unless a portion of the network is included in the definition of that particular BES Cyber System. If the latter approach is adopted then multiple, otherwise independent, BES Cyber Systems might be arbitrarily selected to be a single BES Cyber System in order for this requirement to be met and still allow for reasonable security management.
27.46	Detroit Edison	Disagree	The definition may be interpreted to include maintenance devices. Revise as follows "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the Electronic Boundary of the BES Cyber System."

#	Organization	Yes or No	Question 27 Comment
27.47	Ameren	Disagree	The phrase "from a device external to the BES Cyber System," is open to interpret. Please clarify if this refers to a device physically external or electrically external.â€,â€,â€,
27.48	Alberta Electric System Operator	Disagree	The word “user” should be removed from “interactive user session” because it implies human interaction and does not consider automated malware.
27.49	Progress Energy - Nuclear Generation	Disagree	This definition is not clear to me. I recommend Remote Access be defined based on NIST 800-53 Appendix B slightly modified to accommodate industrial control systems. “Access to a BES Cyber Security System by a user or process communicating from an untrusted network”
27.50	Bonneville Power Administration	Disagree	This has the same issues as the definition of "External Connectivity". In fact, the definition could simply be "an externally connected interactive user session. Recommend that the definition be reworded to use the definition of External Connectivity, along with a suitable redefinition of that term, as described in question 13. If not, recommend - "Remote Access - For the purposes of this standard, remote access is defined as an electronic connection with control capabilities to a BES Cyber System, using a data communications path that encompasses, in some or all portions, links outside the control of the Responsible Entity. "Also add a definition of wireless access that makes it clear that such access is always an example of external connectivity. The definition should exclude such protocols as Bluetooth and infrared, which are intra-system, not inter-system methods. Note that even non-interactive wireless access should be controlled.Suggestion: Wireless electronic access for the purpose of this standard means access to or from a BES Cyber System to another cyber system using wireless communications. Even if both systems and any wireless access points are under the control of the Responsible Entity, the wireless communications path itself is not. For that reason, any wireless electronic access is considered to be external connectivity."

#	Organization	Yes or No	Question 27 Comment
27.51	Kansas City Power & Light	Disagree	This is too broad and could include devices such as Remote Terminal Units.

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R11 has moved to CIP-005-5- Cyber Security - Electronic Security Perimeters, Requirement R2.

Commenters expressed concern that for items R11.2 and R11.3, given the definitions provided in the standard, how is remote access provided without external connectivity? The SDT agrees and notes that a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters also expressed concern that there are inconsistent definitions for "external connectivity" and "remote access". The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity: The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access: **A**ny user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 28 Comment
28.1	WECC		Again consider replacing with requirement for remote access plan that provides specific requirements and conditions for remote access.
28.2	Florida Municipal Power Agency	Agree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the

#	Organization	Yes or No	Question 28 Comment
			BES Cyber System.
28.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
28.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
28.5	Bonneville Power Administration	Agree	This agreement assumes that External Connectivity is suitably redefined. Also, consider the following changes:1 - Remove Wireless from the title and the requirements.2 . If wireless is to be addressed, add a new requirement item specifically for wireless, dealing with the requirements on wireless access that are in addition to those for remote access in general.
28.6	E.ON U.S.	Disagree	: E.ON U.S. does not believe that compliance requirements are necessary for low impact systems
28.7	Southwest Power Pool Regional Entity	Disagree	“Required for external connectivity only” does not make sense. A properly configured wireless access should never directly connect within the secured network, thus any access will be “external.”
28.8	Luminant	Disagree	11.2 and 11.3 should be for Routable External Connectivity only
28.9	American Electric Power	Disagree	11.2: Regarding "If remote access is used and/or implemented, document the allowed methods for remote access", does this mean the list of approved ports and services? If not, what is meant by "allowed methods"?
28.10	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined.

#	Organization	Yes or No	Question 28 Comment
			Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.
28.11	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
28.12	Black Hills Corporation	Disagree	Applicability needs to be consistent previous non-wireless requirements.
28.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
28.14	LCEC	Disagree	Clarify what is meant by external connectivity only. Is this referring to any access to a BES cyber system component as defined earlier in the standard?
28.15	The Empire District Electric Company	Disagree	Comments: For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.16	Platte River Power Authority	Disagree	Disagree with the inclusion of Wireless.
28.17	Hydro One	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.18	ISO New England Inc	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”

#	Organization	Yes or No	Question 28 Comment
28.19	Northeast Power Coordinating Council	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.20	American Transmission Company	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.21	MRO's NERC Standards Review Subcommittee	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.22	NextEra Energy Corporate Compliance	Disagree	For Low Impact BES Cyber Systems, (1) documenting the allowed methods for remote access per 11.2, and (2) establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges per 11.3 should not be required. The identification of use restrictions for wireless technologies per 11.1 should be a sufficient security management control for Low Impact BES Cyber Systems. 11.2 and 11.3 will be administratively burdensome if required for practically every BES Cyber System.
28.23	San Diego Gas and Electric Co.	Disagree	Instead of defining requirements by using the impact levels, SDG&E feels it would be more appropriate to factor in the level of risk associated with the BES Cyber Systems to define the requirements for wireless and remote access.
28.24	Dairyland Power Cooperative	Disagree	Is external connectivity considered to be from outside the entity’s premises, or is it considered to be from outside the protected BES system (including for instance a corporate LAN). If it means outside the premises, then it seems deficient to not document the access-especially when later enabling of external connectivity could occur without the involvement of the supporting the BES cyber system. If it means external to the BES cyber system, then “external connectivity” and “remote access”

#	Organization	Yes or No	Question 28 Comment
			are redundantly used in 11.2 and 11.3.
28.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
28.26	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
28.27	National Grid	Disagree	o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access” o National Grid also suggests deleting the requirement 11.3 for Low Impact BES CS.
28.28	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. Without understanding the defined intent suggested specific changes may be vague. Remote access is defined but not external connectivity. Is there a distinction?
28.29	American Municipal Power	Disagree	Please provide a little or no impact category
28.30	BGE	Disagree	Remove the requirement for Low on 11.1, 11.2 and 11.3
28.31	Garland Power and Light	Disagree	Requirement 11.1, 11.2, 11.3 - remove Low Impact classification from all 3
28.32	Detroit Edison	Disagree	Requirements 11.2 and 11.3 specify “Required for external connectivity only”. This is redundant. It is not possible to have remote access without external connectivity by definition.
28.33	Emerson Process Management	Disagree	Since this standard is for remote access, is the "external connectivity" potentially redundant or extra? If there is no external connectivity, how can user establish an interactive session remotely?

#	Organization	Yes or No	Question 28 Comment
28.34	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
28.35	ERCOT ISO	Disagree	Table 11 should address remote and wireless access across all requirements in keeping with the title of the section.
28.36	Consultant	Disagree	Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.
28.37	Alberta Electric System Operator	Disagree	The AESO suggests moving row 11.1 in Table R11 to a separate section governing wireless as a standalone requirement.
28.38	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comment that “for external connectivity only” is redundant and should be removed from R11 Table 11.2 and Table 11.3 impact levels.
28.39	Reliability & Compliance Group	Disagree	the external connectivity qualifier
28.40	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create

#	Organization	Yes or No	Question 28 Comment
			confusion regarding the applicability of the criteria for each impact level.
28.41	US Bureau of Reclamation	Disagree	The level for Low Impact is not consistent with Electronic Access Management requirement in R8.

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimeters, Requirement R2

Commenters suggested the need to separate wireless and remote access, and Requirement R12.1 appears to be duplicative of R8.2 and has been removed. The SDT agrees and notes a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

Several commenters suggested that R8 and R12 are duplicative as both require quarterly review and verification of accounts and associated access privileges. The SDT moved all requirements for verification of accounts and associated access privileges into the revised CIP-004-5.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

#	Organization	Yes or No	Question 29 Comment
29.1	WECC		See comments for R10/R11 consider combining this into a requirement for a Wireless Plan and Remote Access PlanThis requirement could be rolled into R8.
29.2	Southern California Edison Company	Agree	Additional clarification may be provided on criteria for control systems. It seems that a control center is temporally viewed as a distributed control system; each node (footprint restricted to one facility but electronically extends scope of control to at least one other facility) can be treated as a "control center". The drafting team should

#	Organization	Yes or No	Question 29 Comment
			develop a guideline document that presents a discussion of the local definition of a control center as a facility or system that has the ability to control more than one BES asset, side by side, with definition of the electronic boundaries of a BES system. Remote access within a facility and from beyond a particular physical facility can have different risk profiles.
29.3	Southwest Power Pool Regional Entity	Agree	Agree with the wording as presented. See comments to question 30 about applicability.
29.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
29.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12.
29.6	MRO's NERC Standards Review Subcommittee	Agree	Note impact level comments under question 30.
29.7	Progress Energy - Nuclear Generation	Agree	R12 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
29.8	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
29.9	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that

#	Organization	Yes or No	Question 29 Comment
			the Responsible Entity must take.Our agreement with this Requirement is contingent on the redefinition as discussed in Question 27 and the definition of wireless electronic access stated above.
29.10	GTC & GSOC	Agree	We generally agree but disagree with the inclusion of the term Wireless in the requirement and associated table. Neither have anything to do with wireless as distinguished from other remote access.
29.11	Independent Electricity System Operator	Disagree	- R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.12	Luminant	Disagree	12.1 should be for Routable External Connectivity only
29.13	US Bureau of Reclamation	Disagree	Access management should be established for all impact lelvels. If the requirements of R11 are going to be established, R12 needs to be established to support enforcement. Further, what is meant by quarterly review.
29.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
29.15	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is a little more difficult, consistency of approach will result in greater security.
29.16	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.We also suggest eliminating R12 and combine it with R8.2 (quarterly review and verification of accounts and associated access privileges), as these are part and parcel of account rights management.
29.17	Hydro One	Disagree	For consistency with 12.1, recommend removing “wireless” from R12.Recommend changing Requirement 12.1 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Similarly to our previous comment

#	Organization	Yes or No	Question 29 Comment
			to R11, we don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e. if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.
29.18	ISO New England Inc	Disagree	For consistency with 12.1, recommend removing "wireless" from R12R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.19	Northeast Power Coordinating Council	Disagree	For consistency with 12.1, recommend removing "wireless" from R12.Recommend changing Requirement 12.1 from "quarterly review" to "annual review". There are no additional benefits to the shorter review period.
29.20	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Table 12 o redundant with Table 11 and Table 8. Suggest including this review as part of the review conducted in 8.2. o suggest removing 'and verification.' We don't understand the benefit to this and question if it is possible for remote access.
29.21	Constellation Power Source Generation	Disagree	In general, Constellation believes that wireless controls should be combined with network controls, as the same controls will be applied.
29.22	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.

#	Organization	Yes or No	Question 29 Comment
29.23	Northeast Utilities	Disagree	It is our belief that the review of access privileges conducted under Requirement 8 would satisfy the intent of this requirement as well and that R12 should be eliminated.Hence, this requirement is not needed as long as it is clear that remote access will not be granted unless explicit specific rights are granted to some asset they connect with. Access should not be given access to a protected area unless there is a need to access a specific asset, i.e., there is no business need to just grant network only access.
29.24	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
29.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that if remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges, it is unclear how this access is supposed to be verified and what is accepted as part of the verification process. This is the same as the comments to address question #20 of this questionnaire. If remote access is used and/or implemented, documenting and implementing a quarterly review and verification of the personnel with remote access and their associated access privileges

#	Organization	Yes or No	Question 29 Comment
			may not be sufficient. This process needs to be tied in with personnel (1) gaining authorized remote access to a BES Cyber System, (2) modifying their access privileges to a BES Cyber System due to change of the user's access rights due to change in role or responsibility and, (3) loosing authorized remote access to a BES Cyber System due to a revocation of electronic access to a BES Cyber System.
29.26	National Grid	Disagree	o National Grid recommends an annual review for verification since quarterly review does not have much benefit. o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”
29.27	Progress Energy (non-Nuclear)	Disagree	Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
29.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
29.29	Consultant	Disagree	R12 is an account management requirement. The requirement should be moved to R8 as an aspect of account management.There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R12. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems."
29.30	CWLP Electric Transmission, Distribution and	Disagree	R12. Due to the requirements access revocation in R9 this requirement should be extended to an annual review.

#	Organization	Yes or No	Question 29 Comment
	Operations Department		
29.31	Southern Company	Disagree	R12.1 addresses remote access only and does not include wireless, the table title and R12 includes wireless.
29.32	Allegheny Energy Supply	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.33	Allegheny Power	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.34	EEI	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.35	PNM Resources, Inc.	Disagree	Requirements for disabling access or user accounts in periods that are less than 6 hours are unrealistic, especially on weekends or during off-hours.
29.36	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the wireless and remote electronic access management apply to devices external to the BES Cyber System's network.
29.37	Manitoba Hydro	Disagree	Since Requirement R12 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Consider adding a requirement for securing the wireless access point.
29.38	ERCOT ISO	Disagree	Table 12 should address remote and wireless access across all requirements. 12.1: Should be combined with other access management requirements (physical, cyber, information).
29.39	BGE	Disagree	Tables 11 and 12 are out of synch.
29.40	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
29.41	FirstEnergy Corporation	Disagree	The Table is titled “Wireless and Remote ...”For consistency we suggest that 12.1 be

#	Organization	Yes or No	Question 29 Comment
			revised to state "... personnel with wireless and remote access ..."
29.42	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
29.43	We Energies	Disagree	We Energies agrees with EEI: Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.44	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
29.45	Detroit Edison	Disagree	Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.Requirement 12.1 specifies "Required for external connectivity only". This is redundant. It is not possible to have remote access without external connectivity by definition.

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimiters, Requirement R2.

Commenters suggested a reword of this item to remove "for external connectivity only", since remote access cannot be granted without external connectivity. The SDT agrees and has made this change.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

Several commenters suggested that R9 and R12 are duplicative. The SDT moved all requirements for revocation of access privileges into the revised CIP-004-5.

#	Organization	Yes or No	Question 30 Comment
30.1	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12. At minimum, R12 should be consistent with R8.
30.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
30.3	Progress Energy (non-Nuclear)	Agree	See Comment 14.Not needed. There already is another requirement for cyber access reviews.
30.4	Northeast Utilities	Agree	Suggest eliminating R12 - see response to Question 29.

#	Organization	Yes or No	Question 30 Comment
30.5	Independent Electricity System Operator	Disagree	- For R12.1 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
30.6	ERCOT ISO	Disagree	12.1: Should apply to Medium Impact BES Cyber System.
30.7	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protection and type of access granted. Wireless technology needs full security and encryption in regards to any level of BES Cyber System.
30.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
30.9	USACE HQ	Disagree	At a minimum, 12.1 should be required for all impact levels. Requirement 11 creates a document of remote access procedure and who has the right to use it, but for low and medium impact systems it is not required to update the same as per requirement 12.1.
30.10	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
30.11	Tenaska	Disagree	Combine 12 and 13
30.12	The Empire District Electric Company	Disagree	Comments: For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.13	Alberta Electric System Operator	Disagree	Create additional requirements in Table R12 for Medium and Low impact levels. Suggest semi-annual review for Medium Impact, and Annual review for Low impact.
30.14	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is

#	Organization	Yes or No	Question 30 Comment
			a little more difficult, consistency of approach will result in greater security.
30.15	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.
30.16	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station).
30.17	American Transmission Company	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.19	Consultant	Disagree	Item 12.1 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.

#	Organization	Yes or No	Question 30 Comment
30.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
30.21	WECC	Disagree	Medium Impact should still have the requirement as well.This should apply to all impact levels.
30.22	National Grid	Disagree	National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”.
30.23	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
30.24	NextEra Energy Corporate Compliance	Disagree	NextEra believes that regarding 12.1, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
30.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’.
30.26	American Municipal Power	Disagree	Please provide a little or no impact category
30.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Specifically, if 11.2 and 11.3 require documenting allowed methods and processes for remote access, then table 12 should require quarterly review of the access granted via 11.2 and 11.3. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.

#	Organization	Yes or No	Question 30 Comment
30.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
30.29	Hydro One	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.30	Northeast Power Coordinating Council	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.31	Southwest Power Pool Regional Entity	Disagree	Remote access should be periodically reviewed for all impact categories. Ideally, a more frequent review should be required for High impact systems.
30.32	Allegheny Energy Supply	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.33	Allegheny Power	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.34	EEI	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.35	ISO New England Inc	Disagree	Should be across the board, and annually for allRecommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
30.36	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary. Furthermore, requirement R12.1 is duplicative of R8.2.
30.37	ReliabilityFirst Staff	Disagree	Suggest “Required for external connectivity only” for Medium Impact in row 12.1.
30.38	Network & Security	Disagree	Suggest including Medium Impact systems with external connectivity.

#	Organization	Yes or No	Question 30 Comment
	Technologies Inc		
30.39	US Bureau of Reclamation	Disagree	Table R12 should be applied to all Impact levels in keeping with requirements established in R11.
30.40	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS that “for external connectivity only” is redundant and should be removed from R12 Table 12.1. The table should therefore read:R12 Table 12.1: Low Impact: N/AMedium Impact: N/AHigh Impact: Required
30.41	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.
30.42	PacifiCorp	Disagree	The term verification needs further definition. Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
30.43	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
30.44	We Energies	Disagree	We Energies agrees with EEI: Requirement R12 appears to be duplicative of R8.2 and should be removed.

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R7.

Commenters suggested making the timeframes for revocation in R13 the same as R9. In response, the timeframes for revocation requirements have been simplified as follows:

- Revocation of access to BES Cyber Systems at the time of the termination or resignation and by by the end of the next calendar day for reassignments or transfers action,
- Revocation of access to BES Cyber System Information by by the end of the next calendar day for terminations or reassignments, and
- Additional requirements were added to address revocation of user accounts on BES Cyber Systems and shared accounts.

Commenters expressed concerns that persons who transfer are not automatically considered a threat to the system, and the timeframes for revocation should reflect this. In response, the requirement for transfers now states a review of access is required on the transfer date, and any unneeded access is revoked when it is no longer needed.

Commenters suggested keeping the revocation timeframes the same as defined in CIP Version 3. The SDT notes that FERC Order 706 directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Organizations usually have termination procedures to return company property and perform exit interviews. Processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

#	Organization	Yes or No	Question 31 Comment
31.1	WECC	Agree	Agree with criteria but recommend combining with R9 Revoking Access.This could be rolled into R9

#	Organization	Yes or No	Question 31 Comment
31.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
31.3	Florida Municipal Power Agency	Agree	Consider combining R9 with R13 and making the timing consistent. In 13.1, 13.2 and 13.3, "when job duties no longer require ..." is ambiguous and should be tied back to the policy of R1.
31.4	Progress Energy - Nuclear Generation	Agree	R13 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
31.5	Minnesota Power	Agree	These criteria are generally acceptable, except for the statement that "Each Registered Entity shall revoke remote access by disabling one or more of the multiple factors required..." The requirement to implement multi-factor authentication is not included in CIP-011-1.
31.6	Independent Electricity System Operator	Disagree	- There is no requirement for removing external access for cause. Does R9.1 cover this access? Should for cause be changed to involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R1
31.7	PacifiCorp	Disagree	: The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.8	USACE - Omaha Anchor	Disagree	13.1 - '... when job duties no longer require remote access' should either be changed 'when terminated for cause' or if the verbiage is deemed appropriate then the length of time to change the password needs to be greatly expanded. Just because an employee changes jobs does not mean they are a threat to the system, they still have the appropriate clearances and training.13.2 & 13.3 - since we are talking about a current employee who is just changing jobs the high impact numbers are crazy. The person is not a threat to the system, they have the necessary background.

#	Organization	Yes or No	Question 31 Comment
			Recommend times be the same as medium impact system.
31.9	Xcel Energy	Disagree	A 1 hour revocation time in R13.1 is completely unworkable. Examples where this is impossible include a termination by a vendor or joint access partner, or a termination during evening hours or weekends/holidays, when IT staff needed to terminate the access can not respond within 1 hour. The 4 and 6 hour revocation times for job duty changes are unjustified and unneeded. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
31.10	BCTC	Disagree	Â Suggest collapsing Requirements 13.1 to 13.3 into one.Â Time targets would be the same as those suggested in Requirement 9 above
31.11	Alberta Electric System Operator	Disagree	Are the "multiple factors" referenced in R13 defined?
31.12	Tenaska	Disagree	Combine 12 and 13
31.13	BGE	Disagree	Combine 13.1, 13.2 and 13.3 into one requirement. Revocation for high impacted systems should be 24 hours to maintain consistency with other requirements with CIP-011.
31.14	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
31.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access. Revocation of remote access within one hour for Control Centers is unreasonable for high-impact

#	Organization	Yes or No	Question 31 Comment
			Systems when the revocation is unrelated to termination with cause. If revocation is the result of one's job duties no longer requiring access, then E ON U.S. suggests next-business day should be adequate. Likewise, six hours for Transmission substation systems, and four hours for Generation Systems is unreasonable. Next business-day revocation should be adequate for all of these situations and presents little, if any, additional risk. E.ON U.S. requests clarification as to what is included in the term "multiple factors" for remote access.
31.16	EEI	Disagree	EEI suggests the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.17	Constellation Energy Control and Dispatch, LLC	Disagree	-Eliminate the timing differences for revoking access when no longer required that exists between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.-The previous requirements have
31.18	FirstEnergy Corporation	Disagree	For 13.1, 13.2, 13.3 - Change text to '...when job responsibilities no longer requires BES Cyber System remote access'.This table should include a consideration when termination for cause. Should parallel Table 9 expectations.The recommended times are unreasonable for transfers/job reassignments.We have the same concerns with inconsistent application in regards to Impact Level as we previously identified in Table 9. See our comments to Questions 22 and 23.
31.19	Exelon Corporation	Disagree	Implementing revocation of access in as short a time as those proposed would require major changes to many enterprise wide systems in order to document compliance. Why do these time periods differ from those for physical and electronic access? Exelon feels these requirements are too restrictive and might necessitate moving to a 24/7 position to monitor the need for access revocation. Exelon's position is that the

#	Organization	Yes or No	Question 31 Comment
			access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
31.20	USACE HQ	Disagree	It does not make sense to create three (3) separate requirements for three specific environments only, I suggest to have only one requirement that reads “Revoke remote access when job duties no longer require BES Cyber System remote access”.
31.21	APPA Task Force	Disagree	New: R13 Table 13.1: For personnel terminated for cause on a preplanned basis. Low Impact: N/AMedium Impact: 8 hourHigh Impact: 8 hourThe Existing 13.1 - 13.3 will need to be renumbered if this new 13.1 is accepted.
31.22	National Grid	Disagree	o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access” o Reword “remote access” as “Remote access (LAN and wireless) communication interface o 24 hours is the minimal practical time for revoking access. A 1 or 4 hour revocation of access is not reasonable. National Grid suggests keeping times same as in Table R9.
31.23	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23. Furthermore, NextEra believes the timeframes suggested will be burdensome to administer since personnel that have authorized remote access have by definition also authorized electronic access. With this current draft, it connotes that when revoking access to High Impact Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access; the Responsible Entity has 1 hour to revoke remote access per 13.1 and has 36 hours to revoke electronic access per 9.2. We suggest making the time requirements consistent and up date the timeframe to "as soon a practical but within 36 hours" for both 13.1 and 9.2
31.24	Dominion Resources	Disagree	Please see Dominion’s response to Questions 15 and 22. Dominion also requests that

#	Organization	Yes or No	Question 31 Comment
	Services, Inc.		the removal of authentication needed for remote access suffice to meet the intention of this requirement for "immediate" revocation.
31.25	American Electric Power	Disagree	Please see response to Question 32 for additional detail.
31.26	Puget Sound Energy	Disagree	Puget Sound Energy disagrees with the current wording of the criteria. "...when job duties no longer require BES Cyber System remote access" is an abstract concept that will be impossible to quantify in order to validate compliance with the requirement. Puget Sound Energy suggests rewording to "Revoke remote access to...BES Cyber Systems when notification by personnel that job duties no longer require BES Cyber System remote access. In light of the 4 hr to 72 hr clock to revoke access, Puget Sound Energy suggests some measurable trigger from which to start the countdown to required revocation timeframes.
31.27	Detroit Edison	Disagree	R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.
31.28	LCEC	Disagree	R13 requirements should be moved to the account management section.
31.29	Southwest Power Pool Regional Entity	Disagree	R13: The objective states that access will be revoked by disabling one or more of the multiple factors required for such access, yet multiple factor access authentication has yet to be prescribed. 13.1, 13.2, and 13.3 simply states "revoke access." As stated, the requirement is unclear and inconsistent between the object statement (Requirement) and the criteria. It may be beneficial to swap Requirements 13 and 14, prescribing remote access authentication controls before prescribing revocation of such access.
31.30	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to "remote access".Recommend moving this Requirement to the Boundary Protection Requirements.

#	Organization	Yes or No	Question 31 Comment
31.31	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend moving this Requirement to the Boundary Protection Requirements.
31.32	ISO New England Inc	Disagree	Recommend using the same thresholds as R9Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”Recommend moving this Requirement to the Boundary Protection RequirementsR13.1, R13.2 and R13.3 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday. R13.1, R13.2 and R13.3 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the change.”
31.33	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
31.34	Regulatory Compliance	Disagree	Remove R13 altogether and treat revocation of remote access the same as system access.
31.35	Garland Power and Light	Disagree	Requirement 13.1 - Medium Impact should read 48 hours instead of 36 hours and High Impact should read 4 hours instead of 1 hour. To be as strict as written is not necessary for just a job duty change
31.36	Reliability & Compliance Group	Disagree	Revocation for employees terminated for cause needs to be included.

#	Organization	Yes or No	Question 31 Comment
31.37	Southern California Edison Company	Disagree	SCE recommends matching R13 with R9. The time limits for high-impact generation BES is less than transmission substation BES, whereas they are the same in R9. SCE also suggest that 13.2 and 13.3 be given the same time limit.Also, SCE requests clarification about the types of devices that must be revoked. Order 706 seeks immediate revocation to devices and facilities. While order 706 has been unequivocal in the requirement of this control, they do not specify that access to “each” device must be individually revoked. The drafting team should be asked to provide supplemental guidance with this requirement to state that immediate revocation in timeframes shorter than 24 hours to “boundaries” electronic and physical be instituted.
31.38	SCE&G	Disagree	SDT needs to account for transitional periods when incumbent needs to train a replacement for job tasks. In this case when would time period begin for "no longer requiring access". There would be no timestamped document to start the clock.
31.39	ERCOT ISO	Disagree	Should be combined with other access management requirements (physical, cyber, information).
31.40	Manitoba Hydro	Disagree	Since Requirement R13 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns. Please clarify if the “one or more of the multiple factors required for such remote access...” refers to the electronic access controls in Requirement R14. Please clarify what “such access” means.
31.41	Alliant Energy	Disagree	Specifically 1 hour system access removal is not even possible in an environment that is largely automated and unreasonably creates an environment of non-compliance. More generally, Table 13 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the

#	Organization	Yes or No	Question 31 Comment
			business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
31.42	Allegheny Energy Supply	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.43	Allegheny Power	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.44	Duke Energy	Disagree	Table 13: How will this apply in case of a death?13.1 change 36 hours to 48 hours
31.45	MidAmerican Energy Company	Disagree	The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.46	Ameren	Disagree	The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.
31.47	Southern Company	Disagree	The time limits in 13.1 are needlessly short in the context of an employee who is not

#	Organization	Yes or No	Question 31 Comment
			being dismissed for cause but is simply having his job duties changed. In addition, it is not clear exactly what the trigger point is for the start of that time table.
31.48	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
31.49	Dairyland Power Cooperative	Disagree	These rules seem redundant to table R9. Why are there redundant rules for remote access accounts vs regular accounts? Any rules here should be for something that is unique to remote access.
31.50	US Bureau of Reclamation	Disagree	This requirement appears to be in conflict with R9. In reading R9 it is not clear that it does not also include remote access. Just as in R11 remote needs to be defined especially since R9 does not indicate remote access is excluded as this standards implies. Further, requirements need to be established for all system impact levels and timeframes need to be realistic and achievable. Shorter timeframes, as established in the table, would appear to be more applicable to individuals terminated for cause.
31.51	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.

#	Organization	Yes or No	Question 31 Comment
31.52	Bonneville Power Administration	Disagree	This requirement is not necessary. It is already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference.If the Requirement is retained, then the objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
31.53	Progress Energy (non-Nuclear)	Disagree	This revocation is not based on termination for cause. It will be very difficult to meet the 1 - 6 hour revocations. If termination was for cause would an individual not need physical access to get remote access - we are required to physically secure areas around remote access? Shouldn't all access, system, physical, remove etc. have consistent revocation times?Revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage.This should be no different than the revocation of cyber access. This requirement is not needed. Also the time limits as proposed for High Impact are impractical and will only lead to unnecessary self-reports that provide no benefit to system security.CIP-011 R13.1 thru .3 What is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
31.54	CWLP Electric Transmission, Distribution and	Disagree	Time frames should be extended to 72 hours or next business day, whichever is longer.

#	Organization	Yes or No	Question 31 Comment
	Operations Department		
31.55	Con Edison of New York	Disagree	Timeliness of access removal is important. These criteria can be interpreted (R13.1 for example) to mean remote access needs to be revoked within 7 hours of the actual time of change of job duties. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the change within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 7 hours from notification of the need for change.R13.2 and 13.3: it is not clear that the standard defines either a Transmission or Generation BES Cyber System.
31.56	We Energies	Disagree	We Energies agrees with EEI: Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems." We Energies agrees with EEI: Suggest adding requirements to address the removal of remote access for low impact systems.
31.57	GTC & GSOC	Disagree	We recommend this requirement include language that would allow personnel to retain access during a transition period while training their replacement. We recommend the language used in requirement 5, row 5.8: "personnel who no longer require such access."We also recommend that termination for cause should be handled seperately. All other time lines should be commensurate with the associated risk and consistent throughout all requirements.We recommend the language in Table 13 should be consistent with 5.8 and 5.9 in Table 5.We recommend requirements 13.1, 13.2, 13.3 should include the words "the entity determines the" between the words "when" and "job"; this would prevent an auditor from second guessing an entity's decision on required access. The requirement should also specifically state that this does not preclude a person from retaining access in order to assist his replacement with fulfilling his old job duties during a transition of

#	Organization	Yes or No	Question 31 Comment
			responsibilities.
31.58	Network & Security Technologies Inc	Disagree	Wording suggests multi-factor authentication is required for all systems subject of R13, but R14 only requires multiple factors for High Impact systems. Also suggest swapping order of requirements in R13 and R14.

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R5.

Commenters suggested aligning with R9 normal revocations. In response, the requirements for revocation have been consolidated to CIP-004-5 R7.

Commenters suggested including targets for Low Impact BES Cyber System revocation. The SDT notes the applicability to Low Impact BES Cyber Systems has been removed.

Commenters suggested times need to be stated in business days. In response, times have been changed to calendar days. The use of business days is not appropriate because this can be interpreted to include exclusions for weekends and holidays.

#	Organization	Yes or No	Question 32 Comment
32.1	Luminant	Agree	13.1 should be changed to 48 hours (2 days)
32.2	USACE - Omaha Anchor	Agree	Agree - just want to reiterate the times associated with removal for a job transfer are ridiculous. The person has been trusted and trained - it's not an emergency just because they changed jobs. (Due to lack of personnel - if this happened on a Friday - we would have to treat it as an emergency.)
32.3	Idaho Power Company	Agree	Need to make this consistent with revocation requirements for normal electronic access. Why would these timelines be shorter?
32.4	SCE&G	Agree	The timeframes, specifically for High Impact Control Center assets, are extreme.
32.5	US Army Corps of Engineers, Omaha Distirc	Disagree	"when job duties no longer require" will be very hard to account for. Time frames are unrealistic / impossible. Times should be stated in terms of business days. It would be more realistic for High Impact BES Cyber Systems to be Next Business Day and for Medium Impact Cyber Systems to be 2 and 3 business days.

#	Organization	Yes or No	Question 32 Comment
32.6	Florida Municipal Power Agency	Disagree	1 hour is not reasonable. Planned termination for cause can be 1 hour, but, otherwise the 1 hour is not reasonable. Consider aligning the times with R5 and R9. Access revocation alternatives/mitigation techniques should allow for deviation from the standard, or be recognized. For example, escorted supervision while restricting access to communication devices/computers should be a reasonable way to get around the 1-hour requirement if it can't be met for some particular reason.
32.7	American Electric Power	Disagree	13.1 - 13.3, regarding all information in column "High Impact BES Cyber System". These values are not feasible on a system unless it is managed with a domain controller or has only a few network components. Suggest using the 36/72/72 as required in the R9. There is no need to make this more restricted than the local access.There also does not appear to be a requirement to revoke access within 24 hours for a termination for cause. Is that the intent?
32.8	Con Edison of New York	Disagree	13.1,2,3- may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
32.9	ERCOT ISO	Disagree	13.1: 1 hour may not be possible. Especially in light of access granted to external organizations (ie: an RC or BA with access a TOP's systems).
32.10	Southern California Edison Company	Disagree	A longer time frame (range of <72 hours for high medium and low impact systems) should be instituted for each device. Revocation should not be treated as a monolithic requirement and should be such that it leverages controls instituted by boundary protections.
32.11	Constellation Energy Commodities Group Inc.	Disagree	Align all high and medium impact systems on the 72 hour standard to eliminate confusion and allow consistent administration.

#	Organization	Yes or No	Question 32 Comment
32.12	MidAmerican Energy Company	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and not understood why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.13	PacifiCorp	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and it is not understood clear why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk difficulty to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.14	American Transmission Company	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-

#	Organization	Yes or No	Question 32 Comment
			compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
32.17	Tenaska	Disagree	Combine 14 and 11
32.18	The Empire District Electric Company	Disagree	Comments: As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.19	Alberta Electric System Operator	Disagree	Consider adding “120 hours for external connectivity only” to all Low Impact BES Cyber System levels (13.1, 13.2, 13.3).
32.20	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
32.21	Duke Energy	Disagree	Drafting team, please explain the basis for the 1 hour, 6 hour, and 4 hour requirements for the High Impact column. These appear to be overly restrictive and arbitrary. Similar to the comment above, these items are much more achievable if "remote" and "external" are defined as external to the plant in a generation

#	Organization	Yes or No	Question 32 Comment
			environment. Also, as stated above (question 27), remote connectivity requires more unambiguous definition.
32.22	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access
32.23	USACE HQ	Disagree	First, requirements 13.1, 13.2, and 13.3 should be required for every level of impact. Second, to avoid the "Friday 5PM no longer required access" scenario, the language should be change as follow: for High Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the following day after the no longer access required for external connectivity only", for Medium Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the second day after the no longer access required for external connectivity only", and for Low Impact BES Cyber System in 13.1, 13.2, and 13.3 (please refered to my answer to question 31), from "----" to "Close of Business Day (COB) of the third day after the no longer access required for external connectivity only".
32.24	Network & Security Technologies Inc	Disagree	If authentication is required for remote access to Low Impact systems (R14), it should be covered by R13 revocation.
32.25	WECC	Disagree	If the employee can access the system remotely why can the entity not remotely disable the access? Please have another look at the hours for the medium impact level.This should apply to all impact levels and Medium and Low impact systems should require not more than 24 hour timelines for revocation.
32.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
32.27	BGE	Disagree	Low impacted systems should have a timeframe defined for revocation

#	Organization	Yes or No	Question 32 Comment
32.28	FirstEnergy Corporation	Disagree	Need clarity on '...for external connectivity...'. For example, does this mean consoled in (directly connected) as well as remote electronic logon?Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.Similar concerns as previously stated with Table 9. See Questions 22 and 23.
32.29	Detroit Edison	Disagree	Please explain the reason for different revocation times between High Impact on 13.2 and 13.3.
32.30	American Municipal Power	Disagree	Please provide a little or no impact category
32.31	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23.
32.32	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12 and Table 13. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
32.33	Progress Energy - Nuclear Generation	Disagree	R13 durations should align with those described in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
32.34	LCEC	Disagree	R13 requirements should be moved to the account management section.
32.35	ISO New England Inc	Disagree	Recommend using the same thresholds as R9 Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope

#	Organization	Yes or No	Question 32 Comment
			to “remote access”
32.36	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.37	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.38	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
32.39	Public Service Enterprise Group companies	Disagree	Remote access should be governed by the same rules are normal access. The time frame in 13.1 for High Impact BES Cyber Systems is unreasonably short. Notifying and securing the appropriate personnel to disable access once the job duties no longer require access may not be possible in all circumstances to guarantee that access is always revoked within 1 hour. This may not be operationally feasible. The timeframe should be similar to access revocation for user with non-remote access as specified in Table R9 item 1.9 (i.e. within 24hrs).
32.40	Manitoba Hydro	Disagree	Remote electronic access to BES Cyber Systems should be revoked for Low Impact BES Cyber Systems, and not permitted indefinitely. The remote access revocation period for generation High Impact BES Cyber Systems should be 6 hours, the same as for the Transmission High Impact BES Cyber System.
32.41	Exelon Corporation	Disagree	Requirements 13.1, 13.2 and 13.3 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time

#	Organization	Yes or No	Question 32 Comment
			levels and having a different timeframe for a control center than other locations? With the exception of a termination for cause, what is the basis for requiring access removal for someone who was a trusted employee on such an aggressive timeframe? What is the risk that is being addressed by making a 1 hour timeframe requirement?
32.42	Southwest Power Pool Regional Entity	Disagree	Revocation timeframes should be expressed in business days.
32.43	National Grid	Disagree	Same as in Q. 31.
32.44	San Diego Gas and Electric Co.	Disagree	SDG&E feels that the key for this requirement is the definition of the phrase "when job duties no longer require remote access". This phrase can be interpreted in a couple of different ways. The more strict interpretation is that a person would no longer need access after their session is complete, or perhaps after taking a break or going to lunch. This could happen a few times per day, depending on the work. A second interpretation could mean that a person no longer needs access after a 6 month long project is completed or there is a reassignment to another part of the company after 3 years of working on the BES Cyber Systems, etc. In the former case, it becomes a large burden to revoke access within one hour several times per day, and could be a manual process on some systems. On the other hand, if you consider the second interpretation (6 month project or transfer after 3 years), SDG&E would ask why is it so important to revoke remote access with 1, 4, or 6 hours after such a long period of time that a person has had access? Sometimes it takes time for a person to get reassigned, change locations, change projects, etc. In this case, 4 hours would be the minimum that SDG&E feels is practical to be able to comply with.
32.45	Progress Energy (non-Nuclear)	Disagree	See comment 14.This should be no different than the revocation of cyber access revocation. This requirement is not needed.
32.46	GTC & GSOC	Disagree	See comments to question 31 above

#	Organization	Yes or No	Question 32 Comment
32.47	BCTC	Disagree	See our response for table 9 time targets
32.48	Constellation Energy Control and Dispatch, LLC	Disagree	See response to Question 31.
32.49	Regulatory Compliance	Disagree	STRIKE Table R13
32.50	EEI	Disagree	Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.EEI suggests using a uniform number of hours across various facility types for high and medium.EEI suggests using 7 calendar days for medium.EEI suggests using 8 hours for high impact.EEI suggests adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System."
32.51	Allegheny Energy Supply	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.52	Allegheny Power	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.53	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comments noting that as written, the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access). However we feel the one area where an entity is vulnerable is when personnel are terminated for cause. We see this as the most extreme case when an

#	Organization	Yes or No	Question 32 Comment
			entity should be diligent in protecting remotely accessible BES cyber systems and act within the time of a normal shift. We suggest 8 hours for termination for cause, except when a termination is preplanned, in which case a shorter time period may be feasible. Similar to the comments we provided regarding R9: We know there are pressures to have access restricted as soon as possible but we are trying to be realistic given the time it will take to remove access from systems which have multiple owners, are in remote locations and which have numerous devices to access. It seems that the drafting team is basing their proposed timetable on a control center where the cyber systems are more IT focused and have controls that can be turned on and off easily.We propose the following changes to the Impact Levels of R13:R13 Table 13.1: (NEW) Low Impact: N/AMedium Impact: 8 hoursHigh Impact: 8 hoursR13 Table 13.2: (Old 13.1)Low Impact: N/AMedium Impact: 36 hoursHigh Impact: 36 hourR13 Table 13.3: (Old 13.2)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 WeekR13 Table 13.4: (Old 13.3)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 Week
32.54	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.In certain circumstances, it may not be possible to adhere to the proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule. The need for more immediate time constraints, when compared to electronic access as defined in Requirement R9 that is not remote is understood, but both the Requirements in R9 and R13 need to take into account reasonable business processes that impact notification of employee reassignment and separation.Minnesota Power recommends that the timelines for R13 be consistent with those established in R5 and R9, but would agree that terminology should be included urging Registered Entities to expedite this process as much as possible with regards to remote access.

#	Organization	Yes or No	Question 32 Comment
32.55	GE Energy	Disagree	The revocation targets for High Impact systems will be almost impossible to meet for revoking vendor personnel access (Table R13 HI BES remote access must be terminated within 1 hour of access no longer being required). It also seems to be in conflict with the revocation times in Table R9? These need to be linked together.
32.56	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
32.57	US Bureau of Reclamation	Disagree	The timeframes for High Impact are not consistent with R9 and appear to be too stringent. Further, requirements need to be established for all system impact levels.
32.58	Oncor Electric Delivery LLC	Disagree	These proposed time frames are not practical as most HR systems are separate (and should be) from real-time operations of the BES. The time-frames for High Impact cannot be different from Medium, as they utilize the same back-office information systems.
32.59	Bonneville Power Administration	Disagree	These requirements are not necessary. They are already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference. In addition, this requirement could force Cyber System administrative personnel to take action to revoke access even if it means not performing other actions needed to support real-time operations, or risk non-compliance. As an example, if a BES Cyber System has failed for some reason, the corrective actions should take precedence over revoking access. Under those circumstances, an entity could find itself in the position of deliberately allowing non-compliance in order to restore the integrity of the BES. The required time frames are impossibly short for high impact systems. It is difficult to justify dropping all other actions to revoke access for someone unless there is reason to believe that the individual poses a threat. In that case the requirements of R9 are in effect.This

#	Organization	Yes or No	Question 32 Comment
			requirement seems to conflict with R9 and Table R9. Table R9 allows 24 hours for access revocation due to termination for cause. Table requires revocation within 1 hour, even if termination for cause is not required.Recommendation: Remove this requirement entirely. Treat revocation of remote access as just another revocation of access under R9. Otherwise, increase the time frames to something achievable.
32.60	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.
32.61	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
32.62	We Energies	Disagree	We Energies agrees with EEI: Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.We Energies agrees with EEI: Suggest using a uniform number of hours across various facility types for high, medium and low.We Energies agrees with EEI: Suggest using 7 calendar days for medium and 14 calendar days for low impact.We Energies agrees with EEI: Suggest using 8 hours for high impact.We Energies agrees with EEI: Suggest adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session

#	Organization	Yes or No	Question 32 Comment
			with a BES Cyber System from a device external to the BES Cyber System.”

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Requirements for remote access in CIP-011-1 R14 have moved to CIP-005-5 - Cyber Security — Electronic Security Perimeters.

Commenters expressed concern that the scope of the "Banner" requirement should be clarified and that having a banner is not a security control. The SDT agrees and notes that the requirement to have appropriate use banners was considered administrative and has been removed.

Several other commenters suggested splitting wireless and remote access requirements. The SDT notes that a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

#	Organization	Yes or No	Question 33 Comment
33.1	WECC		Don't see the security value of requiring login banner as required in 14.4. This requirement seems to stem from the belief that in a legal prosecution the court would need to show that the system was misused or accessed inappropriately and that a login banner accomplishes this by notification. Since most attacks are done via automation today, and internal attackers are likely required to sign an acceptable use policy this requirement seems to only add operational cost. Additionally, one can prove that inappropriate use was done by the mere fact that the person is using the system without authorization. Also keeping this in for only high impact systems would let attackers easily know which systems are high impact/value. Recommend dropping criteria all together. The appropriate use banner criterion does not belong here. This is a legal protection, not a security control, and would be better placed in a policy type requirement. Consider replacing "multi-factor" with "strong", and offering

#	Organization	Yes or No	Question 33 Comment
			additional language to clarify the term. "Strong" auth should be required for all remote access. Provide distinction between remote access from untrusted locations, such as the internet, and remote access from trusted locations, such as a backup control center.
33.2	Duke Energy	Agree	14.4 requires a TFE
33.3	Regulatory Compliance	Agree	BUT14.2 - What is the risk protection versus cost, time and overhead to implement?
33.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
33.5	CWLP Electric Transmission, Distribution and Operations Department	Agree	Is multifactor access control limited to electronic methods only? Can the use of enabling or disabling a device such as a modem equal to a portion of multifactor controls?
33.6	Puget Sound Energy	Agree	Puget Sound Energy agrees with the criteria, but suggests NERC provide clarity in regards to 14.4. Is NERC requiring an "appropriate use banner" on the user screen for the initial attempt of remote access, or for all interactive attempts established after successfully authenticating remotely? Example: Is an appropriate use banner only needed for a 2-factor VPN connection screen, or at all systems accessed through a 2-factor VPN (operating system and application(s) on BES Cyber System Components?
33.7	Progress Energy - Nuclear Generation	Agree	R14 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
33.8	GTC & GSOC	Agree	We recommend references to wireless should be removed from R14 and the associated table. The actual requirements are not related to wireless as distinct from

#	Organization	Yes or No	Question 33 Comment
			other remote access
33.9	Green Country Energy	Agree	Will their be guidance? How about changing the statement to "reasonably ensure" that no unauthorized access is allowedExample: If my processes allow anyone to be authorized, I then can "ensure" no unauthorized access will occur.
33.10	Independent Electricity System Operator	Disagree	- R14.1 and R14.2 seem to be stating the same thing. R14.2 is covered by R14.2.- R14.4 - Shouldn't the use banner be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will
33.11	American Electric Power	Disagree	14.1: Regarding "If remote access is used and/or implemented, include authentication controls". Suggest replacing "include" with "document".
33.12	FirstEnergy Corporation	Disagree	14.2 this could be difficult to implement depending on the definition of "interactive user session" within the definition of remote access.14.2 - add '...authentication controls for remote access mechanisms'14.3 - add 'remote access' somewhere in this sub-requirementWith R14.4, it requires an appropriate use banner; there is no allowance for equipment that can not support a banner.
33.13	Luminant	Disagree	14.4 - where technically feasible
33.14	Southwest Power Pool Regional Entity	Disagree	14.4 is overly prescriptive. Consider revising the requirement to simply state "Display an "appropriate use banner" upon an interactive attempt to access a BES Cyber System, stating that unauthorized use of the system is prohibited."
33.15	BCTC	Disagree	Â R 14.1: remove Required as the requirement is satisfied under R14.2R14.4: text "remote electronic access" devices; suggest that the language be rewritten/ simplified so the objective is clear - i.e. ensure appropriate CCAs display appropriate use banner when connecting to these assets remotely
33.16	Southern California	Disagree	As stated above, remote access should be thoroughly documented and full encryption

#	Organization	Yes or No	Question 33 Comment
	Edison Company		and authentication methods applied.Also, SCE requests that the drafting team review the intent of R14.4 and R7.2 and consider combining the requirements.
33.17	Tenaska	Disagree	Combine 14 and 11
33.18	Alliant Energy	Disagree	Consideration should be given to whether or not the access provides control capability or simply read only.
33.19	ISO New England Inc	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, please update the wording. If NO, the Requirements are confusing because we use wireless that is not remote access, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection RequirementsR14.1 and R14.2 seem to be stating the same thing.14.2 should have requirement for medium. 14.4 appropriate use banner - is this required for legal steps in the event of an issue... this is not a security control.If the banner is need then the use banner should be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will allow the traffic through without displaying a banner.
33.20	Northeast Power Coordinating Council	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, the wording should be revised. If NO, the Requirements are confusing. Wireless that is not remote access may be used, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection Requirements.
33.21	Florida Municipal Power Agency	Disagree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Item 14.4 is very specific in requiring “appropriate use banner” this should be removed or reworded to cover various methods of notification. Also the standard should demand that no identifiable details be given about the system before authentication is complete.We believe items 14.3 and 14.4 are going to set the stage for numerous TFE’s within the industry. Many devices (e.g.,

#	Organization	Yes or No	Question 33 Comment
			protective relays) do not support explicit access permissions and appropriate use banners.
33.22	USACE - Omaha Anchor	Disagree	Have concerns about 14.2 “multifactor authentication.” Would prefer terms either “multi-authentication.” If we were to implement multifactor we would be removing levels of access to our system and potentially making it easier to hack if they can overcome the multifactor issue.
33.23	Black Hills Corporation	Disagree	If two cyber systems are on the same protected network, and within the same physical boundary, should two-factor authentication be required? We don’t think so, but according to the definition of remote access and this requirement it would be.
33.24	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
33.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes the multifactor controls required in section 14.2 is too specific. “Strong technical controls” is a preferred update to the requirement. There may be better controls from a security and reliability standpoint, but as the requirement stands, Responsible Entities are limited in the technological implementations to support compliance to the requirement.Requirement 14.3 specifying that responsible entities must “deny access by default; [specifying] explicit access permissions” is unclear. Since this is supposed to be related to remote electronic access, the requirement should clarify that the end user is explicitly denied access thru the access point(s) of the network containing the BES Cyber System unless explicitly allowed access into that network.Requirement 14.4 requires the displaying “of an ‘appropriate use banner’ on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.” This appropriate use banner should be required upon every new connection and entry attempt to the BES Cyber System network, for example a firewall or SSL VPN connection that controls remote access. Also, allowance for TFE's in 14.2 through 14.4 should be included.Regarding 14.2, NextEra

#	Organization	Yes or No	Question 33 Comment
			would like clarifaction for the required multifactor authentication controls. Is it required for assets within the boundary or does it only apply to the control of wireless and remote access to electronic access points to BES Cyber Systems? or both?
33.26	Constellation Energy Commodities Group Inc.	Disagree	Provide clarification regarding acceptable use banner (14.4) - in some instances such banners cannot be added to system. Make clear that the requirement may be met by displaying a banner upon workstation sign-on or upon user entry to the remote access environment. What is the specific meaning of authentication controls in 14.1? Since this is called out separately from two-factor authentication, I interpret it to mean that remote access cannot be enabled via generic accounts, only via user specific accounts with authentication (password) known only to the individual. Is that the idea?
33.27	Detroit Edison	Disagree	R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.
33.28	Ameren	Disagree	R14.1 - The complexity and scope of the documentation of the Low Impact Systems will be challenging to keep succinct for auditors.R14.3 - Deny access by default is not needed. Requiring authentication implies access is denied by default.R14.4 - Not all systems support user banners. This will be hard to keep from being a TFE on many “high” systems.
33.29	Southern Company	Disagree	R14.1-4 addresses remote access only and does not include wireless, the table title and R14 includes wireless.
33.30	Entergy	Disagree	R14.2 dictates multifactor authentication controls for only high impact BES Cyber Systems. Entergy recommends serious consideration of extending this to low and medium impact BES Cyber Systems where localized wireless technology is employed.

#	Organization	Yes or No	Question 33 Comment
			Eliminate 14.4. We understand the purpose of this requirement but do not believe that it adds to the protection of any cyber system. If it is to be added then it should be placed outside of the wireless and remote electronic access control section and placed elsewhere. Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
33.31	US Bureau of Reclamation	Disagree	R14.3: Add deny access by default requirement for low systems. Specific access permissions are not required, however.
33.32	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that a definition of what is meant by "multifactor authentication controls" be included in a definition box near R14.
33.33	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal. Criteria in 14.3 and 14.4 are very specific in application of technology that may not be supported by devices in the field. These criteria should be removed or reworded to cover various methods of operation. If the drafting team keeps these requirements the following is our recommended language: R14 Table 14.3: If a BES cyber system component supports explicit access permission capability, the device should deny access by default. R14 Table 14.4: If a BES cyber system component supports notification capability, remote electronic access control device users should be notified that unauthorized use of the system is prohibited.
33.34	MidAmerican Energy Company	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in-scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are

#	Organization	Yes or No	Question 33 Comment
			defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.35	PacifiCorp	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in- scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.36	Bonneville Power Administration	Disagree	The objective of this requirement ('to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 33 Comment
			appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition: Table R14, Section 14.2 is excessive. Given the draft Standard's definition of external connectivity, remote access could also be a case of accessing a system from a nearby system over secured communications paths. An example would be a user on one BES Cyber System accessing another BES Cyber System in the same Control Center. It is not reasonable to justify multi-factor authentication in these circumstances. In addition, many existing systems do not have the capability of enforcing multi-factor authentication. Finally, there are other authentication controls stronger than username/password which are not multifactor: biometric, one time passwords, dial-back, and so forth. Recommendation: Delete the requirement. If not, change the definition of "external connectivity" as discussed in question 13, and change the requirement from "multifactor authentication controls" to "authentication controls stronger than username/password".Section 14.4. There are significant issues with this requirement. - The warning banner is a legal requirement, not a security requirement. Its only purpose is to provide support for legal recourse if someone violates what it says. - No unauthorized person should be accessing High Impact Cyber Systems. Any user with authorized electronic access will have completed security training, which includes proper use of BES Cyber Systems. Any unauthorized user will ignore the banner. - It does not prevent unauthorized access, and therefore does not support the purpose of the requirement. - The requirement has technical feasibility issues. To provide specific scenarios: 1. The user connects from a device controlled by the Responsible Entity, using networks owned by the RE. The user authenticates at the local device. When attempting to connect the the BES Cyber System, the firewall access point allows the traffic, based on the originating point within the trusted network. The user again authenticates at the BES CYber System. At no time does the user authenticate at the access point itself (nor does the rest of Table R14 require authentication at the access point.) In fact, under these circumstances firewalls generally do not have the capability to request authentication or present a banner. 2. The user connects via a

#	Organization	Yes or No	Question 33 Comment
			VPN. The VPN client authenticates the user, then uses a PKI certificate to authenticate to the access point. The user is then granted access to the network and can proceed to authenticate and connect to a BES Cyber System. At no point did the user authenticate to the access point, nor was there an opportunity to present a banner.Recommendation: The best solution is to eliminate the requirement. If the requirement cannot be removed:First, change the definition of remote access and/or external connectivity as discussed above. This would eliminate the requirement to present a banner to users attempting access from equipment belonging to the Responsible Entity. Second, allow the banner to be present at locations other than the access point. A possible revised requirement would be: "Display an "appropriate use banner" to the user that, upon an interactive attempt ..." Also, change "Required" to "Required for external connectivity only".
33.37	Consultant	Disagree	The terminology "wireless and remote access" is redundant. The definition of remote access (near requirement R11) includes wireless access implicitly. Suggest using the defined term "Remote Access" rather the redundant terminology.Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.Items 14.1 & 14.2 - The terminology "is used and/or implemented" seems redundant. It appears that being "implemented" creates the vulnerability, and the requirement for control. Suggest changing the words "is used and/or implemented" to "is implemented".Item 14.3 - This includes two different requirements: (1) Deny access by default & (2) specify explicit access permissions. The first requirement is a technical implementation and should remain here. The second is an account management requirement and should be moved to the account managment requirement R8.
33.38	Minnesota Power	Disagree	These criteria are generally acceptable; however, Minnesota Power requests that the Standards Drafting Team consider defining “authentication controls.”Also in Part 14.2, the requirement regarding the use of multifactor authentication controls sets a technology-specific direction that may not stand over time, including the possibility of

#	Organization	Yes or No	Question 33 Comment
			biometric authentication that, while not multifactor, is a stronger control.
33.39	Dominion Resources Services, Inc.	Disagree	To avoid the potential for TFE's associated with R14.4, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.
33.40	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
33.41	Progress Energy (non-Nuclear)	Disagree	What conditions would dictate different authentication controls for different impact levels? Is it better for them to all be the same?R14.4 is unnecessary. The population of persons granted remote access rights is extremely limited and these people are highly trained and trustworthy. The appropriate use banner is used in situations where a general population was granted this type of access and that is not the case for remote access to any control systems.
33.42	National Grid	Disagree	What types of authentication controls are valid? (Authentication level such as a shared password or a user level control)
33.43	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
33.44	Network & Security Technologies Inc	Disagree	Wording of 14.4 gives the (doubtless unintended) impression a banner must be displayed on the user screen of electronic access control devices. Re-word to clarify banner must be displayed on the user screen of the accessing device.

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R14 has moved to CIP-005-5 R1.

Commenters expressed that the 'deny by default' requirement should also apply to Low impact BES Cyber Systems. In response, the SDT agrees that some network access control should apply to all BES Cyber Systems, including the Low Impact BES Cyber Systems. CIP-005-5 R1 – Electronic Security Perimeter allows considerable flexibility for the entity to determine which security controls to apply, because of the significant number of Low Impact BES Cyber Systems.

Commenters suggested requiring a banner on Medium and Low Impact BES Cyber Systems. However, the SDT disagrees and felt the requirement to have "appropriate use banners" was administrative; therefore, it has been removed.

#	Organization	Yes or No	Question 34 Comment
34.1	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
34.2	Bonneville Power Administration	Agree	But see comments on R14.2, above. In addition, 14.4 is only acceptable if the definitions of remote access and external connectivity are changed, as discussed above. A banner is appropriate for someone accessing a BES Cyber System from completely outside the control of the entity.
34.3	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
34.4	FirstEnergy Corporation	Agree	With the exception of the concerns presented in the previous question.

#	Organization	Yes or No	Question 34 Comment
34.5	Oncor Electric Delivery LLC	Disagree	(R14.2)Multifactor authentication in legacy substation devices is extremely difficult and not needed. Appropriate logging and access controls will eliminate most threats. (R14.4)Appropriate Use Banners are not possible on many legacy dial-up devices used in substations. Appropriate logging and access control will eliminate most threats.
34.6	Southwest Power Pool Regional Entity	Disagree	14.2 and 14.4 should also apply to Medium impact BES Cyber Systems.
34.7	US Army Corps of Engineers, Omaha Distirc	Disagree	14.2 Multifactor authentication will be a major burden for small IT staffs. Standard should offer alternatives to mitigate - stronger passwords and or more frequent password changes.
34.8	WECC	Disagree	14.3 should be required for low impact.Remote access controls should apply to all impact levels.
34.9	Black Hills Corporation	Disagree	14.4 should be “Required” for all. Others are OK.
34.10	ERCOT ISO	Disagree	14.4: Should apply to Medium Impact BES Cyber System.
34.11	Tenaska	Disagree	18.1 all should be each.19.1 Validation of inbound data is more often done on the host application level and not at the boundary or host level.19.2 Is this RTU data? The protection is done at the applications level and I cannot examine data at my perimeter if it is encrypted at the host level.
34.12	Progress Energy (non-Nuclear)	Disagree	Believe it should be required for Low, Medium and High for R14.1, R14.2 and R14.2.
34.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
34.14	The Empire District	Disagree	Comments: We believe items 14.3 and 14.4 are going to set the stage for numerous

#	Organization	Yes or No	Question 34 Comment
	Electric Company		TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access.
34.16	Entergy	Disagree	Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
34.17	Dominion Resources Services, Inc.	Disagree	High Impact should be removed from 14.1 since it is covered by 14.2.
34.18	GE Energy	Disagree	If user accounts are audited on Medium Impact systems (see question 20), there should be an appropriate use banner.
34.19	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
34.20	US Bureau of Reclamation	Disagree	It would seem that this criteria is in conflict with sound business practices. The concept of allowing access by default to Low Impact BES Cyber Systems does not make sense. Add deny access by default requirement for low systems. Specific access permissions are not required, however.
34.21	MidAmerican Energy Company	Disagree	Items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.Table R14 should be rewritten in a manner that minimizes TFEs. As an example, eliminate the word upon in 14.4 to eliminate TFE for systems that can only display banners immediately after access.

#	Organization	Yes or No	Question 34 Comment
34.22	National Grid	Disagree	National Grid suggests having 14.3 for Low Impact systems as well.
34.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes Medium Impact BES Cyber Systems should have to comply with requirement 14.4. However, the rest of the impact levels are appropriate.
34.24	American Municipal Power	Disagree	Please provide a little or no impact category
34.25	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, and Table 14. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
34.26	Garland Power and Light	Disagree	Requirement 14.3 and 14.4 Should add "required" to all impact levels
34.27	USACE HQ	Disagree	Requirements 14.3 should be required for every level of impact.
34.28	San Diego Gas and Electric Co.	Disagree	SDG&E believes that Medium impact assets should also be required to have multifactor authentication controls (within the definition question mentioned in Question 33).
34.29	ISO New England Inc	Disagree	Should apply to all
34.30	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in row 14.2.
34.31	Consultant	Disagree	Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.
34.32	Alberta Electric System Operator	Disagree	The AESO suggests adding the following to Table R14: o 14.3 - Required for Low Impact. o 14.4 - Required for Low and Medium Impact.

#	Organization	Yes or No	Question 34 Comment
34.33	Southern California Edison Company	Disagree	The same authentication methods should be applied to all Levels.Also, SCE requests that the drafting team provide justification for the lack of a deny access by default for low impact system.
34.34	Minnesota Power	Disagree	These impact levels are generally acceptable, however to maintain consistency with Table R10, Parts 10.4 and 10.5, the High Impact cell in Part 14.1 should be blank since it is addressed in Part 14.2.
34.35	American Transmission Company	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.36	Florida Municipal Power Agency	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.37	MRO's NERC Standards Review Subcommittee	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.38	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
34.39	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R14:R14 Table 14.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR14 Table 14.2: Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.3: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.4: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R15 through R19 have moved to CIP-007-5 R1 through R4.

For physical ports and services, several commenters expressed confusion around the term "externally accessible." The SDT agrees, and "externally accessible physical ports" was removed and substituted with physical ports used for "network connectivity, console commands, or removable media."

In addition, for physical ports and services, commenters expressed concern that physical port protection seems unnecessary, since overall physical security and personnel vetting is required, and many devices do not allow for configurable disabling of ports. The SDT agrees the objective of disabling unnecessary physical ports is primarily to prevent accidental propagation of malicious code. In response, the requirement was modified to "restrict" access. A description of acceptable forms of restriction is included in the measures; for example, these could be physically disabling the port or including signage about the use of ports.

For security event monitoring, several commenters stated that there is no need for weekly log review/clarity or manual log review since continuous monitoring is required. The SDT disagrees and references paragraph 528 of the FERC Order 706 that provides context for a weekly log review. The requirement allows for a review to include a sampling or summarization of security event logs.

For security event monitoring, several commenters expressed concern that there is no definition of "cyber security event" (i.e., a normal good logon is a "security event"). The SDT agrees and has modified the requirement to ensure that audit events must be organizationally defined. An enumerated list of events in the Standard is of little value.

For security event monitoring, commenters expressed concern that the requirement can be interpreted to include monitoring and logging for systems that don't support this functionality. The SDT agrees, and in response, this requirement was modified to apply log generation to the BES Cyber System (rather than the component) and allow the entity to define the generated events to audit.

For patch management, commenters expressed concern that not every patch is applicable to a BES Cyber System. The SDT agrees with this observation and notes that this requirement should be covered through the patch evaluation process. The focus of the requirement should be a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner."

For patch management, commenters expressed concern that flexibility is needed for the installation of patches; these dates can be based on equipment outage schedules, which could change the frequently or grid conditions that may or may not allow patching. The SDT agrees that the date of installation needs to be flexible to take into account equipment outage situations or high risk system conditions that could present an undesirable time for installing patches. Requiring an install date for the patches does nothing to improve BES Cyber System reliability. The overall goal of security patching should be to decrease the latency between security patch release date, application vendor certification date, entity testing, and implementation date. The SDT has revised the patch management requirements to achieve this goal.

For patch management, some commenters posed the question of what starts the clock for patching (release vs. availability vs. OS vendor vs. control system vendor). The SDT agrees there should be a starting point, but requiring an install date for the patches does nothing to improve BES Cyber System reliability. In response, the requirement has been modified so that Responsible Entities are required to create or revise an implementation plan within 30 days of the patch release from the identified source of the patches.

For malicious code prevention, commenters posed the question of whether the standard requires testing against actual malicious code. In response, the SDT disagrees and feels the intent was strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.. This has been clarified in the guidance for the standards.

For malicious code prevention, commenters expressed there is still nothing specifying that malicious code prevention does not apply to field or network equipment. The SDT agrees, and in response, the requirement was modified to include malware prevention processes. It is now much more a “what” and not a “how” level of requirement.

#	Organization	Yes or No	Question 35 Comment
35.1	Dairyland Power Cooperative		15. It is good that this section is not wrongly specific as CIP-007:R4 is. This should allow for solutions that are not specifically signature based. This should allow for a network-based solution rather than individual solutions on each component. BES systems should not be used like typical Internet user systems, and therefore it should not be enforced that Internet user solutions be applied.16.2 requires a fixed implementation schedule of patches. However there should be an allowance that not every little security patch needs application, and it should be acceptable to defer insignificant patches until a later date when a significant patch needs to be applied. Additional controls to compensate may not be needed other than the security already designed to isolate a BES cyber system.17.1 Focusing on documenting the process to

#	Organization	Yes or No	Question 35 Comment
			harden seems wrong-the focus should be on requiring/verifying that a system is hardened. 19.1/19.2 How is validating inbound data (19.1) different than determining if inbound data has been compromised (19.2)? Was the intent of 19.1 to validate/authenticate the remote host/application on inbound connection? There should be requirements to restrict inbound connections from known remotes only. Validation of data should be defined. Perhaps inbound need definition too. Is it inbound initiated connection vs. data transferred inbound regardless of initiation direction?
35.2	National Rural Electric Cooperative Association (NRECA)		In R17.1, what specifically is the mitigation plan required to address/accomplish? Please ensure this requirement is clarified to explain this better.
35.3	Progress Energy (non-Nuclear)		R16.2 fixed dates for generating stations that depend on outages for implementing this is impractical as outage dates frequently change. Also, the ambiguity from v1-v3 (resulting in so many TFEs) remains here and still needs to be addressed.R17.2 - do not understand the externally accessible port requirement, there are no externally accessible physical ports outside of the six-walled boundaries, requirement not needed.CIP-011 R15 - Require detecting and responding to introduction of malicious for Medium Impact Cyber Systems which could be an electronic relay, what if there isn't a commercial solution for installing malware detection for relays or any other electronic device that runs with only proprietary closed firmware? Would it be impractical to require this only for devices that run a general purpose programmable commercially available operating system such as Microsoft Windows Operating System variants/UNIX and LINUX variants/SUN SOLARIS variants/Apple OS variants, etc --- or Is there going to be TFE process for these such as for switches, etc.?We like that this requirement does not require the use of traditional virus protection software.CIP-011 R18.3 - Requirement to keep logs of system events for 1 year for each high impact device could be massive in terms of storage and archive and may not be technically feasible for electronic relays.CIP-011 - R19 table - Need additional clarification as to what data validation methods (data integrity checking) are to be

#	Organization	Yes or No	Question 35 Comment
			employed. Can this be satisfied solely by employing Secure FTP or Secure ICCP for all inbound data?Calibration ports on programmable relays must remain open for calibration but this requirement would require rendering them unusable. We want to ensure this use is interpreted as “normal” operations.CIP-011-1 R15.3 (System Security) - The statement ‘Implement processes to test and update malicious code protections’ should be clarified to specify that in no case should malicious code be purposefully exposed to operational BES Cyber Systems as a part of this testing.CIP-011-1 R16.2 (Security Patch Management) - Requiring a ‘fixed date for either installation of the applicable patches or completion of mitigating measures that address the vulnerability’ is too inflexible in a real world where such activities may need to be accomplished during the next plant outage.CIP-011-1 R19 (Communications and Data Integrity) - This sounds like a ‘best practices’ type of requirement, but depending on how BES Cyber Systems are defined, this could require redesign/implementation of front-end processors on all inbound traffic to all Control Center BES Cyber Systems. Such a requirement cannot be quickly implemented without significant potential impact on the BES. We would like to suggest that this be listed as a requirement for any new BES Cyber System implemented at a Control Center.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”
35.4	FEUS	Agree	Agree with Comments: The drafting team should consider revising the wording of 17.1 from ‘implement a mitigation plan’ to ‘implement mitigating measures’ to reduce confusion with mitigation plans submitted to correct a violation.
35.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R15.This is very poorly worded, and too open to interpretation on a number of areas.15.1 - how do you audit this item? FMPA suggests: “Document and implement procedures implemented to limit the

#	Organization	Yes or No	Question 35 Comment
			propagation of malicious code."15.3 - This could be interpreted to read that you need a full-scale development environment/copy of your production system to introduce malware to and guage the responsiveness of the mitigation techniques you put in place. If the intent of the standards is to protect the BES, by testing malicious code on systems that's not helping anyone. Time should be spent making sure it doesn't happen, not testing to see what happens when you introduce it. FMPA suggests "Review logs of malware detection systems within the following time periods: 30 calendar days for medium impact, 7 calendar days for high impact."R16.FMPA agrees with the intent of this standard; however there are some underlying issues that should be addressed before the standard is implemented. One such example might be a requirement to change out hardware to meet a new patch released by a vendor; before equipment is purchased it has to be tested - in some cases equipment shortages may make it impossible to comply with the 30-day requirement.R17.17.1 - How does "external connectivity" apply to network ports being shut down? Does that mean for devices that route data to other external networks?17.2 - What does "externally accessible physical ports" mean? Does this refer to ports that are connected via Ethernet cable to an area outside of the protected area? If so, the standard should explicitly say this.R18.18.1 - Requiring components that do not have logging capabilities to be monitored could be a real problem. While there are a number of technical ways to accomplish logging of systems, there is no clarity in the standard as to what is and is not acceptable levels of logging on a device - this needs to be better defined. FMPA suggests "Implement automated tools or organizational processes to monitor and log all available system events that are related to cyber security for all BES Cyber System components." This would give more flexibility in collecting data from other centralized devices (such as SCADA systems) and limit the data collection to what is available.18.2 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.3 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.4- what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining

#	Organization	Yes or No	Question 35 Comment
			criteria?R19.This is a very difficult implementation. As a general comment, if the intent is to protect the BES, perhaps more effort spent on ensuring that no unauthorized machine can communicate with BES components is a better place to spend effort.
35.6	Emerson Process Management	Agree	For R16, keeping cyber systems current so that they can be supported with security patches is very essential in maintaining system security. This should be a requirement under R16 and provide a TFE opportunity if this can not be met immediately, but with a auditable mediation plan.
35.7	SCE&G	Agree	How does the SDT intend to account for equipment incapable of supporting certain requirement (e.g. malicious code)? Will the TFE process be utilized. If so, it would be helpful for entities to see where the SDT envisions initially allowing for TFEs.
35.8	Southern California Edison Company	Agree	SCE requests guidance on whether the list of requirements apply to each component or if they only apply at a system level. For instance, can testing and malicious code protection in R15.3 be performed at a system level or should each component demonstrate this capability?A separate standard with highly prescriptive methods to document situations where it is not technically possible to implement a certain control, controlled and auditable documentation of mitigation plans will enable registered entities to record instances of non-conformity.A prime example would be that R 17.1 may be impossible to implement because of the technical design for a particular device. While the standard allows or a mitigation plan, the draft does not indicate whether or not the lack of such capability is a case of strict compliance.
35.9	Nebraska Public Power District	Agree	Security protection for cyber components that cannot connect to an external network do not require the same level of protection as those cyber components with connectivity to an external network. I recommend adding an exclusion to R16 and R18 for cyber components that cannot be connected to an external network.
35.10	USACE - Omaha Anchor	Agree	This is a less strenuous requirement than previous version of CIP. Previously every

#	Organization	Yes or No	Question 35 Comment
			item in the ESP had to comply - requirement states every system must comply - implying not every item must comply as long as the system does.
35.11	Xcel Energy	Agree	While we agree overall, we do have some suggestions/requests for clarification1. R15 to R19 should allow for TFEs2. R18.4/R20.6 We do not agree with a need to review logs every 7 days.3. R19.1 Further definition is needed of the expectation to "Validate data". Our concern is if were to include RTU data that can not be validated. A TFE allowance may be needed in this case.
35.12	Independent Electricity System Operator	Disagree	- R15.1 define malicious code. For R15 and sub requirements, does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- - R16.2 does not require that the mitigatio
35.13	National Grid	Disagree	1. Inconsistency in using "processes" versus "one or more processes" in all requirements. National Grid suggests using "one or more processes". 2. Recommend new wording for 15.2 similar to 26.2 -Respond to the detection of malicious code.3. Recommend new wording for 15.3 - Implement processes to test and update protections in place to respond to the detection of malicious code.4. Recommend using the controls for Low Impact BES CS too since once the code is propagated it spreads across network irrespective of low/medium/high BES CS.5. Recommend changing 16.1 from "release" to "availability". 6. Recommend removing "with a fixed date" from 16.2 because the cyber system may not be available for maintenance due to grid system conditions.7. Request a R17 local definition of "attack surface".8. 17.2 - recommend changing "externally accessible physical ports" to "externally accessible physical communication ports". Also please clarify external to what.9. Request a local definition of "security events".10. In 18.2, is the SDT considering providing the timeline for issuing alerts and also to respond to those alerts? 11. Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.12. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - "Some manual review of logs to improve automated detection settings, even if

#	Organization	Yes or No	Question 35 Comment
			alerts are employed on the logs."13. Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days.14. Recommend that R19 should "insure the integrity of the data."15. Recommend that 19.1 should be "Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.16. Recommend that 19.2 should be "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.14	Southwest Power Pool Regional Entity	Disagree	15.1: The criteria should "limit the introduction and propagation of malicious code." 15.3 should require such testing prior to implementation rather than assuming. The objective statements in R16 and R18 are prescribing a requirement through the use of the statement "to ensure." 16.1: Clarify who is "releasing" the security patch. For example, is it being released by the operating system vendor (e.g., Microsoft) or the third-party application vendor (e.g., the EMS/SCADA vendor) subsequently certifying the patch against the supported application? 16.2: Clarify that compensating measures must be implemented within a prescribed timeframe after determining a security patch to be applicable unless the patch is installed within that prescribed timeframe. If compensating measures are implemented as an interim measure, they must remain in place until the security patch is installed with the understanding that the compensating measures can be improved during the interim period. 17.1: The term "mitigation plan" has an enforcement connotation. Consider requiring the documentation and implementation of compensating measures instead. 17 overall: there are a number of additional system hardening techniques other than disabling logical and physical ports. Additional hardening should be required for High impact systems. See the baseline configurations found on the Center for Internet Security web site for additional information. 18.2: This requirement presumes 100 percent availability of the monitoring process, which is unreasonable for automated solutions. Additionally, prescribe a timeframe for issuing alerts for detected system events.

#	Organization	Yes or No	Question 35 Comment
			18.3: Consider rewording the criteria to read “Maintain logs of system events related to cyber security for the specified time period.” 18.4: The requirement to maintain records documenting the review of logs is a compliance evidence issue and should not be included in the requirement. 19.1: Questionable if this is an auditable requirement. Clarify what is intended by inbound data validation? 19.2: Encrypted data does not mean uncompromised / valid data. Is this requirement essentially the same as 19.1? Is this asking for the validation process to be external to the normal validation processes included in the application software running on the BES Cyber System? Is this an indirect requirement to implement “Secure ICCP?”
35.15	Regulatory Compliance	Disagree	15.3 - STRIKE "testing" from the criteria. There is very little bennefit to test signature. 16.1a - Need clarification on components not patchable.16.b for those devices that are patchable - assessment of patches within 30 days.16.2 - Clarification - assess whwther vulnerabilities exist for a device.17.2 - need definition of external connectivity - more guidance on physical switch ports18.4 - propose 30 days for 30 days for manual review of automated systems - it is redundantR19 - wait and see - need guidance
35.16	LADWP	Disagree	15.3 states to test and update malicious code protections. Testing the code protections should be removed.
35.17	Network & Security Technologies Inc	Disagree	16.1 - Please clarify meaning of “release” of security patches by specifying patch source (the corporation, organization, or individual that wrote it?). This matters because some application vendors combine O/S patches in “bundles” they release to customers with service contracts.17.2 - Given the restrictions on physical access and the requirements to train and background check personnel with unescorted physical access to BES Cyber Systems, this requirement seems unnecessary. Moreover, on any given day it may be very difficult to predict whether a given physical port might be of use in an emergency troubleshooting or restoration situation. Could be contentious during audits.R18 - Does the SDT intend that Responsible Entities be able to, if necessary, determine what user(s) was on what system and when? If so, this

#	Organization	Yes or No	Question 35 Comment
			requirement should be made explicit.19.1 - Please clarify types of “inbound” data this requirement applies to. Operational data only? Mirrored backup data received at a backup Control Center from a primary Control Center? An emergency “hot fix” from a SCADA/EMS vendor? Meaning of “validate” also needs to be clarified. SDT has solicited input on which proposed requirements should be “eligible” for TFEs - surely this is one. Depending on the intent of this requirement, “data validation” may be something that can only be done in a useful/meaningful way by application logic.19.2 - We consider this to be an unenforceable requirement and therefore suggest it be dropped unless compelling evidence exists that replay and/or MITM attacks are a real and growing problem. Investigating a single occurrence of invalid data could consume scores of person-hours, lengthy interactions with communication providers, other Responsible Entities (e.g., for a BA that operates a Control Center that receives all its data feeds from other companies), and even law enforcement with no guarantee of success. Cryptographic protection of in-transit data, even if achievable (probably not unless a Responsible Entity owns and/or controls both ends of the data feed), offers no protection against corruption of data at the source and could also cause latency issues.
35.18	ERCOT ISO	Disagree	16.1: Clarify “release” from whom--the product vendor (e.g., Microsoft) or other vendor that prohibits installation of a patch until certified with their applications?17.1: Compensating measures should be allowed in instances where a mitigation plan to achieve strict compliance is not possible. 18.2: Specify the timing for responding to alerts. 18.3: Should be removed to data retention section. 18.4: Should address the use of automated security event monitoring systems. TFEs should be allowed for R16. TFEs should be allowed for R17.TFEs should be allowed for R18.TFEs should be allowed for R19.
35.19	MidAmerican Energy Company	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation

#	Organization	Yes or No	Question 35 Comment
			to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.20	PacifiCorp	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.21	ReliabilityFirst Staff	Disagree	16.2 - need a time frame (60 days), for row 17.1 does there need to be a time frame for implementation of a mitigation plan?
35.22	Luminant	Disagree	17.1 implement a mitigation plan or compensitory measures
35.23	Progress Energy - Nuclear Generation	Disagree	Agree with Table 15, R16.2, Table 17, 18.1 AND 18.2. R15-R19 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments. Durations for R16.1, R18.3, and R18.4 should align with comments in Attachment 1.
35.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.15.3 should include more clarification on what "testing" entails and whether that just refers to signature updates.Recommend replacement of the word "known" with "discovered" in R18. 18.4: more clarity

#	Organization	Yes or No	Question 35 Comment
			needed regarding the allowance of both automated and manual review of logs. R19 creates a potentially impossible level of obligation. Recommend striking.
35.25	American Transmission Company	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.26	MRO's NERC Standards Review Subcommittee	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.27	Western Area Power Administration	Disagree	Assuming one can detect and respond to the introduction of malicious code, how is it expected that we limit propagation of malicious code? By definition, malicious code is often not detected, and if it is detected (by virus prevention software, for instance), that software generally quarantines or deleted the malicious code automatically. This section seems to need a little thought as to what is really being required. This opens up technical interpretation of what "limits" malcode. This also assumes only a specific

#	Organization	Yes or No	Question 35 Comment
			vector (rootkit, malware, virus/worm) but doesn't address Denial of Service attacks which could be much more serious. Maybe they need to specify intent. R16: A plan for every patch as opposed to relying on the change control process? This seems excessive.R17: Seems to be an improvement. For 17.2, does this mean plug up physical ports like USB? This is unclear. If it does, cannot rely on physical perimeter for protection?R19: Since this applies only to external connectivity (ICCP connections or equivalent), how is it intended that we validate the actual data coming into the system? What level of validation? Ex: end-point validation (ipsec and certs) vs application endpoint (ssl), the way this is worded it goes WAY beyond this. This is not a communications validation issue. Are they wanting to get to MITM attacks? If so it isn't clear.
35.28	E.ON U.S.	Disagree	CIP-011, R15.1 Limiting propagation of malicious code is an integral part of any standard A/V protection. If this requirement is calling for something more than this then the requirement should be clarified to remove this ambiguity. If it is one and the same as R15.2, then E ON U.S. suggests combining these two sub-requirements.CIP-011, R17.2 The term "...externally accessible physical ports" is ambiguous. Does this refer any externally-facing port through which a party may attempt to gain unauthorized electronic access to a BES Cyber System Component? Or, does this refer to an externally-facing port directly on the BES CSC itself?CIP-011, R18.3 The requirement to maintain logs for one year is a significant burden. This can be a tremendous amount of data depending on the level of logging enabled.CIP-011, R18.4The expectations regarding review of logs should be more clearly defined. The whole point in having "continuous security monitoring for detected system events" is to avoid the extremely burdensome requirement of manually sifting through tremendous volumes of log data. Though some mechanism should be in place to ensure the automated logging and alert systems are not disabled, the requirement to manually review system logs is excessive and provides little if any security enhancement.CIP-011, R19.1The expectations for validation of data inbound to a BES Cyber System should be more clearly defined. How is this reasonable to be accomplished? Parameter checking is already a common mechanism within most

#	Organization	Yes or No	Question 35 Comment
			SCADA / DCS systems, but this does not protect against tampering or data manipulation within the prescribed bounds for a given data point.CIP-011, R19.2 Same comment as for R19.1...how is this to be accomplished?
35.29	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
35.30	The Empire District Electric Company	Disagree	Comments: As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.31	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy has the following concerns with requirements R15 - R19:R15 - A TFE may be required for programmable electronic devices within a substation environment where is not technically feasible to manage malicious code.R16.1 - The definition of a “release” needs to allow for vendor verification of the applicability of a patch to a given systems functionality before the thirty day clock begins.R17.2 - CenterPoint Energy recommends clarification as to what are considered "externally accessible physical ports" R18 - the phrase "related to cyber security" is ambiguous. R18.2 -implementing "continuous security monitoring that issue alerts for detected system events related to cyber security" would seem to require installation of external communications to remote substations increasing their vulnerability. R18.4 - A manual review every 7 calendar days is overly burdensome. Automated processes are already mandated to detect and alert personnel of cyber security events. CenterPoint Energy recommends a 30 day review.R19.1 - Concerned

#	Organization	Yes or No	Question 35 Comment
			with the method to "validate data inbound to a BES Cyber System". This requirement is intended to address data integrity issues associated with man-in-the-middle attacks, but it does not specifically address the issue. It leaves open the issue of data which was intentionally or unintentionally manipulated by responsible entities. The issue becomes something different if our Control Center must validate data from a Reliability Coordinator or Transmission Operator which has been intentionally or unintentionally modified by trusted personnel. Data integrity implies encryption. This requirement should state: “One or more of the following encryption standards are required to ensure data integrity inbound to the Control Center.R19.2 - Concerned with ability to provide evidence that we "evaluate invalid data inbound to a BES Cyber System" to determine whether the data has been compromised maliciously with current systems capability. As stated previously, this requirement does not address the issue of malicious entities entering malicious data from the endpoints. This requirement is an attempt to address issues associated with MITM attacks. Inherent in the various SCADA protocols is error detection and data delivery, but not data integrity. The ICCP protocol is encapsulated within TCP/IP. The TCP/IP protocol will ensure communication reliability and error detection, but it will not ensure data integrity.
35.32	Entergy	Disagree	Entergy suggests making requirements in general apply to high, medium, and low assets alike and provide a footnote to allow a TFE for assets which are not capable of meeting the requirements. 17.1 suggests that unused network ports only have to be disabled in the event there is external connectivity. This requirement appears to be extremely relaxed from version 1. The current language suggests that the perimeter firewall can be used to control port usage thus relieving the requirement to control at the asset itself. In 17.2 there is a reference to externally accessible physical network ports. Entergy suggests language change to just say “unused physical network ports.” In 18.2 there is a time requirement of maintaining logs for 1 year for high and 90 days for medium. Maintaining logs for 1 year can be problematic due to the amount of space required. Suggest making requirement for 90 days for high, medium and adding the same requirement for low assets. Also suggest adding a footnote to allow TFE for

#	Organization	Yes or No	Question 35 Comment
			assets that are unable to meet requirements. In R19 it appears the requirement is to encrypt all data coming into a BES Cyber System. The intent is to ensure data integrity. Most EMS systems have CRC checks, and reasonability checks, etc., embedded in the systems to validate the integrity of the data being received. Entergy does not believe that encryption is required for all digital data as it greatly increases overhead, operation and troubleshooting of the data networks. Entergy suggests that encryption should be required for remote access as remote access connectivity many times traverses the Internet or some non-private network links at some point. Entergy suggests providing alternate methods to validate inbound data rather than encryption.
35.33	Southern Company	Disagree	For 17.2, what does this mean? An externally accessible physical port would require a switch next to an open window or something.R15.3 requires testing of malicious code protections. This is an effort better left for malware protection suppliers. Often only the production system is available to the end user, the quantity and frequency of malware release prohibit an effective end user test program.R16.1 requires assessment of security patches within 30 days of release. This assessment is typically performed by control system supplier to assure that no adverse impact occurs to their product. Often only the production system is available to the end user. The end user has no control over vendor testing schedules. If this requirement is placed on the end user MS KB977165 type “blue screen” events may occur.R16.2 The requirement of a fixed date for patch installation may not be possible in all cases if a system restart is required for an operating unit.For R15 & R16, there is the potential that implementing malicious code detection and security patch management on substation devices could interfere with the primary function of these substation devices which is the reliable delivery of power.For R17.2, what will be considered acceptable for rendering physical ports unusable? We should not be required to permanently disable ports thereby making the ports unavailable for future use.For R18, not all BES Cyber System components in substations are capable of monitoring and logging system events.For R18, implementing security monitoring processes on substation devices may interfere with the primary function of these substations devices which is the reliable delivery of

#	Organization	Yes or No	Question 35 Comment
			power.R18.2 Clarify intention, is continuous monitoring with manual review of logged alerts acceptable? What is a "detected system event"? Is a single or double incorrect password attempt an alarmed event?R18.1 requires an automated log system R18.4 requires a review of log events. Is a manual review of all logs required in an automated system or just the alarms?
35.34	Detroit Edison	Disagree	In 15.2, "respond" is vague. Propose rephrase to read "Detect the introduction and mitigate the effects of malicious code."Remove table entry 19.1 since it is redundant to 19.2.The term "applicability" in 16.1 is vague. Consider introducing vulnerability severity classifications to patch management that determines the action and timetable required. Please note that this is submitted for consideration as a concept. The language and time tables will need further review and editing before this would be ready to add to the standard. o Level 4 - Intruders can easily gain control of a BES Cyber System Component, which can lead to the compromise of BES Cyber System security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the introduction of backdoors. High: patch within 7 days; Medium: patch within 14 days; Low: patch within 30 days. o Level 3 - Intruders can possibly gain control of a BES Cyber System Component, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. High: patch within 14 days; Medium: patch within 30 days; Low: patch within 90 days. o Level 2 - Intruders may be able to gain access to specific information stored on a BES Cyber System Component, including security settings. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files, directory browsing, disclosure of filtering rules and security mechanisms, and unauthorized use of services. High: patch within 30 days; Medium: patch within 60 days; Low: patch during next system maintenance window. o Level 1 - Intruders may be able to collect sensitive information from a BES Cyber System Component, such as the precise version of software installed, open ports, services, etc. High: during next system maintenance window; Medium: during next

#	Organization	Yes or No	Question 35 Comment
			system maintenance window; Low: Patch during next system maintenance window.
35.35	RRI Energy	Disagree	In regards to 17.1, for clarification purposes, based on the definition of external connectivity written in the Standard, if a web server is actively listened on port 80 inside the BES boundary protection but is not accessible externally from the outside of the BES boundary protection, the Responsible Entity does not have to report and assess that port and service.In R17.2, what does externally accessible mean? Ex. Physical port is on a device that is in a cabinet, the cabinet is within a building, and the building is within a fence-lined property. Is the port non-accessible? What type of physical ports are we trying to protect? Is it only physical "network" ports? How about USB ports, PC (PCMCIA) Card slots, CD/DVD drives?Not all devices can be logged such as PLC's, meters, etc.; therefore 18.1 should allow for a TFE.In regards to R19, what defines an internal versus external boundary. Within a single facility, are all boundaries internal? If cables transverse hallways between "computer rooms" within a Control Center does an external connection exist? Can a back-up control center be an extension of a primary control center where all data connections between the control centers are considered "internal"?
35.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
35.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R16, but recommends changes as follows: o Regarding Part 16.2, this requirement contains no timeframe by which this schedule must be developed. If it was intended that the development of this schedule is to coincide with the activity described in Part 16.1, then that should be explicitly stated. Also, there is no limitation regarding how far in the future is reasonable to set the "fixed date." Minnesota Power recommends that if a timeframe for the "fixed date" is not established in the Standard then there should be a stipulation that if the date for installation of the patch is greater than a pre-determined amount (say 45 days), then mitigating measures need to be in place until the security patch is implemented.Minnesota Power generally agrees with the

#	Organization	Yes or No	Question 35 Comment
			proposed Requirements R17, but recommends changes as follows: o Regarding Part 17.1, the first sentence creates some confusion. Minnesota Power recommends that it be reworded as follows: “One or more processes to ensure that for each BES Cyber System Component, only those network accessible ports and services that are required for normal and emergency operations are enabled.” o For Part 17.2, is it the Standards Drafting Teams intent that a CD or DVD drive be considered an “externally accessible physical port?” If so, this should be explicitly defined. Logically, mounting a DVD is no different than plugging a memory stick into a USB port.Minnesota Power generally agrees with the proposed Requirements R18, but recommends changes as follows: o If it is the Standards Drafting Teams intent that Requirement R18 apply only to cyber security events, then Minnesota Power recommends that the term “security events,” which is used throughout this requirement, is reworded to state “cyber security events.” o Regarding Part 18.1, the Standards Drafting Team should consider clarifying the timeframe within which the monitoring of system events should occur (i.e., real-time, minutes, hours, days, etc.). If monitoring is done using a manual process, rather than an automated tool, real-time may not be possible, and guidelines should be established regarding how quickly events must be examined. o Is it the Standards Drafting Teams intent that Part 18.1 address the collection of security events into logs and Part 18.2 address the process to review and act upon the logs collected under Part 18.1? If so, the Standards Drafting Team should consider wording that would clarify the differences between these two Parts. o In Part 18.2, does the term “continuous” refer to “real-time?” If so, Minnesota Power recommends changing the term to real-time to avoid confusion. o Minnesota Power recommends rewording Part 18.3 as follows: "Retain logs of system events related to cyber security for the specified time period." o Minnesota Power recommends communicating all time frames in calendar days to eliminate confusion regarding what constitutes “1 year.” o Regarding Part 18.4, if 18.2 provides for “continuous” monitoring of system events for these same systems, why is it also required that a Registered Entity manually review these logs? In addition, can the Standards Drafting Team provide guidance regarding what should be included in this review? On an SEIM, for instance,

#	Organization	Yes or No	Question 35 Comment
			these logs can be enormous - to the point that manual review is not possible within reasonable time constraints.Minnesota Power generally agrees with the proposed Requirements R19, but recommends changes as follows: o Regarding Part 19.1, How, in real-time operation, can external data be validated (protocols already validate message structure)? For example, an LBA receives unit set-points from its ISO-BA via ICCP. If the data being received is within operating limits for that unit, it is "valid." The ISO may truly be requesting the unit to drop by xx MW. How is that differentiated from someone altering an inbound message to maliciously tell a unit to drop by the same xx MW value? The process for echoing values back to the external system does not solve this, since this, too, can be manipulated. o Part 19.2 appears to be a specific instance of Part 19.1 and given that this Part starts with the phrase "Where not cryptographically protected," it seems that Part 19.1 may be misstated. Is Part 19.1 supposed to discuss "protecting" inbound data, rather than "validating" it, via encryption, authentication, etc.? Also, in Part 19.2, what constitutes "invalid" data? Is this data which is outside of normal operating limits? Or maybe outside of reasonability limits? Again, maliciously inserting perfectly normal or valid data could have detrimental effects to the BES, whereas "invalid data" should, by default, be thrown out by normal processing.
35.38	Idaho Power Company	Disagree	Need to put a limit on how far out the fixed date should occur for implementation or mitigation of security patches. R18 refers to security events but the sub-requirements refer to system events related to cyber security. Need to make this clearer that the focus is on abnormal system events as a normal authorized log-in is a normal security event but not one that needs review or response.
35.39	NextEra Energy Corporate Compliance	Disagree	NextEra believes the current language did not provide clear guidance and is too lax which leaves room for interpretation. The following are the recommended updates for the requirements:15.1 - Implement technical, procedural and/or process controls to limit the impact of code which modifies or destroys data, steal data, allow unauthorized access Exploits or damage a system, and does something that user did not intend to do. o Implement technical controls, where technically feasible, to

#	Organization	Yes or No	Question 35 Comment
			detect and mitigate malicious code o Implement technical and/or procedural controls to limit the propagation of malicious code o Implement technical and/or process and procedural controls to respond to introduction of malicious code15.2 - Malicious code protections should be updated at least on a quarterly basis if applicable updates are available and technically feasible. Updates should be tested prior to implementation to ensure no adverse impact by the software updates.As far as the order of requirements, detection should come first and it should be a requirement by itself. Combined 15.1 and 15.2 and removed 15.3 from the initial version.NextEra believes the implementation of processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated was not clearly identifiedThe current language did not provide clear guidance and left room for interpretation. The following are the recommended updates for the requirement: 16.1 - The Responsible Entity shall establish a security patch management assessment program to track, evaluate, and test cyber security patches within 30 calendar days of their release to validate their applicability to its BES Cyber Systems.16.2 - The Responsible Entity shall develop an implementation schedule with a fixed date for either installation of the applicable security patches or the completion of mitigating measures that address the vulnerability if application of the security patch is not technically feasible.It should be stated that there needs to be a program to track, evaluate, and test cyber security patches within the defined timeframe that are applicable to the BES Cyber System.It is also recommended that there is more in depth guidance on the implementation schedule.CIP-011-1/R17Did not account for technical feasibility for disabling of ports.The following are the recommended updates to the requirements:17.1 - Implementation of process (es) to ensure that only those network accessible ports and services required for normal and emergency operations are enabled. In cases where unused network accessible ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document and implement compensating measures to mitigate the risk of exposure.If it is not technically feasible, the entity must have documented compensating measures to mitigate the

#	Organization	Yes or No	Question 35 Comment
			risk of exposure. This requirement should be applied to Medium and High BES Cyber Systems.The CIP CIP-011-1 Table R18 - Security Event Monitoring to ensure that security events are known, logged, and responded to on BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates: 18.1 - Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components, where technical feasible. Instances, that are not technical feasible the Responsible Entity shall implement manual processes to mitigate risk exposure.18.2 - Implement and document security processes for continuous (24/7 365 days, except when conducting system maintenance of the monitoring devices) security monitoring that issue alerts for detected system events related to cyber security.18.3 - Maintain system logs of system events where technical feasible, related to cyber security within the specified time period. If not technically feasible, the Responsible Entity shall document and implement manual processes to mitigate risk exposure.18.4 - The Responsible Entity shall verify that the log and alerting system is working in the time intervals mentioned. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs within 90 daysAdded language provides more definition.The CIP-011-1 Table R19 - Communications and Data Integrity to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates:19.1 - Validate data inbound in the Control Center for specific connections and verify if those are the correct connections. 19.2 - Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to the BES Cyber System in a Control center to determine whether the data has been compromised. All unauthorized access attempts to a control center must be identified and investigated.Added language provides more definition.Also, In 15.1, please clarify the term "limit propagation". How would a Responsibility Entitity demonstrate the compliance to 15.1? Is a documented

#	Organization	Yes or No	Question 35 Comment
			technical or procedural control to limit the propagartion of malicious code sufficient? Furthermore, NextEra asks that examples be provided on how to meet this requirement at BES Transmission Facilities where all BES Cyber System Components are not capable of running anti-virus software.In 16.1, is the assessment necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, what is a reasonable "implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability"In 16.2, is an implementation schedule necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, if the "installation of the applicable security patches" would cause a risk on the availability and performance of BES Cyber System, is it sufficient to complete the mitigation measures that address the vulnerability? If so, we propose that the language of 16.2 be modified to have this as an option in lieu of the installation of the applicable security patchesIn 17.1, does this apply only to BES Cyber System Components that are accessible from the outside? If yes, does this apply only to the ports that are externally connected or for all ports if the BES Cyber system Component has external connectivity?In 18.4, please clarify the term "review logs of system events" -- how will compliance be demonstrated?In 19.1, how do we validate data inbound to a BES Cyber System in a Control Center? Please provide methods that could be employed by the Responsible Entity. Could 19.1 and 19.2 be simplifeid by jjust requiring cryptographic protection for High Impact BES Cyber System in a Control Center?Regarding R-18, the log review of assets is too short. (i.e. 30 / 7 days). With this constraint, there will be limited knowledgeable personnel available for review. Some systems do not provide data to allow for this type of analysis. Need support from external vendors, which may not be feasible on a weekly / monthly basis. Due to volume in the industry, it is anticipated that vendor resources will be limited to support us in this capacity. NextEra suggests at least quarterly for Medium / High.18.1 states logging events "related to cyber security". This is subject to broad interpretation and should be clarified. NextEra suggest providing specific examples, such as: Abnormal System Shutdown Account Lockouts Admin User Account Changes

#	Organization	Yes or No	Question 35 Comment
			All Domain Account Logon Failures All Group Account Changes All User Account Changes All Policy Changes Domain Admin Acct Logon Failures Domain Admins-Admin Group Acct ChgDomain Admins-Admin Group ChgDomain Trust Rel Policy ChangesEvent Log FullLogon Logoff SummaryNormal System Startup-ShutdownPassword Changes and ResetsSecurity Log ResetsSrv Wkst All Logon FailuresTerm Srv All Logon Logoff SuccessesTerm Srv All Session Discon-ReconUser Account Creation or DeletionUser Account Password ChangesUser Rights Policy Changes18.2 uses the term "issue alerts" which could imply alarming or otherwise performing a notification. If NextEra had to raise an alert for every system event we could potentially have a continuous alarm stream. If it is determined that event alarms are necessary, then the events have to be further defined and our systems have to be specifically tuned on site for the real running environment.NextEra recommends defining the term further to either include explicit alarm/notification or not. Would also push further for alert in the form of logging to be reviewed or alarmed for review.19.1 states validate data inbound to a control center. Data should be further classified as data directly related to real-time BES operation. If a Monitoring and Diagnostics Center is classified a control center they would potentially have to perform data validation on all historical data made available to that center, depending on interpretation. An alternative is to further classify or define "validate" to allow validation simply by verification of traffic from a reliable source, i.e. identifying the source historical data server.NextEra proposes considering validation of the originating source rather than validating the data itself.
35.40	Con Edison of New York	Disagree	o R16.2 requires a “fixed date” for apply security patches or mitigation. This requirement does not take into consideration that entities may require vendors to test the patches on their systems before they will be applied to operational systems. The release dates for these patches is not fixed by the vendor. The requirement should allow for the planned install date to be a fixed period after the patch is tested and available to the user. A fixed date may be a challenge when predicated on manufacturer certification which may introduce unnecessary risks to operations. o R17.1 “external connectivity” is expected to mean external to the (ESP) boundary. o

#	Organization	Yes or No	Question 35 Comment
			R17.2 It is not clear what externally accessible physical ports includes. External to the location or external to the device (i.e.: located on the front of the workstations) o R18.2 - need clarification on type of events that need continuous monitoring; security logs can be voluminous with excessive informational notifications o R18.4 - if automated tools are used this should not be required o R19 - need more info on ensuring data integrity. What does "external" mean? Does this require special checks of RTU inbound data? Unclear what will be considered validation. Is Encryption validation? If the RTU data is not encrypted is the EMS validation of data sufficient? If the systems (especially legacy equipment) do not support integrity checks the addition or development may not be possible or recommended. Will this require a TFE?
35.41	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R15.1 - Puget Sound Energy feels that "Limit propagation..." is an abstract term and needs clarity to it in order for NERC to be able to consistently validate compliance.R15.3 - Puget Sound Energy suggests clarity to what type of testing is required of malicious code protections. Is NERC requiring functional testing that the malicious code protections are reliably functioning or security testing (penetration testing)?R17.1 - Puget Sound Energy would like clarity into the degree of documentation required to validate compliance with "...required for normal and emergency operations are enabled." Puget Sound Energy would also like clarity into NERC's definition of "enabled" and "disabled". For example, can network accessible ports be "enabled" and "disabled" through the use of host based firewalls?R17.2 - Puget Sound Energy suggests that the disabling of physical ports on BES Cyber System Components only be required where physical security protections are not required, as outlined in Table 5. If physical security is provided, per Table 5, then the disabling of physical ports seems unnecessarily redundant. Puget Sound Energy would like clarity on "externally accessible physical ports", in cases where the BES Cyber System Component is physically protected by measures outlined in Table 5.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate

#	Organization	Yes or No	Question 35 Comment
			dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing “continuous security monitoring that issues alerts”.R19.1 - Puget Sound Energy requests clarity into what NERC means by “validate data inbound”. “Validate” is subjective and Puget Sound Energy would like clarity on how entities can prove compliance. Puget Sound Energy would also like clarity into the scope of the inbound data it must validate. For example, is NERC asking for validation of interconnections with other utilities and balancing authorities or validation of every RTU that provides an inbound data stream to a control center’s BES Cyber System?
35.42	BCTC	Disagree	R15 - Â Change title to “Prevent Malicious Code”Â 15.1 - suggest replacing the words “Limit propagation” to “Prevention”Â 15.3 - we do not agree with this requirement. Recommend removal of the words “to test”. It is not a good practice to introduce malicious code into a BES Cyber System - even in QA!Â Another potential area for TFEsR16 - Â R 16.2: if the patch results in a system upgrade it could take up to 6 months to implement the patches; if the patch does not result is a system upgrade then recommend allowing 30 days to implement said patchesR17 - Â The requirements needs to provide more guidance on how to provide evidence for open/ closed TCP (static) versus UDP (dynamic) ports Â R 17.1 Guideline would be appreciated on how to meet this requirement. We have struggled with this one in the past.Â Provide a definition of what is “system hardening” R 17.2 - what is the objective of this requirement? We feel that simply disabling a physical report does not provide much value from a security perspective (i.e. can unplug an active port and plug in an unapproved device); instead we recommend locking down devices’ MAC addresses as this would result in a more secure environmentR18 - Â R18.3. A year seems excessive to require an entity to retain ALL logs. What is the objective in requiring utilities to do this?R18.4. Suggest breaking this one in to two requirements - one for log review and the other for maintaining records - current wording can be interpreted as having to retain events for medium impact systems for a longer period than high impact? R19 - Â R19.1. We request a definition of what is meant by “validation” as well as guidance on how to perform this taskÂ Potential area for TFEsÂ

#	Organization	Yes or No	Question 35 Comment
			R19.2. We are struggling with how to comply with this requirement. We have an IDS implemented in our environment where users are alerted on suspect packets - is this what this is referring to? Intent not clear with the current wording.
35.43	WECC	Disagree	R15 - alright with all criteria, R16 - alright with all criteria, R17 - Item 17.1 should cover local ports and services not just network ports and services. Consider removing the words "network accessible" like text in previous standards and make required for Medium and High impact levels. Physical ports should be rendered unavailable on components of Medium impact systems as well as High. Item 18.2 needs to define "continuous" or remove it from the criteria. R17 - Consider adding more criteria for system hardening including system base-lining or move system base-lining from the change management section to here. Look for other overlap between R17 and change management. R19 - agree with criteria but would suggest adding the following after validate data "(eg. syntax checking, bounds checking, sanity checking, etc)"There needs to be more language specifying a definition of malicious code, what it means to limit its propagation, and to detect and respond to its introduction. As written, there is very little to audit against in this requirement.Additional language is needed to describe what it means for a patch to be released.System hardening should be required for all systems, not just those that are externally connected.Additional language is needed to clarify the requirements for security event monitoring, for example, what continuous monitoring means.Log review intervals are too long to be effective.The data integrity criteria are good additions but need additional language to clarify the intent. What does it mean to validate inbound data? Also, consideration should be given to the fact that cryptographic protection is not fully effective in all circumstances. More direction is needed as to when cryptography is an acceptable control. Also there are no requirements in the standard that define criteria for cryptographic controls.
35.44	Alberta Electric System Operator	Disagree	R15 - Change requirement to include confidentiality, to address potential MITM or MITB attacks. "...malicious software that could affect availability, integrity, or confidentiality of the..."Table R16 - include additional row similar to 16.1, but to

#	Organization	Yes or No	Question 35 Comment
			assess security patches within 60 days. Make this a requirement for Low Impact BES Cyber Systems. All BES Cyber Systems should be assessed, however High and Medium Impact systems should be assessed sooner.Table R19 - 19.1 states "Validate data inbound to a BES Cyber System in a Control Center." And the corresponding impact states "Required for external connectivity only." Based on the definitions, "inbound to a BES Cyber System" can only be from a device "external to the BES Cyber System" so the impact is redundant. Similar situation for 19.2. Suggest changing "Required for external connectivity only" to "Required". Table R19 - consider adding additional rows to Table R19 to address validating inbound data to BES Cyber Systems that are not in a control centre. 19.1 Validate data inbound to a BES Cyber System in a Control Center. Required for Medium and High 19.2 Validate data inbound to a BES Cyber System. Required for High19.3 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously. Required for Medium and High19.4 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System to determine whether the data has been compromised maliciously. Required for High.
35.45	LCEC	Disagree	R15 - Testing for malicious code protection is not auditable.R16 - Device end of life support issues need to be addressed. Release needs to be clarified to address the situation where a vendor may release a security patch for a BES Cyber System Component but it is not yet approved by the BES Cyber System vendor.R17 - o It is not often clear whether the standard is referring to logical and physical ports. Physical, logical or both should be specified any time the term port is used.R18 - What constitutes a security event?Is the 90 day requirement meant to be an absolute 90 days as opposed to 3 years and 90 days to be able to show compliance?R19 - How would one validate inbound data? Was this clearly meant to be data integrity as opposed to data protection? Why was this scope chosen?
35.46	Dominion Resources	Disagree	R15 - The stated intentions of the SDT at the May Workshop were to reduce TFEs and to distinguish between Control Centers vs. Substations and Power Stations. Neither

#	Organization	Yes or No	Question 35 Comment
	Services, Inc.		of these stated goals is presented in R15. TFEs will be required for 15.2 and 15.3 and there is nothing indicating that these should not apply to field equipment or network equipment (e.g., firewalls, routers, switches). Dominion agrees with the stated intentions of the SDT team.To avoid the potential for TFE's associated with R15.2 and R15.3, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.R16.2. The word "fixed" should be replaced with "planned" to allow some flexibility for installing the patch. 17.2. It should be clarified that an alternative where the equipment does not provide a configurable method of disabling the port is that methods, such as using security tape, to indicate any tampering with the port may be used.18.2. This section will require a TFE since many devices do not have the capability of issuing alerts. A footnote to avoid need for a TFE should be added.18.3. One year is too long to maintain logs for network devices. Storage space is at a premium. There will be a substantial increase in cost to increase storage space for each high impact cyber system This should be changed back to 90 days for High Impact cyber systems. 18.4. Logs of system events should only be required to be reviewed every 90 days. Logs should be reviewed only when an alert is issued for a detected system event. Routine reviews would take an extraordinary amount of time with no expected substantial results. R19. Common methods for ensuring data integrity include physical protection of the asset, authentication and authorization of data sources/inputs, using data validation and error checking rules at the application or database level, and a variety of other technical, operational and management controls. Dominion recommends the wording used in R19.1 be modified as follows to state the objective without specifying how it should be accomplished since the methods vary depending on the nature of the system and the technology in use:"19.1 Implement methods to maintain the integrity of data inputs to a BES Cyber System in a Control Center. " 19.2. It is sometimes impossible to determine if data has been compromised. Dominion understands that the proposed re-wording for 19.1 will also suffice to meet the requirements for 19.2 and recommends that 19.2 be removed.

#	Organization	Yes or No	Question 35 Comment
35.47	FirstEnergy Corporation	Disagree	R15 - We prefer the new text over the old CIP standards and it would reduce TFEs. In R15/Table 15: need some type of exception for devices incapable of running anti-malware.R16 - We prefer the new text over the old CIP standards. R17 - We prefer the new text over the old CIP standards.R17/Table 17: Need clarity on "externally accessible and physical ports". Does that mean serial, parallel, USB, Fireware, etc. or ports that are capable of transmitting routable protocols (e.g. network interface cards).R18 - 18.4 - Need greater clarity around whether automated alarming can be used rather than manual review of system event logs. Also - should it be specified somewhere in R18 that these sub-requirements apply to electronic security only, not physical security events (which is spelled out in R6)? 18.2 - We question the use of the word 'continuous' in this sub-requirement as this would be difficult for those entities that use 'organizational processes' to monitor and log.R19 - Overall this requirement appears to be too broadly worded. 19.1 - The use of the word 'validate' seems vague. Is the intent of the SDT that entities provide the specifics on what 'validate' means - e.g. the appropriate data or a point-for-point comparison, how often, etc? 19.2 - Many existing systems do not provide a means to accomplish compliance with this sub-requirement - for example, legacy RTU protocols. R19/Table 19: Need clarity on "invalid data". How do you evaluate invalid data?
35.48	US Army Corps of Engineers, Omaha Distirc	Disagree	R15 needs to be limited to general processing equipment. Requirement for anti-virus type software on all systems will numerous TFE's. R18 logging of all BES Cyber System components will generate numerous TFE's. R19 concerned about what realistic measures are available to meet requirements.
35.49	US Bureau of Reclamation	Disagree	R15.3 - If it is truly intended that entities test malicious code protections (not just ensure signatures are up to date and that protection software is running, the Standard should provide some additional guidance. Few entities are going to be willing to introduce malicious code, even into a test system, to verify malicuious code protection. Further, there is not timeline for when the malicious code protection must be tested. It would not be unreasonable to require and annual test of the

#	Organization	Yes or No	Question 35 Comment
			malicous code protections. The malicious code protections should be an intelligent requirement. Some devices that are not addressable may not need malicious code protection. R16.2 - Suggest the phrase "if the patch will not be installed" be added to the end of the requirement. R17.2 - Is locking within an enclosure satifactory? R18.3 - Suggest medium impact requirement be "for at least 90 calendar days" and that high impact timeframe be considered for reduction, perhaps to at least 180 calendar days.R19.1 - Explain how this is to be accomplished within the Standard - based on some specific criteria. This requirement is too open-ended. Since the concept of BES Cyber Systems now includes such devices as programmable multifunction or solid state relays, the requirement to "validate data" inbound makes no sense. Many of these devices reside within a control center. The definition now includes those center which are used to control more than one BES generator. The data going into the relays is from transducers either inside or outside the physical security perimeter but within another physical security perimeter. This data may be digital or analog. How would it be validated, cryptographically progracted or analyzed for malicious compromise?It is not clear how an "interactive user" session would apply to "programmable" relays.
35.50	Ameren	Disagree	R16.1 - This requirement should address documenting the installation date of patches and that patches have been installed.R18 - should only apply to network based systems with external connections only; currently this required is not limited on what it applies to.R19.1 and R19.2 - There is no way to comply with this standard without requiring the vendors to write better code. Suggest removing these requirements.
35.51	Northeast Utilities	Disagree	R17 appears to be significantly weaker than the previous standards. It also does not appear to align with the draft change control standards. Ports and services are a strong control to ensure only services required for operation are allowed. At minimum the High Impact BES Cyber systems should be “Required”.R19 needs more explanation. What does validate data mean?

#	Organization	Yes or No	Question 35 Comment
35.52	Hydro One	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing 17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Requirement 18.4 seems to have one purpose and that is to prove 18.2. To us this seems redundant since R18.2 require alert for system events. Why do we need a review at some later point? We recommend removing the requirements R18.4 Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Please clarify the applicability of R19. Does this requirement apply only to code releases into the system or it applies only to external data streams (e.g. weather data from a service provider, data from RTUs etc)?
35.53	ISO New England Inc	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious codeBelieve the SDT meant that 15.3 testing insures that the deployment will not adversely impact security. However the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			16.1 from “release” to “availability”Recommend removing “with a fixed date” from 16.2 because the cyber system may not be available for maintenance due to grid system conditions, implement based on your documented patch process. Request a R17 local definition of “attack surface”Recommend changing 17.2 from <<Disable, or render unusable, externally accessible physical ports>> to <<Disable or secure externally accessible physical communications ports>>Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber SystemsR18.3 Some automated tools do not have separate log retention based on the asset. The log retention applies to all assets. It is unclear if the log retention is the actual log from each Cyber System component or the log that an automated tool keeps (ie parsed out info from syslog). Either way a years worth of logs will require terrabytes upon terrabytes of storage for useless information. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommend that R19 should “insure the integrity of the data.”Recommend that 19.1 should be “Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should be “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.54	Northeast Power Coordinating Council	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Recommend that 18.4 be re-worded to be consistent with FERC Order 706 paragraph 526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.55	USACE HQ	Disagree	Requirement 15.1 should be deleted from the list. Limiting the propagation of malicious code is a logical step in the “respond to the introduction of malicious code” phase, process which is required in 15.2. Therefore 15.1 present a possible double jeopardy since it is logical to think that when responding to the introduction of malicious code in the environment the steps will include limiting the propagation of the same before removing it from the system. Also, requirement 15.1 language is to broad in the interpretation of it. “Limit propagation of malicious code” implies that the code has moved through some part of the system, therefore the question is, how much movement of the code is acceptable when creating a response process?. The acceptable answer to this question could depend on the auditor’s subjective views of what is acceptable safe propagation of the code inside the system.
35.56	Garland Power and Light	Disagree	Requirement 16.1 - Reword requirement to say assess within 60 days - reason is because we feel it is adequate to check the vendor web site every 30 days and allow 30 days for testing and determination of implementationRequirement 18 - Reword

#	Organization	Yes or No	Question 35 Comment
			requirement to allow for Responsible Entity to develop a definition of a "system security event". The words are used in the main requirement and each subrequirement. Requirement 19 - o Delete Requirement R19 - Control systems currently validates data for quality and limits and then tags the data with any issues so that downstream applications can handle appropriately. This is sufficient for the security and reliability of the BES. R19 is impractical for implementation in the field for large or small utilities. This will reduce reliability of the overall system.
35.57	Oncor Electric Delivery LLC	Disagree	Requirements 15.1 and 15.3 are not necessary. The use of antivirus and malware software is problematic on some systems, while “whitelisting” requires additional hardware which may contain its own vulnerabilities. Detection and response should be sufficient. Many programmable devices are not capable of propagating malicious code or running prevention software.Requirement 18.2 does not apply to many legacy cyber systems and should only be applicable to systems which utilize routable communications.
35.58	Manitoba Hydro	Disagree	Revise the wording of Requirement R15 to “... integrity of the BES Cyber Systems.” Please clarify the intent of “test and update malicious code protections”. Requirement R16.2 should be revised to indicate the development AND implementation of the schedule. The wording of Requirement 16.2 currently does not require the application of mitigating measures prior to the installation of the applicable patch, and may need to be revised. For Requirement R17, please what is the meaning of “network accessible ports”, and “externally accessible physical ports”. Are physical ports enclosed within an unlocked cabinet “externally accessible ports”? Are physical ports within a non-public space, “externally accessible ports”? Requirement R18 does not contain any requirement for response to security event alerts or monitoring. Remove the word “maliciously from Requirement R19.2. It may be very difficult to determine if the data compromise was malicious or not. There are no specifics given with respect to “limit” propagation in Requirement R15.1. It is assumed to be at the Responsible Entity’s discretion in terms of criteria, means, etc. There are no specifics given with respect to “validate” data in Requirement R19.1 so it is assumed to be at the

#	Organization	Yes or No	Question 35 Comment
			Responsible Entity's discretion in terms of criteria, means, etc.
35.59	San Diego Gas and Electric Co.	Disagree	SDG&E thinks that R17.2 sounds good in theory (disabling external physical ports on assets), but in practice this can be difficult to achieve without damaging the port for future legitimate use. Many shops use epoxy or other glue-based products to physically disable / protect such ports, and these solutions tend to be permanent. If we are physically protecting the asset from access anyway with card readers and other physical means, why is it necessary to take this redundant step of sealing physical ports on assets when only people with authorized physical access (who have had training) can actually access the asset?SDG&E has concerns about the viability of complying with R19.1 (validating inbound data to a BES Cyber System in a control center) in a situation where the incoming data is encrypted. How does the SDT define "validate"? Where does the validation need to occur?SDG&E also has concerns about the viability of complying with R19.2 (evaluate invalid data for malicious compromise) without MUCH additional vendor support. How does the SDT define "evaluate invalid data"?
35.60	Platte River Power Authority	Disagree	Suggested Revision (clarify what to test):15.3 Implement processes to update malicious code protections including testing security controls
35.61	Duke Energy	Disagree	Table 15: will need a TFEWithin generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.Requirement 16.1: Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems. Release from whom? It makes a big difference if the patch is released from Microsoft, for example, or the patch is released from the control system vendor (e.g. Emerson, Invensys, Areva, etc.) as to how/if the patch is implemented to prevent risk to the BES cyber system.Table 17: for devices inside a locked cabinet, are the physical ports on that device externally accessible?Requirement 17.2: how does the definition of "externally" in "externally accessible physical ports" compare with the definition of external in "external connectivity" in R3? Also, this definition implies that there are physical ports that are

#	Organization	Yes or No	Question 35 Comment
			NOT “externally accessible”. Need to make definition more clear. Suggest taking out reference to “externally accessible”.Table 18: 18.1 - not all devices are capable of logging, need a TFE18.2 - it would be helpful to have a definition of ‘events related to cyber security’18.4 - remove for systems where automated tools are in place. Requirement 18.2: " one or more security processes for continuous security monitoring" - is there any interpretation of the expectation here so that we don't have disagreement at audit? Are alternate controls allowed for BES Cyber Components that don't support logging/monitoring (example: manual review of physical access logs for stand-alone equipment)?Table19:Item 19.1 & 19.2 Additional explanation is needed to explain acceptable threshold for “validation of inbound data.”Clarify validate in 19.1. Is encryption a form of validation?What is meant by Data in 19.1?Requirement 19.1: What types of data validation controls are acceptable to meet this requirement? For example, control totals, presence check etc. Requirement 19.2: Need to provide an example with what methods can invalid data be evaluated to conclude that the data has been compromised maliciously?
35.62	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table

#	Organization	Yes or No	Question 35 Comment
			R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement

#	Organization	Yes or No	Question 35 Comment
			will achieve that end.
35.63	American Electric Power	Disagree	Table R15: 15.1, regarding "Limit propagation of malicious code", suggest replacing "propagation of" with "propagation and introduction of".15.2, regarding "Detect and respond to the introduction of malicious code." Would this be covered in a traditional cyber security incident response program? This should already be covered in R27.Table R16:16.1: Regarding the word "release" within "Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems." Release from who? For example, is it the release of a new patch by Microsoft, or is it the certification of the patch by the control system vendor that the patch does not negatively impact the control system? Further clarification is needed. Patches released by Microsoft are not typically tested for several days or weeks by Control System vendors to validate that the patch does not impact functionality. Industry cannot test software patches as thoroughly as the Control System vendors.16.2: Is it a violation if you do not meet the fixed date? Suggested wording: replace "fixed date" with "scheduled date". Add a provision to supply reasoning for not meeting scheduled dates. The rewording provides flexibility to the Responsible Entity to push installation of the patch to a later date without being in violation.17.2: Add a sentence similar to the last sentence in 17.1, "In the case where unused, externally accessible physical ports cannot be disabled, the Responsible Entity shall document and implement a mitigation plan." The disabling of physical ports is not supported by all network devices. To meet the literal wording an entity may need to physically damage equipment which would void warranties and prevent further vendor support.18.1: Regarding "organizational processes" and "system events that are related to cyber security". Is it reasonable to think this can be done without automated tools?18.2: Regarding "continuous security monitoring", is this redundant to 18.1? If you are implementing automated tools to monitor and log system events are you not providing continuous security monitoring? Suggest removing these words to eliminate double jeopardy.This requirement should be focused on issuing an alert.Regarding "system events related to cyber security", what constitutes a system event related to cyber security? What criteria should be used? Is there an accepted

#	Organization	Yes or No	Question 35 Comment
			standard that an entity will be held to in an audit? If the right system events are not classified in an auditors' eyes, is this a violation? Suggest rewording to reference an acceptable set of minimal system events to monitor. What if a BES Cyber System does not generate a sufficient amount of detail to determine if a cyber security event occurred? Suggest allowing a TFE in this instance.18.3: Regarding "Maintain logs of system events related to cyber security within the specified time period", what if a BES Cyber System cannot store events for the duration required? Is a responsible entity required to go out to a device repeatedly to export their logs if they cannot meet the 90 day or 1 year increment? Suggest rewording to take into account limitations of BES Cyber Systems. Possibly use as a TFE item, if TFE's are maintained.What benefit does this provide for reliability or security? 18.4 is the important element, not the data retention.R19: With real-time or near real-time control systems, these requirements could increase latency and pose a negative impact to reliability.19.1: Regarding "Validate data inbound to a BES Cyber System in a Control Center", validate against what? Is the source being validated? Is the data itself being validated? Is providing encryption on the data sufficient? Who determines the appropriate level of validation? Is it being left to an auditor?Reliability could be compromised if this induces extra latency on the systems sending and receiving real-time data. This should be included as a TFE; older systems may not be able to handle the latency.19.2: Would "bad quality" indicators in the EMS system be an example of this?
35.64	APPA Task Force	Disagree	The APPA Task Force believes that Requirement R15 as currently drafted will require numerous TFE's. Each entity will need to document that they are not following this requirement since a vast array of devices in substations and generation stations are BES Cyber System Components but are not capable of propagating malicious code. Therefore we recommend the following edits for R15:R15. Objective:To protect BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.R15. Requirement:Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in CIP-011-1 Table R15 - Malicious Code Protection. This requirement applies only to BES Cyber

#	Organization	Yes or No	Question 35 Comment
			System Components that have the capability to propagate malicious code. Change the Table legend to "Malicous Code Protections".The APPA Task Force is concerned that the criteria in R15 Table 15.3 do not constitute a reasonable requirement when looking at the transmission and generation environments that will be required to comply. The drafting team may not fully appreciate the full magnitude and implications of the phrase "test and update". We recommend that the criteria in Table 15.3 be removed or only be required for control centers.R16 Objective:To ensure that security vulnerabilities in BES Cyber Systems are mitigated. R16. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management R17. Objective:To reduce the available attack surface of the BES Cyber System.R17. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - System Hardening The APPA Task Force agrees with the MRO-NSRS proposal noting that as written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings. This would require an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We recommend that this item be deleted.R18. Objective:To ensure that security events are known, logged, and responded to on BES Cyber Systems.R18. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring R19. Objective:To protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.R19. Requirement:Each Responsible Entity shall implement processes incorporating the criteria specified in CIP-011-1 Table R19 - Communications and Data Integrity The APPA Task Force is extremely concerned with the actual ability of the industry to comply with the criteria in R19 as proposed. A discussion is necessary to understand if this requirement is actually feasible for all entities with High Impact facilities.

#	Organization	Yes or No	Question 35 Comment
			Utilities hire capable operators to make decisions on incomplete data all the time. If validating the data inbound means another electronic verification, this is impractical. If validating the data inbound means calling a lineworker in the field to check a setting in a substation when an operator is not comfortable with the data he is receiving, this is reasonable, but still not an auditable requirement. We agree with the MRO-NSRS evaluation of 19.2, which notes that as written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously. We recommend that this requirement be removed and placed in the guidance in support of the standard as a future technology.
35.65	Bonneville Power Administration	Disagree	The objectives of these requirements ("to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions," "to ensure that security vulnerabilities in BES Cyber Systems are mitigated," "to reduce the available attack surface of the BES Cyber System, "to ensure that security events are known, logged, and responded to on BES Cyber Systems," and "to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The phrase "Reliability Functions" at the end of R15 is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Does the drafting team mean CIP-01-01 - Attachment 1, Functions Essential to Reliable Operation of the Bulk Electric System? If so, that should clearly be stated. If not, there should be a definition in the Glossary. Table 16, Section 16.2. We applaud the new standard, which makes it clear that immediate mitigation or installation of patches is not required. However, there are still some issues:1. Security patches arrive weekly to daily to multiple times a day. Many may be applicable to systems, but of minimal

#	Organization	Yes or No	Question 35 Comment
			threat. Entities should be able to not only evaluation the applicability, but the threat and risk of the threat to their systems within their environment, and choose to escalate or deescalate patches as appropriate to them. Low impact, or low risk patches may be assigned to a regular patch or maintenance cycle, while high risk patches may be tested and implemented immediately. This should be up to the system owners, and not prescribed in the requirement.2. Mitigation plans are not necessarily applicable. Some patches, while technically applicable to specific equipment or operating systems, may have such a low risk or impact that they entity may choose not to apply the patch.3. There are instances where a patch may be applicable from a security perspective, but the risk it presents from a reliability perspective may outweigh it. 4. Where systems are isolated from external affects, even a patch that applies to a specific device may not be necessary.5. Meaning of "fixed date" is not clear. Does it mean "the same for every patch", or "the date can't be changed"? Both are bad choices. Different patches might require different schedules, depending on their impact and the availability of outage time on the system.R17: Rename this back to "Ports and Services" to avoid confusion. In the electrical industry "Hardened" systems are those that meet specific electrical requirements and interference requirements.Also, the use of the word surface implies something physical rather than electronic.Recommendation for R17: "Objective 17 - To reduce the available electronic attack points of the BES Cyber System.R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - Ports and Services"Table 17, Section 17.1. A mitigation plan might not be appropriate. In the context of NERC standards, a mitigation plan describes the actions that will be taken to achieve compliance. That is not the situation here. Recommendation: "cannot be disabled, the Responsible Entity shall document the reasons for the inability and compensating measures used."Section 17.2. We understand that FERC wishes the standard to address physical ports. However, this could have negative conquences:1. There are hundreds of thousands of devices in service that have physical ports that may not be used. The fact that they are not needed or used normally means that there is nothing connected

#	Organization	Yes or No	Question 35 Comment
			to them. If there is nothing connected to them, they are not vulnerable to any kind of external or remote attack.2 - Disabling physical ports on electrical system components may be: o Impossible o Degrade the operation of the equipment o Render the warranties on the equipment void thereby removing vendor service o Create such a huge national work load that it could never be accomplished.Recommended change - Eliminate 17.2Table R18:18.1 & 18.2 - The use of the term "all BES Cyber System Components" is not accomplishable:1. Many, if not most "components" in the field do not capture what would be considered cyber security related events. They only capture electrical system events. They don't even have the capability to capture access events.It is the access points to these devices that may have the ability to capture even the most rudimentary cyber security information (Access Attempt, Date, Time, Account, Source, Target)2. It may not be possible to place monitoring equipment within electronic monitoring proximity of these components. 3. The term "events that are cyber security related" is not defined. What exactly does it mean? Is this access events, Intrusion Detection systems, Antivirus, ??? Much of this cannot be implemented on or even for "all BES Cyber Components". Recommendation: 1. Remove "components", so that the requirement is at the BES Cyber System level.2. Change "...security for all..." to "...security, as defined by the Responsible Entity, for all..."18.3 has the same issue with the definition of "events related to cyber security". In addition, this time frame has caused some confusion from an audit perspective. - Some have read that to mean that there must be, on the originating system, at all times, at least 90 days worth of logs. While others (rightfully, we feel) are maintaining archives of their logs in alternate locations for 90 days or longer. Recommendation: replace with "Maintain captured log information within the specified time period on-line, in archives, or in some other readily accessible form."Section 18.4. Consistently accomplishing manual review of logs could be difficult for large entities with large numbers of devices, especially within the 7 days required for high impact systems. The obvious solution is the use of an automated log review tool. This should be explicitly addressed in the standard. Recommendation: "Review, either manually or by automated means, logs...." Entries in Table R19 are acceptable only if the

#	Organization	Yes or No	Question 35 Comment
			definition of external connectivity is changed, as discussed above. Otherwise, entities would be forced to validate data inbound from one BES Cyber System to another BES Cyber System, all within the same Control Center. This does not seem to be the intent: using the existing definition of external connectivity, any data inbound to a BES Cyber System uses external connectivity. In that case, why state it so? Clearly, the intent was to validate traffic inbound from outside the Control Center, at most.
35.66	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The requirements are to prescriptive for the range of systems that it will apply to.
35.67	Constellation Power Source Generation	Disagree	The term “release” in R16.1 needs to be further defined. The issue with it being vague is that some patches for a system may be released for all users, but if that system is tied to a distributed control system, the distributed control system vendor has to validate the patch before its implemented by a facility. Using this example, there are really 2 release dates. For auditing purposes, a suggestion would be to define release locally as “the date of which a security patch has been safely validated by a vendor. If another vendor must validate this release before implementation, than the date it has been released by the second vendor will be used as the release date.” R16.2 is not worded correctly. A suggested change would be “Development of an implementation schedule with a fixed date for installation of the applicable security patches and a fixed date for completion of mitigating measures that address the vulnerability, until implementation of the patch.” In R18.1, is the monitoring and logging continuous, or on a fixed schedule? The SDT should add clarity to this requirement. R18.2 discusses issuing alerts but does not give a timeframe for issuing them. A suggestion would be 90 days to ensure a proper review of an incident to determine if it was a cyber event. At the CIP V4 Workshop, the drafting team stated that R18.4 was not meant to be an exhaustive manual review of logs, but rather a check to ensure the automated log is functioning. This needs to be included in the verbiage of the requirement. R19.1 should be reworded to say “Implement a process to validate data received by a

#	Organization	Yes or No	Question 35 Comment
			Control Center's BES Cyber System." Doing so would clarify R19 as a whole, and R19.2 can be removed due to its redundancy with R19.1.
35.68	Public Service Enterprise Group companies	Disagree	There are several clarifications necessary to make the language understandable and ensure that entities know what is required. [1] Please clarify the distinction between requirements 15.1 and 15.2. Performance degradations and potentials for false positives from detection mechanisms that inspect each file when accessed, as possibly implied by 15.2, may not appropriate for real-time systems. [2] In requirement 18.2 please specify what is meant by "continuous"? Is a periodic check sufficient? [3] Please clarify the distinction between requirements 19.1 and 19.2. In requirement 19.1 please specify what is meant by "Validate"?
35.69	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.Please define the stipulation 'Required for external connectivity only'.Are the tools and processes listed in R18 intended to provide automated detection, or manual\narrative logging of events detected under the heading of other controls? If automatic, what sorts of events are contemplated? What is intended by the term 'Validate' in 19.1? Does this mean the identification of a separate, independent source for the data, business rules, or something else? Without understanding the intent of the standards drafting team, I cannot suggest specific changes.
35.70	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of

#	Organization	Yes or No	Question 35 Comment
			the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.71	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.72	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is

#	Organization	Yes or No	Question 35 Comment
			meant by “Implement processes to test and update malicious code protections.” Suggest “Implement processes to detect malicious software, and review annually”.It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.73	Reliability & Compliance Group	Disagree	To help eliminate TFE’s here, you need to add a qualifier such as “to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions if mechanisms exist that can protect the BES Cyber System Component.”
35.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
35.75	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. With respect to requirement 15.1, We Energies believes this may not be possible for non-windows based devices/systems.We Energies agrees with EEI: Requirement 15.3 is unclear as to what is meant by “Implement processes to test and update malicious code protections.” Suggest “Implement processes to detect malicious software, and review annually”.It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be

#	Organization	Yes or No	Question 35 Comment
			protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. We Energies agrees with EEI: Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.76	GTC & GSOC	Disagree	We Recommend: 1. In R15.3: taking out the words "test and" or, alternatively, clarifying what is meant by "test"2. In R19.1: clarifying whether encryption is required or if CRC will be sufficient3. Completely removing R19.2 because of the following reasons referenced from the DHS Catalog of Control System Security: a. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety. b. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
35.77	Midwest ISO	Disagree	What does it mean to validate data in R19.1. What is the expectation if a piece of data has been changed/modified when the value received is within reasonable limits but is not the actual value sent? This could be particularly troubling for the Interregional Security Network and ICCP. For example, how can an RC validate that the SCADA system sent valid data to the ICCP server at a TOP if it is within an expected range? More details around the expectation of validating data would be helpful to ensure entities can be compliant.

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 Requirements R15 through R19 have moved to CIP-007-5 Requirements R1 through R4.

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions for improving these requirements, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. For example, some suggested that certain requirements should apply only to Medium Impact BES Cyber Systems with external connectivity. Others suggested that there were key requirements such as malware prevention that should apply at all BES Cyber System impact levels. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. The intent of this approach is to refine, as commenters suggested, the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in CIP-003-5 through CIP-011-1.

#	Organization	Yes or No	Question 36 Comment
36.1	Northeast Utilities	Agree	Need TFE language added; not all CCAs or protecting assets require malicious code protection.
36.2	FirstEnergy Corporation	Agree	R17 - Does ‘external connectivity only’ mean only firewalls? If not, please provide intent of SDT.
36.3	BGE	Disagree	15.1, 15.2 and 15.3 should also apply to Low impacted systems. 16.2 implies that the patching can only occur on the same day every month.19.1 Define “validate”.
36.4	ERCOT ISO	Disagree	15.1-15.3: Should apply to Low Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
36.5	American Electric Power	Disagree	17.1: Regarding "Required for external connectivity only" within the High and Medium

#	Organization	Yes or No	Question 36 Comment
			impact categories. Is this required for "routable external connectivity" only, or all connectivity?How will items in R18 and R19 be performed on systems with nonroutable connectivity? Will dedicated IT Security Operation staff need to be added to isolated networks to perform the security status monitoring?
36.6	US Bureau of Reclamation	Disagree	Add R15.1, R15.2 and either R18.1 or R18.2 to the requirements for a low impact system. Concept of REMOTE connectivity is not defined. Without that definition, it is hard to assess if a High Impact is appropriate or if no Medium Impact is reasonable..
36.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
36.8	Black Hills Corporation	Disagree	At least 15.2 and 16.1 should also apply to low impact BES Cyber Systems.
36.9	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
36.10	The Empire District Electric Company	Disagree	Comments: For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: “Required for routable external connectivity only”. We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.11	US Army Corps of Engineers, Omaha Distirc	Disagree	define terms "continuious security monitoring" and "detected system events."
36.12	CWLP Electric Transmission, Distribution and	Disagree	Due to the requirement for continuous monitoring and alerts defined in R18.2 the requirement for log reviews every 7 days should not be needed. A standard 30 day review as in the medium impact area should be appropriate for both high and

#	Organization	Yes or No	Question 36 Comment
	Operations Department		medium impact levels.Does the fact that the data has been successfully passed through a Firewall or Access List meet the obligation to validate data incoming to a Control Center in R19 or does this require the data be inspected all the way down to the packet level?
36.13	American Transmission Company	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
36.14	MRO's NERC Standards Review Subcommittee	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.15	Southern California Edison Company	Disagree	In order to appreciate the impact based categorization and reflect the actual impact on BES reliability, an additional requirement can be added to R16 for medium and low impact system. The drafting team should look at NERC PRC standards on maintenance schedules and synchronize CIP patching and upgrades to a maintenance and inspection schedule that is already mandated by NERC.Requirement R18 requiring logs be reviewed manually every seven days, when controls to automatically monitor such logs are already in place, is a control that does not seem to add additional security value. If the intent of the drafting team is to manually ensure and certify that the logging capability is functioning adequately, the drafting should include such verbiage. The current draft language of the standard seeks only a manual review of

#	Organization	Yes or No	Question 36 Comment
			the log rather than the manual verification of the logging capability.
36.16	Progress Energy - Nuclear Generation	Disagree	Incorporate information contained in the matrix in Attachment 1 for durations to ensure consistency by aligning CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
36.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
36.18	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring

#	Organization	Yes or No	Question 36 Comment
			that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement R17 should be applied to both high and medium BES Cyber Systems.
36.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of

#	Organization	Yes or No	Question 36 Comment
			obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is presented to it.
36.21	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only'.
36.22	American Municipal Power	Disagree	Please provide a little or no impact category
36.23	The United Illuminating Co	Disagree	R15.2, introduction of malicious code, responding to the introduction of malicious code is a specific cyber security incident. Suggest 15.2 be limited to processes to detect malicious code. Response is already part of cyber incident response.
36.24	Southwest Power Pool Regional Entity	Disagree	R15: Malicious code prevention is a basic security control and should be applicable to all impact categories. R17 and R19 should not make a distinction between external and non-external connectivity. R17: Once access is gained into the network by any means to any cyber system on the network, external access is immaterial.
36.25	Southern Company	Disagree	R19 comes from the DHS catalog, requirement 2.8.8. In the DHS catalog, there are 4 requirement enhancements, two of which are warnings which could greatly affect reliability. The DHS catalog presumes this requirement would be implemented on a case by case basis after appropriate research and testing. It therefore has no place in a mandatory standard that will force its use everywhere without regard to the reliability impacts. This requirement should be removed from a reliability standard.
36.26	National Grid	Disagree	Refer to answers in Q. 35.
36.27	Manitoba Hydro	Disagree	Requirement 18.4 can be very onerous for the industry for legacy systems which don't support automated log consolidation or review. The requirements must allow more flexibility.

#	Organization	Yes or No	Question 36 Comment
36.28	Garland Power and Light	Disagree	Requirement 19, 19.1 and 19.2 should not be required for any level
36.29	San Diego Gas and Electric Co.	Disagree	SDG&E feels that if R17.1 is a requirement for Medium Impact systems, then R17.2 should be as well for Medium Impact systems. For R18.3 and R18.4, SDG&E recommends that consistency be applied to the requirements to help ease the compliance burden of companies that have both High and Medium Impact BES Cyber systems. SDG&E also feels that instead of using the word "impact" for these Requirements, apply a concept of "risk" for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
36.30	Con Edison of New York	Disagree	Section 15 & 16 should be limited to networked systems. Isolated microprocessors not part of a network should not have the same requirement.
36.31	ISO New England Inc	Disagree	see answer to question 35
36.32	Progress Energy (non-Nuclear)	Disagree	See comment 14.
36.33	WECC	Disagree	See comments for Q35Criteria should aplpy to all impact levels
36.34	LCEC	Disagree	See previous comments
36.35	BCTC	Disagree	See response to Q35.
36.36	Hydro One	Disagree	see response to Question 35
36.37	Entergy	Disagree	See response to Question 35 immediately above.
36.38	Northeast Power Coordinating Council	Disagree	See response to Question 35.

#	Organization	Yes or No	Question 36 Comment
36.39	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 15.1, 15.2, 15.3, and 17.2. Suggest “Required for external connectivity only” for Medium Impact in rows 19.1 & 19.2.
36.40	Duke Energy	Disagree	Table 18: Manual reviews every 7 days is not practical.
36.41	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of

#	Organization	Yes or No	Question 36 Comment
			meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement will achieve that end.
36.42	Alberta Electric System Operator	Disagree	Table R15 - make 15.1, 15.2, 15.3 required for Low Impact BES Cyber Systems, but possibly on a longer time horizon than for Medium and High Impact BES Cyber Systems.Table R16 - make 16.2 required for Low Impact BES Cyber Systems.Table R17 - make 17.1 “Required for external connectivity only” for Low, and “Required” for Medium and High. Make 17.2 required for Medium also.Table R18 - make 18.1 and 18.2 required for Low Impact systems. Make 18.3 90 calendar days for Low Impact systems. Make 18.4 30 calendar days for Low Impact systems.

#	Organization	Yes or No	Question 36 Comment
36.43	Idaho Power Company	Disagree	The review of logs every 7 days or even 30 days is extreme unless the logs are filtered for only abnormal events and only logs of abnormal events are reviewed.
36.44	Ameren	Disagree	The system hardening in Table for R17 is rendundant when other standards already restrict physical access to these systems.â€,â€,â€,R18.1, R18.2, R18.3, and R18.4 - Log file monitoring at Medium Impact Systems will be costly as there may not be bandwidth available to send the logs to a central location to be reviewed. Suggest removing these requirements for Medium Impact Systems.
36.45	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.

#	Organization	Yes or No	Question 36 Comment
36.46	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.47	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System

#	Organization	Yes or No	Question 36 Comment
			Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."EEI recommends deleting R19. As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
36.49	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.We Energies agrees with EEI: The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI:

#	Organization	Yes or No	Question 36 Comment
			Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.We Energies agrees with EEI: Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.We Energies agrees with EEI: Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI: Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."We Energies agrees with EEI: Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it. We Energies agrees with EEI: As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.50	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R15 - R19:R15 Table 15.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.2: Low

#	Organization	Yes or No	Question 36 Comment
			Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.3: (If retained)Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for routable external connectivity onlyWe believe the “continuous security monitoring” as described in 18.2 is not practical for all BES Cyber System Components. We also believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally. Therefore we propose that for Medium impact facilities 18.1-18.4 be “Required for Control Centers only.”R18 Table 18.1: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.3: Low Impact: N/AMedium Impact: 90 calendar days for Control Centers OnlyHigh Impact: 1 yearR18 Table 18.4: Low Impact: N/AMedium Impact: 30 calendar days for Control Centers OnlyHigh Impact: 7 calendar daysR19 Table 19.1: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity onlyR19 Table 19.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity only

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1Requirements R20 through R22 have moved to CIP-005-5 Requirement R1.

Many commenters suggested phrases or aspects of the requirements that needed to be clarified. Several commenters questioned the need for weekly review of log entries, indicating that reviewing log entries at this interval would be burdensome with little or no positive impact on reliability.

Several commenters suggested reverting to the old name of Electronic Security Perimeter in place of Electronic Boundary Protection. In addition, several commenters suggested removing the system boundary protection requirement because it is overly prescriptive.

The drafting team agrees with commenters that some aspects of the requirement were too prescriptive, and has made significant changes to update the requirement both to clarify it and make it less prescriptive, while still addressing FERC Order 706 directives. The drafting team also agreed to revert to the Electronic Security Perimeter designation.

#	Organization	Yes or No	Question 37 Comment
37.1	WECC		Agree with concept, however, some work on the wording might make this more clear. R21 should have an additional item 21.3 - Cyber System components will not be shared with non-BES cyber systems or BES Cyber Systems of different impact levels.The former requirements for ESPs were better. The new language describing access points on communication paths may be an indirect way to get there, but it does not make things clearer or more auditable. This method of describing controls will make matters more complex and create additional work for entities.
37.2	GE Energy	Agree	"Logical Separation." Logical separation should be clarified. Logical separation could mean network access separation through an access point or it could be account separation by having separate user, system or service accounts that are different

#	Organization	Yes or No	Question 37 Comment
			amongst BES systems.
37.3	USACE - Omaha Anchor	Agree	Define 'unauthorized access attempts' is this a ping, or is this when a bad password is given to the system.
37.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R20.20.2 - How does one implement a deny access by default for a dialup modem? That effectively either takes the modem out of service, or if you were to rely on the PSTN to do any kind of 'validation' of the incoming call, this is at best security through obscurity as it is trivial to spoof the callerid which is the only form of data validation that can be done over a dialup line.20.4 - What does "unauthorized access" mean? Does that mean an access attempt? Would a port scan of a firewall qualify as "unauthorized access"?20.5 - What does "unauthorized access" mean? If something as simple as a connection attempt qualifies, this requirement puts a tremendous burden on staff to track every little event that might happen on the firewall, and would not accomplish much in the end. If the intent of the standard is to keep unauthorized login attempts at bay, it should say that.R21.21.2 - Communication through an "electronic access point" for dial-up communications could prove difficult for some devices. Some devices are extremely sensitive to any sort of jitter introduced to a data stream, and having a security device in front of these kinds of devices may introduce enough jitter to make the communications unusable. R22.This seems duplicative of R14, R16, R18 and R23. FMPA suggest modifying those requirements to incorporate the protective cyber systems elements.22.2 - This should be consistent with R16; medium should be required to patch access control points. Also, low should have to patch at least quarterly. For access points, consider forcing high impact to asses 'critical' patches within 7 days.
37.5	Green Country Energy	Agree	Footnotes, guidance document?
37.6	Exelon Corporation	Agree	If systems are connected to a master station/location that is a BES Cyber system, do all the connected systems become BES Cyber systems? At what level do these

#	Organization	Yes or No	Question 37 Comment
			requirements apply - for example at the relay level where someone is logging into the relay? Exelon would like clarification on the definition of the electronic access point - is it at the component level or at the system level?
37.7	Progress Energy - Nuclear Generation	Agree	R20-22 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
37.8	Independent Electricity System Operator	Disagree	- R20.1 R20.4 20.5 and 20.6 External and External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary? - - R20.5 Please define
37.9	National Grid	Disagree	1. National Grid requests clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points. The entity should be required to document only external communication paths with dial up access or routable protocol. Recommend removing R20.1 and 20.2 from LOW impact category.2. National Grid recommends removing “within the following time period” from 20.5 and 20.6. Also, for dial ups it would be difficult to review the alerts in the given time period. Suggest 30 days for logging related to dial-ups. 3. National Grid recommends that 20.6 be re-worded to be consistent with FERC Order P526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”4. National Grid recommends that 20.6 High Impact BES CS should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days. Also should it be included for Medium Impact BES CS?5. National Grid recommends removing 21.2 since it is covered in 20.26. National Grid recommends removing R22 since it is redundant and move it’s table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23

#	Organization	Yes or No	Question 37 Comment
37.10	Dairyland Power Cooperative	Disagree	20. What are the boundary rules for serial connectivity vs. routable protocols. Serial connections can be external to different systems and they can be internal. How do we determine if there is a boundary to protect?21. The logical separation rule needs more detail "Logical Separation" should have a definition. What is the impact for an RTU field device than can be scanned by multiple systems or entities? Is the mere configuration of available data on each physical or logical port enough to satisfy logical separation? What about components used as system-to-system gateways?
37.11	Regulatory Compliance	Disagree	20.1 - clarify - are these communication paths external to the electronic boundary?20.2 - clarify - This implies a firewall for even low impact?20.3 - guidance on what required elements to document20.6 - Clarify if this is for firewall logs only21.1 - Major clrification needed - what about BES Sytems that rely on input and out from system to system in having the logical separations?
37.12	Dominion Resources Services, Inc.	Disagree	20.1. The language "Document all communication paths" is too vague and suggests a need to map out the entire LAN/WAN infrastructure. Based on the May workshop discussion, the intent of the requirement is to document inputs and outputs associated with the BES Cyber System. Dominion recommends the following alternate wording for R20.1:"Document all digital interfaces associated with each BES Cyber System."20.4. Dominion recommends revising the language of this requirement to read:"Document and implement one or more processes for logging all access attempts at each electronic access point."Firewall logs cannot identify all "actual unauthorized access." Someone using a trusted source to gain access to a BES Cyber System would be permitted through a firewall. That is "actual unauthorized traffic" but it is not detectable. Blocked access attempts are shown in firewall logs as a dropped or denied entry.20.5. As explained in the comment for requirement 20.4, firewall logs cannot identify all "unauthorized access attempts." Therefore, Dominion recommends rewording this requirement to read as follows: "Document and implement one or more processes for alerting and review of alerts by designated response personnel at each electronic access point within the following time period."

#	Organization	Yes or No	Question 37 Comment
			20.6. Compliance with this requirement is labor intensive and, therefore, not practical for a large number of BES Cyber Systems. Requiring a manual review every 7 days is excessive for the benefit received and does not make allowances for reviewer unavailability due to sickness, emergency work or vacation. At minimum Dominion recommends extending the review requirement to every 30 calendar days or revising the requirement to allow for selected BES Cyber Systems to be reviewed every 7 calendar days as follows: "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for selected BES Cyber Systems within the following time period."21.1. The word "either" should be inserted after the word "provide." The phrase "or controlled access from one system to the other" should be added after "between each system." This modification is reflected in the revised language below: "Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide either logical separation that prevents access between each system or controlled access from one system to the other."The issue is devices that provide a gateway between 2 systems. An example is the node that passes data between the EMS and ICCP networks.
37.13	Network & Security Technologies Inc	Disagree	20.2 - Current wording could be interpreted to mean an access point is required between a BES Cyber System and any other BES Cyber System the Responsible Entity may have defined, even if on a shared network. Could also be interpreted to mean access points are required on a per routable protocol basis. Assuming these interpretations were not intended, 20.2 should be rewritten for greater clarity.20.3 - Except for "document," this requirement seems to duplicate 20.2.20.6 - Wording suggests this requirement applies to all BES Cyber Systems. Is this what was intended, or is it to be applied to access point devices? Please clarify.21.1 - Please clarify intent and applicability of this requirement. Is it intended to apply to virtual machines? Disk arrays shared by multiple application servers? Both? Neither?21.2 - Redundant if all access points are properly identified. Suggest eliminating it or combining the statement with one of R20's sub-requirements.R22 - Seems to overlook physical protections for cyber systems that establish electronic boundaries.22.4 - Configuration changes such as updating access control settings on a firewall or

#	Organization	Yes or No	Question 37 Comment
			revising the physical access permissions associated with a card key should not be subject to this requirement, and it should so state.
37.14	American Electric Power	Disagree	20.2 & 20.3: Regarding "Document and implement access control at each electronic access point established in Part 20.2", is this redundant to R14 - lines 14.1 through 14.3? Suggest rewording or removing if it poses double jeopardy.20.6: Regarding "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period", does this provide any security benefit? If a system event for cyber security was missed by an automated tool, is it reasonable to expect it to be found in a manual review? What is an entity supposed to look for in this manual review?21.2: Regarding "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", it appears that this is a restatement of the elements of R20. If that is not a correct assumption, the SDT need to provide additional information.
37.15	ERCOT ISO	Disagree	20.2: Recommend using “ingress or egress point” instead of “access point”. 22.1-22.3: Please remove reference to other standard. Address the content in the appropriate standard only. The circular references in the existing standards are very difficult to navigate and provide opportunity to miss the requirement.
37.16	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
37.17	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
37.18	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
37.19	Southwest Power Pool Regional Entity	Disagree	Clarify the requirement. A reader could interpret the criteria as requiring an access point between each defined BES Cyber System regardless of network segment placement. 20.4: More often than not, authentication is performed at the end host

#	Organization	Yes or No	Question 37 Comment
			system. Rather than prescribing logging of attempted or actual unauthorized access at the access point, simply require such logging at the point such unauthorized access is detected. 20.6: What are the minimum expectations for a log sampling program (e.g., how much, how often?). 21: Clarify that shared BES Cyber System Components (e.g., a networked storage device) must be afforded the highest impact categorization of all of the BES Cyber Systems sharing the component (similar to the sharing aspect of the electronic access point definition). 22: Include the requirement to protect the access control system from unauthorized physical access.
37.20	CenterPoint Energy	Disagree	Disagree - R20.2 CenterPoint Energy suggests striking the word dial-up. If dial-up is not stricken a TFE may be required to comply with this requirement for serial dial-up paths.CenterPoint Energy believes requirements, R20.3-R20.6, may require a TFE for compliance for non-routable protocols.R20.6 CenterPoint Energy believes the 7 day calendar requirement to review sampling of log entries is overly burdensome and unnecessary. Controls and alert processes to notify appropriate personnel of unauthorized access attempts are mandated in prior requirements. CenterPoint Energy recommends a 30 day review.
37.21	E.ON U.S.	Disagree	E.ON U.S. interprets R20.1 to require documentation of “all” communication paths which could include communication links to all RTUs, etc. This level of documentation is not necessary
37.22	Duke Energy	Disagree	Elimination of terms such as electronic security perimeter without a completely thought through substitute concept contributes to industry frustration. The industry, at least, had come to understand the concept of an ESP. How the “boundary” is identified does not seem well thought through. In the text box, information such as “...cyber systems sharing one or more common electronic access points ...will be treated at the highest BES Cyber system impact categorization level of the BES Cyber system...” seems to belong in CIP 010 where the actual categorization occurs. This information is NOT a technical control and does not seem to belong in CIP 011. Rather it provides additional information concerning the categorization. This standard

#	Organization	Yes or No	Question 37 Comment
			will cause entities to document a lot of confidential information, which then must be protected. R20 - electronic security perimeter is a retired term, suggest replacing with a different term.Table 20: 20.2 is confusing for initial setup processes. How can we explicitly authorize?Requirement 20.2: The electronic access point can therefore be shared between systems as defined in the text box beside R20. For generation stations in particular, there are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). Sharing such an access point is highly desirable. Requirement 20.2, as written, seems to contradict the definition in the text box in requiring that the Responsible Entity establish an electronic access point on EACH routable protocol or dialup communication path between BES Cyber Systems.Requirement 20.4: this requirement makes sense if remote/external access is defined by the "shared access point" as described here (which seems to be in agreement with comments made in sections R11, R12, R13, where the emphasis was on communication between the devices rather than "at the access point").Requirement 20.6: please consider including the words "related to electronic boundary protection" to make the sentence read as follows: Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs relating to electronic boundary protection for each BES Cyber System within the following time period. Also, where logs are accumulated, there is no way to tell if the user was internal or external to the edge device.Table 2121.1 Suggest changing 'prevents' to 'limits' or remove 'that prevents access'. Within Generation, that access is required. Also, Does "logical separation" include "virtual separation"?21.2. Verify this is not just for control centers.
37.23	RRI Energy	Disagree	For 20.1, define communication path, eg., source and destination(s) only or everything in between?For 20.5, what does "all unauthorized access attempts" mean? If an operator fat-fingered login password, does the standard expect alert and follow up each time? "all unauthorized access attempts" needs to be redefined with some threshold before declaring it as unauthorized access attempt. Otherwise, Entities and operators will spend a lot of time documenting unauthorized access and instead of

#	Organization	Yes or No	Question 37 Comment
			securing their assets.
37.24	Northeast Utilities	Disagree	For 20.5, please provide clarification on the meaning of "all unauthorized access". Every password violation for example, is not an unauthorized access attempt but could be interpreted as such. Do we really need to follow-up on every invalid password attempt? Instead of every invalid password attempt, are password lockouts an appropriate trigger? Also, please consider addressing repeated lockouts in the criteria specified.R22 appears to be significantly weaker than the previous standards. One area that is specifically weaker is with regard to access control to Protective Cyber Systems. How can an entity not authorize, review and revoke a role as important as a firewall administrator?
37.25	Constellation Power Source Generation	Disagree	In R20.1 as well as the definition box, the term digital information needs to be defined further. R21 inherently forces entities to further segment their BES Cyber Systems, which is counter to the entire premise of allowing the entities to define their own BES Cyber Systems. Allowing the entities to define their own BES Cyber Systems would limit the scope of an attack, which the SDT stated in the CIP V4 Workshop as their goal in R21. Constellation suggests removing this requirement entirely. Likewise, R22 should be removed as it is completely redundant. Note that in each sub requirement it merely points to another requirement in the document. A suggestion would be to implement the verbiage found in Table R22 to each of the requirements it points to.
37.26	Alberta Electric System Operator	Disagree	In Table R21, was the intent of 21.1 only for Control Centers? The AESO would suggest removing the Control Center parameter and make 21.1 applicable to all High and Medium BES Cyber Systems.
37.27	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
37.28	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 37 Comment
37.29	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event alerting, change control and change management.
37.30	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R20, but recommends changes as follows: o Regarding Part 20.2, since Low Impact BES Cyber

#	Organization	Yes or No	Question 37 Comment
			Systems do not require any Physical Security as defined in previous requirements, it seems inconsistent to require electronic access point security for those systems. o Regarding Part 20.4, how does the Standards Drafting Team envision that a Registered Entity would log "actual unauthorized access?" Actual unauthorized access is not identifiable since it would appear to have been authorized (or the attempt would not have succeeded. o Regarding Part 20.4, in reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. o Is it the Standards Drafting Teams intent that Part 20.5 require an after the fact review of unauthorized access attempts? If so, it may not be possible to adhere to proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week. If it is the Standards Drafting Teams intent that Part 20.5 address responding and monitoring a potential malicious attack situation, then the time frames are not sufficient.Minnesota Power generally agrees with the proposed Requirements R22, but recommends changes as follows: o The language in Part 22.1 creates confusion. The requirement states that remote access is to be restricted as stated in R14 and that for Low Impact BES Cyber Systems this is required. However, in reviewing Requirement R14, only Part 14.1 is required for Low Impact BES Cyber Systems. As a result, does this mean that only Part 14.1 needs to be implemented for Low Impact Cyber Systems in 22.1 or do 14.1-14.4 need to be implemented? The same should be addressed for Medium Impact BES Cyber Systems. o The same type of confusion regarding the language in Part 22.1 exists in Parts 22.2, 22.3, and 22.4. The Standards Drafting Team should consider whether these cross-references are necessary. It does not appear that Parts 22.1-22.4 are identifying specific criteria, but rather are a reminder that these assets need to comply with R14, R16, R18, and R23.
37.31	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 20.1 is unclear as written. Is the communication path expected to end at each and every end point that receives digital information to each BES Cyber System? If this communication path is to each end point, it would be difficult to demonstrate compliance. Does compliance to this requirement also

#	Organization	Yes or No	Question 37 Comment
			require all the communications paths within a WAN or ISP?Requirement 20.2 does not allow a responsible entity to put more than one BES Cyber System inside an access point since it requires access points between systems. This is highly inefficient and creates access points where not needed and could potentially impact the reliability a BES Cyber System. It is unclear why the requirements are moving away from the well established ESP concept. This concept is well established in 'defense in depth' and other security frame works. The requirements for boundary protection should follow the ESP model from V1 and V2 of the NERC CIP requirements. In addition the definition also (inadvertently) conflicts with the definition given at the start of this requirement related to access points and therefore is open to interpretation by auditors.Requirement 20.4 requires the documentation and implementation of one or more "processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point." Until the definition of remote access is clearly defined, it is unclear how responsible entities must comply and demonstrate compliance. In addition, it is unclear if remote access is considered any an access attempt from outside of the access point.Requirement 20.5 requires, "Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period." The responsible entity should be able to determine the threshold for unauthorized access attempts. The way the requirement is written now, personnel would have to investigate every single denied access attempt including someone who accidentally fat fingered their credentials when trying to gain authorized access to a BES Cyber System component. The recommended approach would be to require a review of 4 or more failed attempts against a common UserID without a successful login within 1 hour. Also consider more than X total bad access attempts within one hour for User ID brute force attacks or reconnaissance. Also, in 20.1, please define what is meant by the word "paths" Is it logical or is it physical path?In 20.4, is a single failed login classified as an attempt? The wording states "all attempts at or actual unauthorized access at each electronic access point"In 21.1, does this mean that for example, a SAN

#	Organization	Yes or No	Question 37 Comment
			(Storage Area Network) can be shared by Cyber System Component and other devices as long as there is logical separation?In 21.1, if two BES Cyber Systems "share" a network switch, does this meet the requirement of "logical separation"?
37.32	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event

#	Organization	Yes or No	Question 37 Comment
			alerting, change control and change management.
37.33	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R21.1 - Puget Sound Energy has concerns that Cyber System Components that are shared between BES Cyber Systems must provide logical separation. For example: For entities with Control Centers that utilize a Microsoft infrastructure, multiple BES Cyber Systems may centrally authenticate (or have logical security controls) facilitated by a single or clustered Microsoft Active Directory domain controller. As the requirement is currently written, Puget Sound Energy feels that those shared domain controllers would not be able to reside on the same local area network segment as the domain they participate in. Puget Sound Energy requests clarity be added in to this requirement.Table 22 - Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
37.34	LCEC	Disagree	R20 - 20.1 Must define what is included in communication paths. If needed specify physical interface. Digital information is actually digital data, control, or signals.20.3 is not auditable. What is access control. There is no defined scope.20.5 includes requirements for cyber incident response which is covered in a later requirement.Need to clearly identify what is considered an access point on multiple interface devices.20.6 what's the difference between this and 18.4?21.2 A BES Cyber System could include components at different physical locations that communicate with each other. This is not technically external to the system so does it apply here?
37.35	FirstEnergy Corporation	Disagree	R20 - 20.6 - Need greater clarity around whether automated alarming can be used rather than manual review of logs. This sub requirement is unnecessary with an automated system in place.R21 - We agree with the use of 'logical separation' in this requirementR22 - We do not like the way R22 refers back to other requirements. This

#	Organization	Yes or No	Question 37 Comment
			is redundant and the requirement should be eliminated.
37.36	Consultant	Disagree	R20 - The terminology appears to be incorrect. Electronic access points do not define an electronic security perimeter. It also seems odd to say the defined term Electronic Security Perimeter is going to be retired, and then use that same term to define a requirement. "Electronic Boundary Protection" is created by identifying an electronic security perimeter based on the logical network connections of cyber assets, which includes electronic access points for External Connectivity that provides Remote Access to the assets within the electronic security perimeter. Suggest retaining the term Electronic Security Perimeter as described here.Table R20 - Items 20.1 & 20.2 - This appears to be "Identifying the Electronic Security Perimeter" as describe in the comment above regarding the usage of the term Electronic Security Perimeter, but stated in more confusing language in both cases.Item 20.3 Suggest rewording as "Implement and document access control mechanisms for each electronic access point (to the Electronic Security Perimeter)."As a general comment you would "implement and document" rather than "document and implement"Item 20.4 Suggest rewording as "Implement and document access attempts and access authorizations at each access point." Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "Required"Item 20.5 contains two requirements:1. Implement and document processes to identify unauthorized access attempts at each electronic access point.2. Responsible entities shall review unauthorized access attempts in the time frame specified.Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "48 hours" & "12 hours".Item 20.4 - It would appear to create an excessive administrative burden without corresponding decrease in risk to require this review every 12 hours for High Impact Assets. Suggest changing required review time to "Daily".Item 20.6 - The requirement statement is subjective in regard to the degree of sampling, sorting, and filtering allowed, expected, or required. This is a requirement similar to event log review of Table R18 - Item 18.4 and the wording of these two requirements should be similar.Item 20.6 -

#	Organization	Yes or No	Question 37 Comment
			This requirement is regarding access through electronic access points and "7 calendar days for external connectivity only" is redundant. Suggest deleting "for external connectivity only"Item 20.6 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 20.4 and 20.5 (as commented) require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Items 20.1, 20.4, & 20.5 - Delete the word "all" It is redundant and unnecessary to the requirement statement. (The word "all" should be removed from "all" requirement statements in the standard")Table R21 - Item 21.1 This requirement appears to create a mutually exclusive situation where shared cyber system components are separated. The wording needs to be clarified or, as it is worded it should be deleted.Item 21.1 The application of the requirement to control centers creates an added dimension to the impact categorization. The application of requirements is based on impact categorization. Modify the impact categorization criteria to capture the assets where this requirement should be applied.Item 21.2 This item appears to restate what is previously stated in the referenced R20. If some additional requirement is intended, then that requirement should be included in the reference R20 requirements list, rather than a 'hidden' requirement that is cross-referenced here.R22 - This requirement appears to be redundant. The requirements referenced in the Table R22 (R14, R126, R18, & R23) appear to include whatever is listed in this requirement. If there is some additional requirement that is intended, that requirement should be put in the respective referenced requirements. Each requirement statement and table should be contain everything related to that requirement, rather than having a separate requirement that 'adds' to other requirements.
37.37	Xcel Energy	Disagree	R20.1 - The definition and level of detail for “communication paths” is needed. For example, does this include a commercial telephone carrier used to communicate between relays?R20.2 - Clarifying language is needed for “Establish an electronic

#	Organization	Yes or No	Question 37 Comment
			access point". Does this mean in documents, drawings, etc?R20.5 - This requirement needs clarification. Are these intended to be automatically generated alerts, such as logs? The current language could be interpreted to require a 12 hour review of a login attempted that failed due to an incorrectly typed login ID, as automated software may interpret this as an authorized login attempt. Also, 12/48 hours to complete a review of a failed unauthorized login attempt is unreasonable and unnecessary. R21.1 - We would like additional information on what type of "logical separation" is expected.
37.38	Ameren	Disagree	R20.1 - This will require use of a firewall at all locations or similar devices. Simply documenting this information is not practical for non routable devices. Also, clarify if communication paths, refer to physical equipment or locical paths. R20.2 - What is the difference between R20.2 and R20.3? Suggest combining the two requirements.R20.5 - 12 hours does not allow for weekends or for events that occur outside business hours. This should be increased to 24 hours or lowered to 24x7 (continuous). Also, need to clarify whether the alerts need to be reviewed during the time frame given (48 hours, 12 hours, or 7 days) or that alerts need to be sent every 48 hours, 12 hours, or 7 days. Please clarify how often should alerts be sent and how often do they need to be reviewed. R21.2 - Where does an RTU or serial communication fit into this requirement? Need to add more clarification on this requirement of what devices are included. R22 - Need to add requirements at a minimum for account listings, approvals, and access controls. There are no considerations for risk assessment or training for users of these devices. Also, these devices should be included in the Vulnerability Assessment.
37.39	US Bureau of Reclamation	Disagree	R20.2 should be modified to read "Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems." Define the use of "other devices" in this context. R20.4 - add "where feasible" to this requirement.R21.2 - Please provide and example...

#	Organization	Yes or No	Question 37 Comment
37.40	Entergy	Disagree	R20.5 Entergy cannot understand the reasoning behind the criteria of 12 hours? Why not 6 or why not 24?R21.1 is unclear and must be reworded to better reflect exactly what the SDT had in mind. We cannot guess at what that might have been.R22 - Entergy suggests R22 apply equally for high, medium and low assets; and thatthe requirements for processes and procedures in this section should be placed back into each of the respective sections (R14, 16, R18 and R23).
37.41	Western Area Power Administration	Disagree	R20.6 - Is this a requirement to review, and document the review, of logs weekly?R21.2 - Unclear. Does it mean our "one-way" rule from internal to external? Or does it mean use a proxy located outside the ESP?
37.42	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R20.6. With the obligation of reviewing alerts designated in R20.5 the requirement for manual review of logs should be extended to a 30 day window.
37.43	BCTC	Disagree	R22. Suggest just removing this requirement as it just references previous requirements
37.44	Hydro One	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity’s to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.45	ISO New England Inc	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communications between two end points20.3 should be part of 20.2 - denys and explicit allows might be better language. R20.5 Please define what is an unauthorized access attempt. A user may be authorized but may try to connect using telnet where telnet is disabled. Is this considered unauthorized? Recommend

#	Organization	Yes or No	Question 37 Comment
			removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move it's table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23R21.1 = question on what is "logical separation" very vague
37.46	Northeast Power Coordinating Council	Disagree	Request clarification on "all communication paths" in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.47	Oncor Electric Delivery LLC	Disagree	Requirement 20.4, 20.5 and 20.6 are not applicable to some legacy cyber systems. These requirements should only be required for systems which utilize routable communication.Requirement 22 references other requirements and should be eliminated because it is redundant.
37.48	Garland Power and Light	Disagree	Requirement 20.6 - What we really feel is that this is impractical and should be deleted. However, it was stated at the NERC CIP workshop that the intent was to verify that the automated system capturing various logs off cyber devices was actually capturing each log - intent needs to be added to the requirement or wording changed to better express the intent at a minimum. Requirement 22 - Keep life simple - add the words "and Protective Cyber Systems" after the words BES cyber systems in each of the referenced requirements (14, 16, 18, and 23) and DELETE Requirement 22 - that way, everything is covered by the referenced requirements that this R22 uses
37.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that R20.1 is not clear. What is the point of documenting paths that transmit or receive digital information external to each BES Cyber System if they may not interface with other BES Cyber Systems? In addition, another observation from SDG&E related to R20.1 has to do with non-routable protocols. If this requirement

#	Organization	Yes or No	Question 37 Comment
			includes the documentation of non-routable protocols, it can become VERY expensive to document "chatty" protocols that broadcast to lots of assets (DHCP and BOOTP, to name just two examples).In R20.2, SDG&E asks for a clarification of the term "explicitly".SDG&E recommends grammatical changes for R20.4. We feel it should read "Document and implement one or more processes for logging all authorized remote access sessions and all successful and unsuccessful attempts of unauthorized access at each access point within the following time period. SDG&E suggests the following changes to R20.5: "Document and implement one or more alert processes that includes review of alerts by designated response personnel..." SDG&E feels that R21.1 is a bit confusing and worthy of discussion. If affected cyber systems and components are on the same network anyway, then what are the benefits of logical separation?
37.50	Allegheny Energy Supply	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." (In general, using the existing terms where possible will cause much less confusion.)
37.51	Allegheny Power	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."
37.52	EEI	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for

#	Organization	Yes or No	Question 37 Comment
			manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than "System Boundary Protection."Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.53	Progress Energy (non-Nuclear)	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.Is the relay communications port for local interface with a laptop considered as an electronic access point? If so, this complicates these requirements.R20.1 by external to each BES system do you mean outside individual six walled boundaries?R20.6 is not needed, as long as we do R20.5.For 20.5 - Don't see the need for more than one capability.For 20.6 - change to "document process to ensure automatic monitoring and alerting process is working properly"CIP-011 - R20 - Are communications between Control centers and field RTUs/IEDs which do not employ routable protocols considered remote external communications?R20.6 - Need additional guidance as to what constitutes a manual review and the minimum sampling required.CIP-011 - R21 - Need clarification with guidance as to what constitutes "Cyber systems components in control Centers that are shared between BES Cyber Systems"

#	Organization	Yes or No	Question 37 Comment
37.54	Detroit Edison	Disagree	Table entries 20.4, 20.5, and 20.6 specify external connectivity only. This text is not necessary since the requirement is boundary protection and that implies external connectivity is the scope.
37.55	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on this question, but also provides the following drafting suggestions:R20. Objective:To define an electronic security perimeter thereby minimizing the risk of system intrusion.R20. Requirement:Each Responsible Entity shall document and implement processes that establish electronic access controls point that incorporate the criteria in CIP-011-1 Table R20 - Electronic Boundary Protection. In R20 Table 20.2 we are concerned about the term “explicitly authorized communication.” It is our assumption that a password is sufficient to comply with this requirement. If the drafting team intended another meaning we believe this will not be reasonable and we could not support this definition. We propose the following revised language:Table 20.2: Establish electronic access control on each routable protocol or dialup communications path between BES Cyber Systems and other devices.We recommend that R20 Table 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. R21. Objective:To protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components. R21. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R21 - System Boundary Protection. The APPA Task Force supports the MRO-NSRS proposal to delete criteria in R21 Table 21.2. This is a redundant requirement and would put an entity in noncompliance of 2 requirements for one violation. The APPA Task Force recommends removal of R22. All of the criteria in Table 22.1 - 22.4 refer to previous requirements and will put an entity in noncompliance of 2 requirements for one violation.

#	Organization	Yes or No	Question 37 Comment
37.56	Bonneville Power Administration	Disagree	The objectives of these requirements ("to define an electronic security perimeter thereby minimizing the risk of system intrusion," "to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components," and "to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R20Section 20.1 This is unacceptable. The requirement does not limit the extent of the documentation. Conceivably, it could require documentation of the entire Internet, if the BES Cyber Asset had direct or even indirect access to the Internet. The requirement needs to be limited. Recommendation: Remove the requirement. It is difficult to see how to write it in a way that encompasses all possibilities without leading to results such as the one described above. Instead, document external interfaces as part of the configuration management process.20.2: Requiring an electronic access point between a BES Cyber System and any other system produces unacceptable complication, latency, and administrative burden for a facility with multiple BES Cyber Assets in close proximity. As an example: 20.2 would require that all traffic from one BES Cyber System within a Control Center to any other system within the Control Center to go through a firewall or some other access control device. It is unlikely that this was the intent of the entry. Recommendation: Replace "Required" with "Required for external connectivity only", using the redefinition of external connectivity described above.20.3 Similar issue to 20.2 Recommendation: Replace "Required" with "Required for external connectivity only" throughout the table.20.4 - 20.6. Remove, the are already covered under 18.3 and 18.4. R18 and Table R18 require monitoring of all cyber security events, whether at access points or at BES Cyber Systems themselves.20.6. First, the requirement is already covered more clearly in Table R18. Second, it is unclear why a Electronic Boundary Protection requirement should be addressing BES Cyber Systems. Third, The intent is unclear,

#	Organization	Yes or No	Question 37 Comment
			due to the plethora of "ors" in the requirement. It could be that a manual review is always required, using sampled, sorted or filtered logs. It could also be that a manual view of logs is required, using sorted or filtered logs. It could also be that either a manual review or {sorted or filtered logs} is required. Part of the confusion is that filtering is clearly a method to sample, and sorting may be, as well. It would probably be better not to use those terms at all. In addition, there should be a provision to allow automated review of log entries. Recommendation: Delete the entry.Table R21Section 21.1 is completely unacceptable. It is quite possible in a Control Center for a single Dispatch workstation to provid access to several BES Cyber Systems. The requirement in 21.1 would make this impossible. The alternate would be to provide a separate workstation for each such system, which is unacceptable.Section 21.2 is acceptable only with externally connected redefined as described above.R22 and Table R22: These are references to other requirements. It seems that rather than referring to the other standards from this one, it would be cleaner to simply include this requirement as part of those other standards. That is, put the necessary references in R14, R16, R18 and R23.
37.57	Constellation Energy Control and Dispatch, LLC	Disagree	The timeframe in 20.5 for medium and high should be the same.
37.58	ReliabilityFirst Staff	Disagree	To eliminate confusion, we believe the drafting team should develop a definition for “protective cyber system”. We also believe that Table R22 should include an additional requirement stating, “Implement processes as specified in Requirement R15 - System Security.” and make this new requirement TFE eligible. Further, this new requirement should be “Required” for medium and High Impact BES Cyber Systems.
37.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
37.60	American Transmission	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized

#	Organization	Yes or No	Question 37 Comment
	Company		communication.We believe items 20.4 - 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.61	MRO's NERC Standards Review Subcommittee	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe item 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe item 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe the following should be added to the end of item 20.6: “at each electronic access point established in Part 20.2”. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only. It also makes for a consistent approach with item 20.3.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs

#	Organization	Yes or No	Question 37 Comment
			non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.62	The Empire District Electric Company	Disagree	We believe item 20.2 is going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe items 20.4 - 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.63	We Energies	Disagree	We Energies agrees with EEI: Suggest using electronic security perimeter rather than "Boundary Protection."We Energies agrees with EEI: Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.We Energies agrees with EEI: Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: We Energies agrees with EEI: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.We Energies agrees with EEI: For R 20.5: Document and

#	Organization	Yes or No	Question 37 Comment
			implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.We Energies agrees with EEI: For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. We Energies agrees with EEI: Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.We Energies agrees with EEI: R21: Suggest using electronic security perimeter rather than "System Boundary Protection."We Energies agrees with EEI: Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. We Energies agrees with EEI: R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.We Energies agrees with EEI: Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.We Energies agrees with EEI: There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.64	GTC & GSOC	Disagree	We recommend rewording R21.1 to provide clear direction on what is expected to comply with this requirement because the wording is ambiguous. We are unable to suggest alternative language because we are not certain of the intent. If this requirement would prevent, for example, the use of a shared backup system for two Cyber Systems we do not see the reliability based justification for the requirement and would recommend its elimination.
37.65	Emerson Process Management	Disagree	What is the difference between "Electronic Access" in R20-R22 and the "Remote and Wireless Electronic Access" in R11-R13?

#	Organization	Yes or No	Question 37 Comment
37.66	Manitoba Hydro	Disagree	What is the meaning of “dial-up”? The wording for Requirement R20.2 is unclear. The suggested wording for Requirement 20.2 is “Establish an electronic access point that denies access by default and allows explicitly authorized communications on each routable protocol or dial-up communication path between BES Cyber Systems and other devices. Requirement R20.2 is inconsistent with Requirement R20.3. It is unclear how explicitly authorized communication is allowed without the implementation of access controls for Low Impact BES Cyber Systems. Requirement R20 does not contain any requirement for response to alerts. The wording for Requirement 21.1 is unclear. The suggested wording for Requirement 21.1 is “Cyber System Components that are shared between BES Cyber Systems must provide logical separation that prevents access between each system.” and change the wording in the impact columns to “Control Centre Only”. The wording for Requirement R21.2 is unclear. The suggested wording for Requirement R21.2 is “All external communication to the BES Cyber System must occur through an electronic access point as specified in Requirement R20.” Requirement R22 is missing the requirement for the physical protection of the cyber system that establishes the physical or electronic boundaries of the BES Cyber System. There are no specifics given with respect to ‘logical’ separation in Requirement R21.1 so it is assumed to be at the Responsible Entity’s discretion to determine.

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

Summary Consideration:

Many commenters agreed with the definition of Electronic Access Point, but other commenters requested clarifications in the definition. A number of commenters recommended changes to language concerning systems sharing an electronic access point. Some commenters suggested removing the sharing of electronic access points from the definition.

In response, the SDT has modified the definition of an **Electronic Access Point** to: *"An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets"*.

The sharing of electronic access points is likely not an issue because High Impact BES Cyber Systems are Control Centers and would rarely share an Electronic Access Point with Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 38 Comment
38.1	WECC		Move to definition to beginning of the standard; dislike the definition box in the middle of a requirement. Make clear that access points can be anything that meets the definition and not only firewalls or devices specifically created for this purpose that must be put "in line". Ie. an Access Point can be the actual device itself providing access control.The phrase "where electronic access can be controlled" will prove difficult to audit. Inherently it allows an exception. All communication paths should be in scope regardless of the ability to control electronic access. It is not foreseen that communication paths could not be controlled.
38.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
38.3	NextEra Energy Corporate Compliance	Agree	Is a serial connection to a BES Cyber System considered an electronic access point? Please clarify in requirements.
38.4	Minnesota Power	Agree	Minnesota Power agrees with the proposed definition of electronic access point, but recommends replacing "All cyber systems sharing..." with "All BES Cyber Systems

#	Organization	Yes or No	Question 38 Comment
			sharing..."
38.5	Duke Energy	Agree	The second sentence is a requirement, not part of a definition; consider moving. Specify that "All cyber systems" only applies to BES Cyber Systems. This definition, particularly the concept of "sharing one or more common electronic access points or components" is much more practical in a power plant environment. See previous comments on R11, R12, R13.
38.6	Public Service Enterprise Group companies	Agree	There is general agreement, but need for clarification in the language in one regard. Please clarify whether this requirement would necessitate classifying a Distribution cyber system at a High Impact level if both the Distribution cyber system a High Impact BES cyber system at substation are interconnected using a single router/firewall device to a communications provider. I.e., effectively an additional router/firewall would be required in this situation to not entail classification of the Distribution cyber system at a High Impact level.
38.7	Consultant	Disagree	According to this definition electronic access point where electronic access cannot be controlled for communication paths that transmit and/or receive digital information would not be considered an access point?An access point should defined as locations where information crosses the established protection boundary, or as the locations where external connectivity or remote access occurs. An access point is not dependent on the ability to control the communication path. The sentence "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." is a requirement. It is not a definition nor part of a definition. The concept is sensible, but still not a definition. Suggest moving this to the requirements table.Suggest modifying this definition to be consistent with "External Connectivity" and "Remote Access" definitions.

#	Organization	Yes or No	Question 38 Comment
38.8	Northeast Utilities	Disagree	Agree in principle with the definition but disagree that all cyber assets sharing the access point will be treated at the highest BES Cyber System impact categorization. This will have a big impact on development and test systems as well as other related but not critical systems. How will this impact DMZ systems which by design are not trusted?
38.9	Alliant Energy	Disagree	Alliant Energy agrees with EEI in that it is appropriate to apply protective measures to the literal ingress points (interfaces) on the electronic access points, but not the requirement to apply protective measures to all of the components that connect to said ingress interfaces (to require this creates a house of mirrors.)
38.10	E.ON U.S.	Disagree	CIP-011, R20.1 See previous comments regarding the definition of “external”.CIP-011, R20.1 “Document all communication paths that transmit and/or receive digital information external to each BES Cyber System.” Does this include the WAN if the defined BES Cyber System is inclusive of multiple sites/locations? All equipment and communication paths such as a Sonet ring?CIP-011, R20.3 The term “access control” should be further clarified. Does implementation of firewall rules alone limiting access as defined in R20.2 meet this requirement, or does this require further mechanisms to provide “access control” on an individual user-basis?CIP-011, R20.4, R20.5, R20.6 See previous comments regarding the definition of “external.”CIP-011, R21.1 How might the logical separation called for here be implemented?CIP-011, R21.2 See previous comments regarding the definition of “external.”
38.11	Progress Energy (non-Nuclear)	Disagree	Communication paths may be better defined by including routable protocol and/or ‘external to the BES Cyber System’.Assuming this is the same as external access point it does seem somewhat repetitious.
38.12	American Electric Power	Disagree	Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and receive; or only receive digital information. All cyber systems sharing one or more

#	Organization	Yes or No	Question 38 Comment
			common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).Rational: An electronic access point that provides a transmit and receive path or a receive only path to a BES Cyber System provides an access path into the system to be used for possible exploit. By limiting traffic to transmit only communications the risk to the protected BES Cyber System is reduced since an electronic access point is not provided.
38.13	Entergy	Disagree	Entergy suggests adding specific language to the definition that includes “uses routable protocol or is dial-up accessible”
38.14	APPA Task Force	Disagree	In the APPA Task Force comments for Question 37 we proposed changing electronic access point to electronic access control. We do not feel it is necessary to define an electronic access point. We do believe it is necessary for entities to have control of their boundaries. We have proposed using electronic access control in R10, Account Access Control Specifications, in the place of the term Password since we feel there are other methods of controlling access that are equivalent or superior to password protection. We recommend the drafting team use electronic access control rather than defining another High Impact BES Cyber System outside of CIP-010-1.
38.15	Dairyland Power Cooperative	Disagree	In trying to be general, it adds more question as to the intent. Is an access point one a device physically connecting multiple communications paths? What about a terminal server? Is an authentication server or policy managing server an access control point even if it is not in-line with the path?
38.16	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
38.17	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact

#	Organization	Yes or No	Question 38 Comment
			categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.18	LCEC	Disagree	Need to clarify the specific access point from an interface perspective. What is meant by the term controlling access? Is this from a network protocol perspective? Is a radio link that extends serial communications considered to be an access point?
38.19	Progress Energy - Nuclear Generation	Disagree	Not all EAPs constitute the highest degree of risk especially is nuclear facilities which are highly secure.
38.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.Further, PacifiCorp believes the proposed definition is too broad. The preference would be to and should be restricted it to communications supporting routable protocols and or dial-up communication. In 20.2 the standard refers to the use of an access point on routable protocol and or dial-up paths but the definition is currently proposed to be broader. In plant control systems, we have many devices which use an IP routable protocol and an industrial communication control protocol such as fieldbus or profibus in the same device. The new definition would require each of these devices to be defined as an access point.
38.21	American Municipal Power	Disagree	Please provide a little or no impact category

#	Organization	Yes or No	Question 38 Comment
38.22	FirstEnergy Corporation	Disagree	Please provide clarification and examples on definition. Propose changing the second sentence to “All BES cyber systems sharing one or more common electronic access points or components will be logically separated such that each logical system is treated at its own categorization level or, where not separated, electronic access points will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).”
38.23	Dominion Resources Services, Inc.	Disagree	Please see Dominion’s response to Question 13. The interface between systems contained wholly within an access controlled facility should not constitute an electronic access point or be subjected to the Boundary requirements.
38.24	Southern Company	Disagree	R20.5 Is a single or double access attempt on a single access point required to be reviewed?
38.25	San Diego Gas and Electric Co.	Disagree	SDG&E has concerns about the last half of the proposed definition for electronic access points. If two medium or one medium and one low BES Cyber System share an access point, this definition makes the shared access point High impact? Regardless of other controls that may be in place? We feel that this definition is not reasonable.SDG&E suggests the definition of electronic access points should include the words "...between networks." Otherwise, every device on the network becomes an access point.
38.26	BGE	Disagree	Should include wording to clearly define the communication paths that transmit and or receive digital information to a BES Cyber System.
38.27	Allegheny Energy Supply	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security

#	Organization	Yes or No	Question 38 Comment
			requirements.
38.28	Allegheny Power	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.29	EEI	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.30	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The concept of sharing access points must be better defined. Does connectivity to an outside entity at a firewall constitute a shared access point?
38.31	Luminant	Disagree	The definition of access points infers that cyber systems and BES Cyber Systems can share an access point but 20.2 states that BES Cyber systems must be seperated from other devices. re. Cyber systems protected by same firewall but in different zone
38.32	US Bureau of Reclamation	Disagree	The definition proposed is that "ALL cyber system sharing one or more common electronic access point or components..." Components can mean many things and almost all devices share components which have not impact on the BES. It would be better to indicate that "ALL BES cyber systems sharing one or more common

#	Organization	Yes or No	Question 38 Comment
			electronic access point or BES CYBER SYSTEM components...."
38.33	Constellation Energy Control and Dispatch, LLC	Disagree	The definition should clearly establish that the access point is a place where digital information is transmitted or received.
38.34	US Army Corps of Engineers	Disagree	The definition states that an electronic access point is a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. What does "controlled" mean? Would network switches fall under this definition because network switch ports can be electronically controlled with port security?Suggest definition be changed to: An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled, and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may also be restricting sensitive traffic from leaving a higher security area to a lower security area.
38.35	Bonneville Power Administration	Disagree	The first sentence, "Electronic access point for...digital information.", is acceptable, but only because it says what an electronic access point is, not where one has to be located. Second sentence is completely unacceptable, more so than anything else in the standard, for numerous reasons:First, it leads to the equivalent of CIP-007's including every network device within the Electronic Security Perimeter. In retrospect, that inclusion caused additional workload and costs which far exceeded the gain in security. To repeat that error would be totally unacceptable. The requirement should apply only to BES Cyber Systems, and not all cyber systems.Second, it ignores the level of threat posed by the various systems. Just because a cyber system or even a BES Cyber System is behind the same access point as a High impact BES Cyber System does not mean that poses the same risk to the BES, or even any risk at all.Third, it ignores the possibility of nested access point. For instance, consider systems A and B residing within a highly protected network and sharing a single access point. Add system C residing with a less protected network with an access point to the internet. If A and B access the internet through the same

#	Organization	Yes or No	Question 38 Comment
			access point that C uses, then C has to be treated as stringently as the highest impact of A or B.Fourth, applying impact levels based on the highest level of the BES Cyber System is a problematic issue that has been discussed at length. The mere fact that a cyber component exists within a High Impact BES cyber system does not make that specific component a high impact component. There are levels of impact that should be applied within and to the Cyber System. Devices or equipment (Components) within a High impact BES cyber system, may actually have little or no impact on that cyber system regardless of what happens to them. The standard that applies to that device should not necessarily be tied to the Impact rating for the whole BES cyber system.Finally, the second sentence is a statement of a requirement, not a definition. To use an example, assume a Control Center that relies on nested networks, with the outermost controlling external access, and further firewalls controlling access to their nested layers. The outermost firewall would be a common access point, shared by all systems within the Control Center. In that case, all the cyber systems would have to be treated as BES Cyber Systems at the highest impact level of any BES Cyber Systems in the Control Center. Such a treatment ignores the threat a system might or might not pose to the BES. To provide a somewhat absurd but demonstrative limiting case, a minimally functional print server residing in the outermost layer, barely able to accept an IP address, and having no connectivity except Ethernet on one side and a printer interface on the other, would have to be treated the same as an AGC system within the innermost layer controlling thousands of megawatts of generation at sites scattered across multiple states.Recommendation: Delete the second sentence.
38.36	Southern California Edison Company	Disagree	The requirement does not adequately address the technical nuances of virtualization. The central point of virtualization capability can be interpreted as the “shared” access point. At the same time, the centrally located virtualization device may also be interpreted as a BES critical cyber system. In the first case, the controls for the virtualization system will be those afforded to an access point, which may be less stringent than those afforded to a BES critical cyber system. In the second case, where the virtualization device is a BES critical system, on the user end, end user computing devices such as mobile laptops can potentially be considered as BES cyber system

#	Organization	Yes or No	Question 38 Comment
			component, and on the SCADA end, automation devices would be considered as BES cyber system components. Requirement R21 does not make drawing such distinctions clear of subjective interpretation.
38.37	Oncor Electric Delivery LLC	Disagree	The term “public communication paths” should replace “communication paths”. Systems which are isolated from the internet are less susceptible to cyber attacks.
38.38	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
38.39	Xcel Energy	Disagree	We believe the second sentence places an unnecessary burden on lower impact systems if they are unable to communicate with the higher impact system, as is the case with dial-up based systems.
38.40	We Energies	Disagree	We Energies agrees with EEI Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.41	US Army Corps of Engineers, Omaha Distirc	Disagree	What does "controlled" mean? Definition also appears to contain a requirement "All cyber systems sharing one or more . . " The requirement doesn't appear to be in line with industry practice. A firewall can protect 2 or more networks from external connections and from each other. Both networks do not have to be at the same sensitivity level. suggest definition be changed to:An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may

#	Organization	Yes or No	Question 38 Comment
			also be restricting sensitive traffic from leaving a higher security area to a lower security area.

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions to clarify them, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. For example, the SDT made changes to the applicability column to include the scoping filter of External Routable Connectivity where the use of a routable connection would be required to comply with the requirement, such as the requirement to have Electronic Access Points.

The intent of this approach is to refine the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in the CIP Version 5 standards.

#	Organization	Yes or No	Question 39 Comment
39.1	US Army Corps of Engineers		The statement in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.", is confusing. What is the standard trying to say here?
39.2	GE Energy	Agree	20.2: Low BES systems should be required to document and implement access controls.
39.3	Black Hills Corporation	Agree	21.1 requires further definition of logical separation requirements in a disaster recovery scenario. As stated, this does not allow for control centers to back-up each other in a fail-over mode for disaster recovery.
39.4	Duke Energy	Agree	Agree if the external connectivity is via a shared electronic access point as discussed in previous comments.Apply all requirements, where currently in place, only for external connectivity. 20.6: Review of logs every 7 days is not practical.21.2: Only

#	Organization	Yes or No	Question 39 Comment
			require for external connectivity
39.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
39.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
39.7	GTC & GSOC	Agree	We recommend a slight rewording of R20.2 as follows “Establish an electronic access point that denies access by default and allows explicitly authorized communication on each path where a routable protocol or dialup communication exists between BES Cyber Systems and other devices.”
39.8	E.ON U.S.	Disagree	: E.ON U.S. does not believe there is a need for compliance requirements for low impact systems. High Impact has such a short timeframe for revocation, that it would require employees be available to revoke privileges 24/7. The SDT should adopt a more reasonable time frame- at least 24 hours. E.ON U.S. believes that R22 is merely a repeat of other requirements and therefore should be deleted
39.9	NextEra Energy Corporate Compliance	Disagree	: NextEra believes it is unclear what the timeframes for Medium Impact and High Impact BEST Cyber Systems are supposed to mean. Do response personnel have to review security logs related to external connectivity every 48 hours or are the expectation for designated personnel supposed to respond to an alert within a 48 hour period? The recommendation is to document and establish one or more processes for automated alerting and response to alerts by designated response personnel for unauthorized access attempts at each electronic access point. This requirement would be applicable to both Medium and High Impact BES Cyber Systems. If automated alerting and notification is not technically feasible, Responsible Entities should be able to develop a process to manually review security logs to determine potential cyber security incidents.

#	Organization	Yes or No	Question 39 Comment
39.10	Regulatory Compliance	Disagree	20.1 STRIKE "Required for Low Impact20.5 Propose - 72 hours for Medium Impact Propose - 48 hours for High Impact21.1 - STRIKE "required" for Medium Impact
39.11	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
39.12	Florida Municipal Power Agency	Disagree	22.2 - Add medium, require low to asses quarterly. Consider high impact to review 'critical' patches within 7 days.22.3 - This should be consistent with R18; medium should be required to monitor their systems. Low should review logs at least quarterly for events, or at least have an automated system in place to alert for specific threats.
39.13	ERCOT ISO	Disagree	22.2-22.3: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
39.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
39.15	The Empire District Electric Company	Disagree	Comments: For items 20.4 - 20.6, we believe "for external connectivity only" should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.16	Progress Energy - Nuclear Generation	Disagree	Durations should align with information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
39.17	EEI	Disagree	EEI recommends deleting R21 because it is vague and the risks are addressed in R20. Introducing boundaries within engineered systems will result in decreased reliability.
39.18	Entergy	Disagree	Entergy suggests making R20.3 and R20.4 apply to low impact assets.

#	Organization	Yes or No	Question 39 Comment
39.19	MRO's NERC Standards Review Subcommittee	Disagree	For items 20.4 - 20.6, we believe “for external connectivity only” should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.20	US Army Corps of Engineers, Omaha Distirc	Disagree	Intent of 22.1 is unclear
39.21	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
39.22	Luminant	Disagree	Low impact BES Cyber Systems should be protected but not have to be seperated from all other cyber systems. re introduces the concept of cyber systems in "ESP". R21 How can cyber systems be shared and not be a BES Cyber System
39.23	LADWP	Disagree	Low impact requirements will become an administration issue.
39.24	Minnesota Power	Disagree	Per the discussion regarding these tables in Question 37, Minnesota Power recommends that for Parts 20.1, 20.2, 21.2 and 22.1 “Required” be removed for Low Impact BES Cyber Systems.
39.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. In 20.5, aligning the time requirement on 48 hours for clarity and consistency.
39.26	American Municipal Power	Disagree	Please provide a little or no impact category
39.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
39.28	FirstEnergy Corporation	Disagree	R20 - Timeframes should not be in ‘hours’ (i.e. less than a full day). Tracking by time

#	Organization	Yes or No	Question 39 Comment
			rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.R21 - R21.2 - Remove 'Required' for Low Impact Cyber Systems.R22 - Eliminate - see Q37 above.
39.29	Con Edison of New York	Disagree	R20 dialog box; speaks to inheritance of HIGH Impact BES requirements for all cyber systems with shared access points.o Does the inheritance only apply to R20 requirements or does this mean all requirements for these devices would be at the High Impact level?o If all cyber systems regardless of BES use that are within the same boundary require High, this may cause significant manpower or create the need to isolate the true BES systems. The isolation will take significant time to plan and implemento This standard must allow the use of 1 physical firewall, logically separated to isolate networks without inheritance of BES levelR21.1 does this require Cyber Components on the same isolated network be logically separated? Is that correct?o This should not apply to devices on the same network.o Should only be required for high.R20.6 - if automated review and alerting is used this should not be requiredR22 mentions established physical boundaries --- the draft CIP standards do not mention physical boundaries are the PSP requirements defined in this version?
39.30	Southwest Power Pool Regional Entity	Disagree	R20: Distinction between external and non-external connectivity is not appropriate. R22: Patch management should be applicable to all impact categories.
39.31	Hydro One	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to

#	Organization	Yes or No	Question 39 Comment
			Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.32	ISO New England Inc	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifing “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5Recommend that 20.6 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommended removing R21 in the answer to question 38Recommend moving the R22 criteria in the answer to question 38. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.33	Northeast Power Coordinating Council	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.34	National Grid	Disagree	Refer to comments in Q. 37.
39.35	Oncor Electric Delivery LLC	Disagree	Requirement 20.6 should provide for a review every 30 days.
39.36	US Bureau of	Disagree	Requirement 22.1 conflicts with earlier requirements regarding controls on remote

#	Organization	Yes or No	Question 39 Comment
	Reclamation		and wireless access.
39.37	San Diego Gas and Electric Co.	Disagree	SDG&E feels that too many classifications make compliance more difficult and likely more risky. We would suggest making the time in R20.5 24 hours for both High and Medium impact systems.SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
39.38	LCEC	Disagree	See previous comments
39.39	Bonneville Power Administration	Disagree	See Question 37, above.
39.40	Constellation Energy Control and Dispatch, LLC	Disagree	See response to question number 37.
39.41	ReliabilityFirst Staff	Disagree	Suggest “30 calendar days for external connectivity only” for Medium Impact in row 20.6. Suggest “Required” for Medium Impact in rows 22.2. and 22.3.
39.42	Ameren	Disagree	Suggest removing R21.2 from Low Impact Systems.
39.43	Alberta Electric System Operator	Disagree	Table R20 - For 20.5 set Low Impact to “120 hours for external connectivity only”; for 20.6, set Medium Impact to “30 calendar days for external connectivity only”Table R22 - Consider making 22.1, 22.2, 22.3, 22.4 Required for all Low, Medium, and High Impact BES Cyber Systems because they are protecting the boundary.
39.44	Consultant	Disagree	The impact levels would be impacted by previous comments on this group of requirements.The terminology "for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest removing these words from the table where they occur.

#	Organization	Yes or No	Question 39 Comment
39.45	Southern California Edison Company	Disagree	The standard should read such that the centralized/federated primary virtualization system and its back-up are afforded protections commensurate with the impact level of the automation devices that support a particular reliability function. The standard should comply with the intent of Order 706 to prevent intentional or accidental misuse of BES components and limit BES cyber system classification to the automation nodes and virtualization nodes. End-user computing devices in a virtualization system should be classified as conduits to the virtual system that is protected by an electronic border.
39.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The time frame for requirement 2.5 would be difficult to comply with for smaller entities.
39.47	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R20 - R22 if our changes proposed in Question 37 are accepted:R20 Table 20.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.2: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.3: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.4: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.5: Low Impact: N/AMedium Impact: 48 hoursHigh Impact: 12 hoursR20 Table 20.6: Low Impact: N/AMedium Impact: N/AHigh Impact: 7 calendar daysR21 Table 21.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR21 Table 21.2: (Removed)R22 Table 22.1 - 22.4: (Removed)
39.48	MidAmerican Energy Company	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

#	Organization	Yes or No	Question 39 Comment
39.49	PacifiCorp	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters are concerned about a lack of clarity on what is expected for a baseline configuration, and if it should be applicable to an entire BES Cyber System or to individual components. Commenters also expressed a lack of understanding on how detailed inventories should be and to what category they should apply. Many comments addressed the requirements that include component-based actions for low-impact BES Cyber Systems. These are viewed as potentially overwhelming in the overall CIP compliance process. Also, identifying the physical location of a virtual component is identified in several comments as "confusing." Concerns were also identified about the definitions and clarification around terms. For example, what is meant by "Other documentation," "baseline configuration," and "virtual BES Cyber System component" were the primary terms mentioned. Also, more specific information on "security controls" was requested.

This requirement has been moved into a new standard, CIP-010-1 -- Cyber Security — Configuration Management and Vulnerability Assessments. In response to stakeholder comments, the drafting team has provided additional guidance in the 'Application Guidelines' section for the standard regarding the elements of a baseline configuration. The requirement to have an explicit inventory has been removed. This requirement is effectively inferred by the requirement to document a baseline configuration. The drafting team also agrees that maintaining an inventory for all Low Impact BES Cyber Assets within the current compliance framework in which the NERC CIP standards exist is problematic. As such, the drafting team has made an effort to prioritize controls for Low Impact BES Cyber Assets that don't require the documentation of every individual component and may be managed on a site-by-site basis, where feasible.

Several commenters suggested that inventories and monitoring should also apply to Medium and High Impact categories, since impact of the Low category to the BES Cyber System is minimal, and the effort appears to be greater than the benefit. In addition, there are questions on the timeframe and processes for monitoring. Does it need to be real time or can the Responsible Entity establish a tailored schedule for response to the detection of unauthorized changes? With regard to Requirement 23, Part 23.2, several commenters stated that it was written around typical IT equipment configurations and not the multitude of devices within generating or transmission facilities. They believe that because of this situation, the requirement should be limited to control centers similar to Requirement 23, Part 23.6. They further state that for generating facilities and substations, it would be adequate to require the entity to document and implement one or more processes for configuration change management, and that this would be applied to all Low Impact, Medium Impact, and High Impact BES Cyber Systems.

The drafting team intends for the monitoring and alerting capabilities to occur on a near real-time basis. The drafting team appreciates the concerns regarding substation and generation environments and believes that tools to perform these processes on a near real-time basis in these environments are either too immature to be included as part of a mandatory standard or simply do not exist, particularly since a large number of these cyber assets have no external communication method. Additionally, the drafting team believes that other NERC reliability standards, such as those regarding protective relay maintenance and testing, provide some level of mitigation for this lack in currently available technology.

The configuration management requirements state that an inventory must be developed of the physical or virtual BES cyber components "excluding software running on the component". Several commenters questioned why software should not be considered as constituting a "virtual" BES cyber component. Many comments were also submitted on what is perceived as a cumbersome process around inventory, monitoring, and responding to changes in the baseline configuration. They state that the criteria should be simplified, with items such as removing "physical location" from the requirement.

The drafting team has attempted to address these concerns by modifying the impact levels to which they apply. The drafting team, however, continues to believe that a rigorous configuration management program, including documented baseline configurations, is essential to an effective cyber security program.

#	Organization	Yes or No	Question 40 Comment
40.1	USACE - Omaha Anchor		23.2 - clarify "software" - is this all software on the machine or version of the OS?
40.2	US Army Corps of Engineers		Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring?
40.3	WECC		Not sure that baseline is the right word to use as many entities define baselines only at specific times in implementation projects or as part of system hardening. Item 23.5 says to "assess potentially impacted security controls" then Item 23.6 says to test them. Is this the same requirement? The second bullet in 23.6 is very difficult to read. Consider having a separate requirement for 1) Change Management Criteria, 2) Testing Criteria, 3) Test Environment Criteria.Virtualization is mentioned in 23.1. This is good, but should probably be considered in other requirements as well. In 23.2 an inventory is required of components. Based on the current definition of component,

#	Organization	Yes or No	Question 40 Comment
			this would not need to be done down to the device level; however, management at the device level is needed for effective application of change management.In 23.6 there does not appear to be a provision for changes to the baseline configuration itself. Also, the requirement for established procedures was removed. This will lead to inconsistent testing and makes auditing much more difficult.
40.4	Exelon Corporation	Agree	Exelon seeks clarification on the following questions. Do Requirements 23.2 and 23.4 include relay and SCADA equipment settings and settings changes? Would documentation of an assessment be required in a test environment before each and every relay or SCADA setting change?
40.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.There is no process to identify when any changes made to the BES might affect the actual identification of the BES component(s) as a new impact rating.FMPA does not believe that a Responsible Entity will be able to fully comply with some of these standards as they are written. For example, to fully assess how a change might impact the BES Cyber System could be interpreted to mean the RE would need a fully functional replicated copy of the production environment. FMPA does not believe this is reasonable.
40.6	Progress Energy - Nuclear Generation	Agree	R23 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
40.7	CWLP Electric Transmission, Distribution and Operations Department	Agree	R23.5. What are the ramifications to the Responsible Entity if the assessment is inaccurate and a change does adversely affect the BES Cyber System? Conducting an assessment does not guarantee success as there are always unforeseen incidents that may impact upgrades and new installations.
40.8	Xcel Energy	Agree	We believe additional guidance is requires as to what type of monitoring is expected

#	Organization	Yes or No	Question 40 Comment
			in R23.7. Is active monitoring expected, or periodic review of logs sufficient?
40.9	Dairyland Power Cooperative	Disagree	23 Note that on many SCADA systems, the simple matter of summing two telemetered values may require the modification of software/scripts. For simple calculations such as these the overhead of change control and security track will serious slow the process of making adjustments during a field checkout. Are there any further criteria that can be used to minimize the overhead on changes that are not reasonably expected to impact security posture?
40.10	FirstEnergy Corporation	Disagree	23.1 - Should also exclude data.23.2 - Cyber System Components is used two different ways in 23.1 and in 23.2. And neither uses really match the definition provided in CIP 010. What is expected for a baseline configuration for an entire BES Cyber System as opposed to a configuration for an individual component?23.3 - Change 30 days to 90 days. Remove 'other documentation as necessary' or be more specific as to what that means.23.2 - 23.4: Is the standard requiring the Responsible Entity to update the baseline documentation every time a patch is applied?
40.11	Dominion Resources Services, Inc.	Disagree	23.1 & 2 & 3(inventory only). It should be clarified that the inventory is for in-service equipment and that location refers to an area or room and not to a rack or slot. 23.4. A definition of "Authorize" should be provided.23.5. At the May workshop, an entity said they were audited by 2 regions and each region had a different definition of what cyber security controls were. On this point Dominion recommends that the word "Assess" be changed to "Define cyber security controls and assess." 23.7 Dominion is unclear how this requirement can be met. For example, an alarm is received when a relay is placed into "configure" mode, but there is no ability to see what is being changed. Stated differently, Dominion can respond to a change, but cannot monitor what is being changed. If the relay is in a remote location, Dominion's response time will be impeded. This is the best case scenario. Much equipment does not alarm when its configuration has been changed (e.g., a computer does not generate an alarm when a new program is loaded.) Dominion requests that this requirement be

#	Organization	Yes or No	Question 40 Comment
			removed.
40.12	BGE	Disagree	23.2 custom software/scripts should not be part of the baseline inventory. Recommend having 1 inventory for Low, medium and High.
40.13	American Electric Power	Disagree	23.3: Regarding "Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed", what changes must be authorized and documented? Is this targeting physical network changes or adding/deleting equipment? Is this targeting software changes?23.7: Regarding "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes", is this a continuous monitoring requirement? If not, what is the frequency that a comparison between the actual and latest approved baseline be conducted? Comparing baseline to existing configurations would be a manual process is most instances. Suggest rewording to specify that this will be conducted on the individual BES Cyber System components at some frequency, possibly quarterly.
40.14	Regulatory Compliance	Disagree	23.4 - propose adding - "Authorize and document changes that present a high risk to the BES....23.4a - additional criteria - Entity documents changes into categories of risk, based on the risk assessments determines if changes are in or out of scope.23.7 - unreasonable expectation based on the definition of baseline configuration. Instead propose the following: Do an annual review, recapturing the baseline configuration. Review for unauthorized changes during this process. If unauthorized changes are found remediate and document within 60 days of the documented annual review.
40.15	Southwest Power Pool Regional Entity	Disagree	23.5: Clarify what is meant by “deviation from the existing baseline configuration.” A new or replacement BES Cyber System Component needs to be validated before placing into service even if it uses an existing baseline configuration if for no other reason than to verify the configuration as built matches the baseline. Additionally, “potentially impacted cyber security controls” is highly subjective and open to

#	Organization	Yes or No	Question 40 Comment
			interpretation. Remove the "potentially impacted" language. 23.6: "included in the baseline configuration of the BES Cyber System" has a vendor baseline connotation. Consider clarifying to refer to the currently approved configuration of the production BES Cyber System. Additionally, the criteria need to clarify just what is meant by "baseline configuration." Does this mean the currently approved hardware and software, including versions or release levels? Or is it less granular, such as "a server running Linux and EMS/SCADA software." Without the clarification, the term is open to interpretation and the ability to audit will be affected.
40.16	MidAmerican Energy Company	Disagree	23.7 Most entities do not have the capability, resources or tools currently to live monitor configuration changes on all category A devices. There could be impacts to performance to run agents on equipment and some vendor supported devices may not allow live monitoring.
40.17	BCTC	Disagree	Â R23. Define in more explicit terms the definition of a "baseline configuration" - what comprises a baseline config - i.e. patch level, etc. R23.6. There are expected to be scenarios whereby a test environment may not exist for a high impact BES Cyber System. In such cases would a scenario like rolling out changes to a non-critical environment represent a test environment from a compliance perspective?
40.18	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls.
40.19	E.ON U.S.	Disagree	CIP-011, R23.1 The requirement states that an inventory must be developed of physical or virtual BES CSC's excluding software running on the component. What

#	Organization	Yes or No	Question 40 Comment
			constitutes a “virtual” BES CSC if not software?
40.20	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
40.21	Constellation Energy Commodities Group Inc.	Disagree	Clarify R23 to not require tracking of routine changes within the container of existing software (example, add a point or change data type of a point), but to track code migrations and changes to the baseline of deployed components.
40.22	The Empire District Electric Company	Disagree	Comments: This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.23	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy disagrees with the list of criteria in the baseline configuration. Maintenance of such a list including, software versions, active ports and services, any patches and custom software/scripts will be burdensome and subject to unintended error as the list will contain a significant number of entries. CenterPoint Energy is unsure of the value of such a list regardless of R23 assertion that it is meant “...to prevent and detect unauthorized modifications to BES Cyber Systems.” Unless such a list is reviewed on a daily basis, or perhaps even more often, there is no “detection” involved. As to “protection”, CenterPoint Energy fails to see where that would occur from the development of and maintenance of such a list. CenterPoint Energy does understand the need to maintain current configuration data, however this criteria is too prescriptive.

#	Organization	Yes or No	Question 40 Comment
40.24	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Having a hard time with the idea of documenting the physical location of the cell phone described in question 1.a, and with documenting every change in its location within 30 days of every move.
40.25	Progress Energy (non-Nuclear)	Disagree	If the BES Cyber System Component is a microprocessor relay/device, this can get complicated. These devices have numerous 'configurations' based on an application. Also, firmware versions would need to be considered. Today, most utilities lock firmware on many relay models. Another issue may be when a cyber component is returned to a manufacturer for repair - how do we verify that a replaced operating system component is compliant.R23.2 need to be explicit that the baseline is the inventory in existence at compliance time for existing systems.R23.7 in most existing generating plant systems would not be able to meet this requirement and the value is questionable since the use of administrator accounts is highly restricted by multiple other requirements.CIP-011 - R23 - Need clarification as to what constitutes a "virtual BES Cyber System Component".
40.26	Midwest ISO	Disagree	It is not clear how R23 inventories differ from those inventories that must be identified in CIP-010 R2. To the extent that these are duplicate, the duplications should be eliminated.
40.27	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
40.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R23, but recommends changes as follows: o For Parts 23.1 and 23.2, Minnesota Power recommends that Standards Drafting team define what constitutes a "Virtual BES Cyber System Component." o Regarding Part 23.2, Minnesota Power recommends that the Standards Drafting Team further define the level of software versions are required for tracking purposes. For example, an EMS has hundreds of small programs that make up the system. Each of these individual programs is combined under an

#	Organization	Yes or No	Question 40 Comment
			overall version number. In addition, different Registered Entities, with the same EMS version, may have different internal applications with different levels of fixes. To what level should those be documented? o For Parts 23.5 and 23.6, Minnesota Power recommends that the Standards Drafting Team define the term “cyber security control.” o For Part 23.6, what constitutes a “deviation?” What level of baseline is required? o Regarding Part 23.7, Minnesota Power requests that the Standards Drafting Team consider defining the term “monitor” and identify the level of detail required for these changes. For example many EMS sub-programs constantly create/modify/remove files as a normal course of business. Would these changes need to constantly be reviewed and verified?In general, Minnesota Power believes that the list of items to be tracked/tested/monitored is vague and could cause Registered Entities to incorrectly implement processes to satisfy this Requirement.
40.29	NextEra Energy Corporate Compliance	Disagree	Nextera believes there is not an agreement for the list of criteria that should be included in the baseline configuration, the requirement is a big undertaken to manage the software on BES Cyber Systems and provides little improvement to the reliability of the BES Cyber Systems.The following is the recommended updates:23.2 - Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), physical location, active ports and services, any patches, and any custom software/scripts.Keeping inventory on running software on medium and high impact BES systems will be a big undertaken. With the other levels of controls to develop baseline configurations, software should be excluded.In 23.7, this implies implementation of automated tools to detect configuration changes. Not all systems will support these tools. If not possible to automate, are manual processes acceptable? If so, wording should specify "automatic or manual detection".
40.30	LCEC	Disagree	No. The baseline configuration is not specific enough and leaves much open to interpretation.

#	Organization	Yes or No	Question 40 Comment
40.31	National Grid	Disagree	o National Grid suggests rewording 23.5 - "Assess changes to baseline configuration to verify controls are not adversely affected ..." o 23.6 - Need more information on testing requirements. o23.7 - Expand on "monitor changes". Is the SDT considering a timeline to respond to detection of any unauthorized changes o National Grid recommends the SDT to check the new EOP Backup Facility Standard for testing in 23.6
40.32	PacifiCorp	Disagree	PacifiCorp seeks clarity on 23.2 as to the 'components'. In the case of a server, is this every component in the case (including fans?) or additionally all apparatus which are directly attached (Mouse, Keyboard etc) which would not normally be included in a change record.
40.33	RRI Energy	Disagree	Part 1: does "active ports and services" refer to the network accessible ports and services as mentioned in the above requirement 17.1?Part 2: Some application uses port ranges. Netstat command only reports actively listening port(s). The requirement explicitly states "active ports and services". Some ports in the port ranges may not be active when the netstat command runs. So when the inactive ports are not in use, depending on the vendor/program, entity could be out of compliance. Active could be replaced with "Active or documented system design ports and services".What does "closely models" mean?Is a "test environment" an actual thing or a state? Example: a generation unit is online generating x MWs - no test environment "state' exists due to the unit being online; a generation unit is in a 2 week maintenance outage, all cyber assets related to the unit are in a test environment "state".
40.34	Northeast Utilities	Disagree	Please clarify 23.7. Specifically, does this monitoring need to be automated? If not, how often will the monitoring need to be performed to meet the standard?
40.35	Network & Security Technologies Inc	Disagree	R23 - Sound configuration change management practices can minimize the risk of unauthorized modifications but cannot "prevent and detect" in all instances. Suggest

#	Organization	Yes or No	Question 40 Comment
			revising the overall goal here.23.6 - Suggest adding a provision allowing a Responsible Entity to suspend this requirement under emergency conditions (e.g., to apply an emergency hot fix needed to restore a disabled or impaired BES Cyber System).23.7 - Absent the use of automated tools, this may be a very hard requirement for Responsible Entities to meet. Suggest SDT consider reasonable approaches to how it might be done on a manual basis (e.g., periodic comparisons of running configurations and stored configuration profiles) without imposing an undue burden on Responsible Entities with large numbers of High Impact systems and no current investment in automated monitoring.
40.36	Consultant	Disagree	R23. The terminology "incorporate the criteria" seems incorrect. The table is actually listing the requirements. Suggest changing to "incorporate the requirements".Table R23 - Item 23.1 The terminology "virtual BES Cyber System Components (excluding software running on the component)" seems confusing. Software would seem to be the 'virtual' component, so if software is excluded then the 'virtual' aspect seems unnecessary. Please clarify the intent of this requirement. Item 23.1 The "physical location" of a "virtual component" does not appear to make sense. Suggest rewording to specify physical location of hardware. Item 23.1 & 23.2 Qualification of "physical or virtual" components should be unnecessary. The defined term 'BES Cyber System Component' should be the basis for the requirement. Adding these qualifiers implies that the definition is not adequate. Suggest removing the qualifiers physical or virtual.Item 23.2 Suggest changing "software (including version)" "installed software versions".Item 23.2 & 23.6 The terminology "any patches, and any custom software/scripts" is vague. Suggest changing to "installed patches, and installed custom software or custom scripts".Items 23.3, 23.4, & 23.6 - Suggest changing "that deviate from the existing" to "that modify the existing".Item 23.4 - The terminology "and other documentation" is vague and subjective. Suggest deleting that phrase from this item. While "other documentation" may require an update this requirement should stay focused on configuration status.Items 23.3, 23.4, & 23.5 - The terminology shifts from 'BES Cyber System Components' used in Items 23.1 & 23.2 to 'BES Cyber System' in the last three items. If the inventory & baseline configuration is on the

#	Organization	Yes or No	Question 40 Comment
			component level then these three items should address changes on the component level to be dealing at the same level of detail. Suggest using consistent terminology in this table, either 'systems' or 'components'.Item 23.6 - Suggest deleting "each" as an unnecessary word. "For changes that modify the..." is better phrasing.Item 23.6 - Suggest deleting "software versions, active ports and services, any patches, and any custom software/scripts included in the" as unnecessary wording. The statement that the test environment closely models the baseline configuration should be adequate.Item 23.6 - Suggest punctuation or reformatting the second bullet for clarity. Possibly a separate line item: "For testing changes that modify the document: (1) the results of the testing (2) the difference between the test environment and the baseline configuration..., and (3) a description of measures used to account for the differences in operation between the test environment and the baseline configuration...."Item 23.7. This requirement statement is vague. Does it mean an inventory of hardware to monitor if any additional hardware was added, or hardware was removed? It appears to relate to some type of software status monitoring, but is not clearly stated. The terminology "respond to the detection of any unauthorized changes" is not clear and is subjective. As it is written, suggest deleting this item, or clarify the wording so it is a viable requirement.
40.37	ISO New England Inc	Disagree	r23.2 - custom software/scripts? Maybe better language is those custom software scripts that are required for the function of the BES cyber system component would be more appropriate. Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see answer to question 41)R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.As written, 23.5 is confusing. Suggest using “Assess changes to baseline configuration to verify controls are not adversely affected

#	Organization	Yes or No	Question 40 Comment
			..."Recommend the SDT check the new EOP Backup Facility Standard for testing in 23.6R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?
40.38	Independent Electricity System Operator	Disagree	R23.2 - what is meant by "software". Is this requiring that the version of Notepad, Wordpad, WinZip be recorded or only software that is needed to operate the component?- R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?- - R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.- - R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?- R23.3: replace "existing inventory" with "existing baseline" since above the baseline configuration was defined to include an inventory...; replace "update the inventory" with "update the baseline"- R23.3: what is "other documentation"- R23.3: is 30 days calendar days or business days?- Not clear on the difference between 23.3 and 23.4- R23.5: define "cyber security controls"- R23.6: could the statement "test the changes to the BES Cyber System in a test environment..." be changed to replace the second "test" with another word-what if it is tested in an environment that is not "test" but meets the requirements as stated?
40.39	Ameren	Disagree	R23.3 - Does change only constitute replacing hardware as inventory and replacement of software is not a requirement for low systems? Need to clarify requirement.R23.4 - This requirement will be challenging to audit as there is no clear lower threshold for

#	Organization	Yes or No	Question 40 Comment
			changes to the baseline configuration. Suggest adding the term significant changes.R23.7 - Is this requiring the installation of additional software to perform this function? Some systems may not allow the addition of this type of software, this requirement will likely end up needing a TFE.
40.40	Allegheny Energy Supply	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.41	Allegheny Power	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.42	EEI	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high

#	Organization	Yes or No	Question 40 Comment
			impact cyber systems.
40.43	Constellation Power Source Generation	Disagree	R23.7 describes monitoring, but not how the monitoring should be implemented (automated, manual, etc). What is the timeline to respond to the detection of unauthorized changes? Yearly? Daily? Continuously? A suggestion would be a yearly manual monitoring system.
40.44	Hydro One	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to "Assess changes to baseline configuration to verify controls are not adversely affected ..."Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.Please explain the rational to limit 23.6 to Control Centers only.
40.45	Northeast Power Coordinating Council	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to "Assess changes to baseline configuration to verify controls are not adversely affected ..."Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.
40.46	Garland Power and Light	Disagree	Requirement 23.2 23.4, 23.6 and 23.7 - should not apply to database changes or display changes
40.47	Alliant Energy	Disagree	Requirement 23.7 forces entities to implement discovery tools where they may not already exist into environments that may incur negative impact from the very nature of these discovery mechanisms. Where the operational risk of discovery tool deployment precludes its introduction, this requirement would necessitate manual processes. These manual processes would tax the operational resources normally dedicated to increasing the reliability of the BES.
40.48	Public Service Enterprise	Disagree	Requirement 23.7 may not be technically feasible for certain types of BES Cyber

#	Organization	Yes or No	Question 40 Comment
	Group companies		System Components such as older generation or legacy Remote Terminal Unit (RTU) products. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase “where technically feasible”.
40.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets? SDG&E also requests an example of a virtual BES Cyber System Component (excluding software running on the component).
40.50	Duke Energy	Disagree	Some software on a BES Cyber system may not be relevant to the system (ex. Microsoft calculator or other bundled software) we don’t want to include a version of that. Suggest removing software since the software itself may be the BES cyber systemRequirements 23.3, 23.4, 23.5 - authorization should be able to be made more than 30 days BEFORE the installation.Requirements 23.3, 23.4: documentation via "red-marked" drawings ("interim as built") should satisfy this requirement. Is that the case?Requirement 23.5: as written, it allows the assessment to occur AFTER the fact. Should this not occur BEFORE the change is made?Requirement 23.6: with the proposed definition, it is open for interpretation how closely test environment should model the production environment.Requirement 23.7: what is the expectation for implementing this control? Manual? Automatic? Suggest removing. We are unaware of any device capable of doing this.
40.51	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments to require the current drafted language of R23 Table 23.1 - 23.7 for Control Centers Only. We also offer the following recommendation to cover a Configuration Change Management process for the rest of the facilities:R23 Table 23.8 (NEW): Develop one or more processes for

#	Organization	Yes or No	Question 40 Comment
			configuration change management for BES Cyber System Components in generation and transmission facilities.R23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR23. Objective:To prevent and detect unauthorized modifications to BES Cyber Systems. R23. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management.
40.52	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent and detect unauthorized modifications to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition, Section 23.7 of Table R23 has issues.It is not clear what is meant by "monitor changes...." If this implies some form or ongoing or periodic "monitoring" consider the following:Depending upon the definition of "change" and because of the nature of devices located at substations and other BES equipment, any form of ongoing check or monitoring would be extremely difficult. Because there is the potential for each device to have specific configurations and settings depending up the conditions of the circuit it might be connected to, this would mean that each piece of equipment would have to be manually connected to and checked on a periodic basis. These are industrial controls that are not normally connected to unless service is required for some reason. The definition of a change should not include day to day work processes that are performed to keep the lights on such as settings changes, resetting relays, AV signature updates, or other services and settings kinds of activities. Nor should it necessarily include data changes that do not affect the executable code or configuration of the system. We would expect to be able to define what a change is within our environment.Recommendation: Delete 23.7. Modify R23 to read:Objective 23 - To prevent and detect unauthorized modifications to BES Cyber Systems.R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management. Such processes shall include an Entity-specific

#	Organization	Yes or No	Question 40 Comment
			definition of what constitutes a system change.
40.53	US Bureau of Reclamation	Disagree	The table requires additional clarification, particularly for different sorts of devices (relays, etc.)
40.54	Con Edison of New York	Disagree	These systems are constantly be upgraded all year long with little impact on any security. The need to do this within 30 days is excessive and should be limited to an annual review.
40.55	MRO's NERC Standards Review Subcommittee	Disagree	This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.56	Western Area Power Administration	Disagree	This requires a near-identical test system and makes no adjustments for risk analysis, and does not allow testing on failover devices (maybe) as it says "test environment" specifically. Is that truly the intent?
40.57	We Energies	Disagree	We Energies agrees with EEI: R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.We Energies agrees with EEI: R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.

#	Organization	Yes or No	Question 40 Comment
40.58	Manitoba Hydro	Disagree	We support the baseline approach to change management. It is unclear as to what "other documentation" in Requirements R23.3 and R23.4 is being referenced.
40.59	Emerson Process Management	Disagree	What is the significance of excluding software from the inventory requirement in 23.1 for low-impact BES Cyber System? Cyber security is mostly related to software than hardware. This exclusion does not give any value to the low impact systems.

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Configuration Change Management" is now addressed in CIP–010–1 — Cyber Security — Configuration Change Management

Commenters raised concerns about requirements that include component level actions for Low Impact BES Cyber Systems, such as inventories and development and maintenance of documentation. Commenters believed that the effort needed to implement those actions will detract from other, more critical actions on Medium and High Impact BES Cyber Systems and Components. Some recommendations are to remove Low Impact BES Cyber Systems from all Requirement R23 controls. In addition, because inventories are required in R23.1-2 for Low Impact components, commenters recommend that these should be limited to devices that have an external accessible connection with a potential direct impact on BES reliability. The drafting team appreciates the concern regarding the level of effort necessary for compliance on Low Impact assets. As such, the drafting team has attempted to implement a framework where the controls for Low Impact assets are those that can be implemented at a higher level of abstraction (such as on a site-by-site basis versus a component level basis) or are primarily programmatic or organizational in nature.

Commenters recommended that monitoring changes to the baseline configuration and responding to the detection of any unauthorized changes be limited to control centers only. The commenters submit that although the requirement may be appropriate for certain types of assets, the technology required to monitor many devices in generation and transmission facilities does not exist. As indicated in its response to Question 40, the drafting team appreciates these concerns and has modified the applicability for configuration monitoring to High Impact control centers.

Commenters noted that Requirement R23.2 adds a requirement for a detailed level of inventory including software versions. Commenters were not clear on the granularity required of this inventory. In addition they question how custom code is tracked for systems such as EMS and scripts that are routinely developed to streamline operational functions. In response, the specific language of the requirement regarding the necessary elements in a baseline configuration has been updated by the drafting team with the intent to provide additional clarity. (See Requirement R1, Part 1.1 in CIP-010-5)

Comments were submitted that recommend one inventory be required to cover all Low, Medium and High Impact BES Cyber Systems. It was also suggested that in Requirement R23.6, the requirements identified for Control Centers should only be extended to High Impact BES Cyber Systems as well as Control Centers. In response, the drafting team has adjusted the impact levels of the items that require an inventory to more suitably focus the effort of the Responsible Entity on items that are not as documentation-centric. None of the requirements in proposed CIP-010-5 apply to Low Impact BES Cyber Systems.

Regarding the testing of changes, commenters recommended testing of all High and Medium Impact BES Cyber Systems, not just those in Control Centers. They also recommended, however, that developing a test environment that models the production environment and documents differences should be applied only to High Impact BES Cyber Systems in Control Centers. In response, the drafting team has modified the standard to require testing of security controls for both High and Medium Impact BES Cyber Systems, but only requires testing in a test environment for those High Impact BES Cyber Systems in Control Centers. (See Requirement R3, Part 3.2 in the proposed CIP-010-5).

#	Organization	Yes or No	Question 41 Comment
41.1	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
41.2	Reliability & Compliance Group	Agree	You need to provide a definition of a virtual BES cyber system component.
41.3	LCEC	Disagree	23 What level does the software inventory include? Driver versions? What about devices with embedded OSes? Needs to include functionality testing.Is the requirement in 23.6 for control center only in reference to the cyber system components?
41.4	Black Hills Corporation	Disagree	23.5 should apply to Medium impact BES cyber systems.
41.5	ERCOT ISO	Disagree	23.5-23.7: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
41.6	Regulatory Compliance	Disagree	23.7 - High Impact - "required for Control Center only"
41.7	US Bureau of Reclamation	Disagree	All impact levels should have some minimum level of requirement established.
41.8	Southwest Power Pool Regional Entity	Disagree	Although the language will work as written, it could be improved by separating the component inventory requirement defined in 23.1 from the more comprehensive

#	Organization	Yes or No	Question 41 Comment
			requirements in 23.2, making 23.1 applicable to all impact categories. Similar improvement is possible with 23.3 and 23.4. 23.6: Testing prior to implementation should apply to Medium category systems.
41.9	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls. R23.1-2 requires an inventory of all Low Impact components, this is an intensive work load addition for the Low category components. Components as identified in the definition include all programmable devices. This includes most instrumentation in a generation unit. This should be limited to devices which have an external accessible connection with a potential direct impact on BES reliability.
41.10	WECC	Disagree	Change management and testing should be done for all medium and high impact level BES Cyber System Components not just control center or high.Criteria should apply to all impact levels.
41.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
41.12	The Empire District Electric Company	Disagree	Comments: See comments under question 40.
41.13	US Army Corps of Engineers, Omaha Distirc	Disagree	Define "changes" as used in 23.4. Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring? If automated monitoring is required this could result in numerous TFE's for other than general processing equipment.

#	Organization	Yes or No	Question 41 Comment
41.14	Alberta Electric System Operator	Disagree	In 23.5 and 23.7, consider setting Medium Impact both to Required
41.15	Entergy	Disagree	Inventory and component baseline configuration management are basic care and feeding requirements generally accepted as best practice - 'systems management 101'; and should therefore apply for intelligent infrastructure employed throughout a control system. It is also clear from Order 706 that this is what FERC intends.
41.16	Consultant	Disagree	Item 23.6 - Stating that this is required for Control Centers only adds an additional dimension to the impact categorization. The impact categorization criteria should clearly identify the assets that go into a particular impact classification. The table should only state whether the requirement is required for that classification or not, it should not add an additional classification criteria.
41.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
41.18	Oncor Electric Delivery LLC	Disagree	Need an inventory for Medium and High systems(R23.1) and should document changes for Medium and High systems(R23.3) Requirement R23.7 should allow for manual processes to detect changes. It is also unclear how an entity would document a phased implementation - is it based on "in-service" designation?
41.19	Con Edison of New York	Disagree	o R23 changes and adds to Change Management Configuration requirements. This requirement mentions the need for an inventory of BES cyber components. This is not mentioned in CIP-010 o R23.2 This requirement adds a much more detailed level of inventory including software versions. This would be an extensive task, and does this require an inventory of all, such as any Microsoft Office on the workstations, non- MS app's etc? Shouldn't this be limited to knowing the release level you are on, without the line-by-line level information? How do you handle custom code for custom systems such as EMS?How do you manage scripts, they can be written to pull information from the database as shorthand; would that count? These are routinely

#	Organization	Yes or No	Question 41 Comment
			written by staff to get something quickly, and to address repetitive solutions/commands.
41.20	American Municipal Power	Disagree	Please provide a little or no impact category
41.21	Madison Gas and Electric Company	Disagree	R23.1 states: Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.The BES Cyber System Component definition states: One or more programmable electronic devices (including hardware, software and data).... This requirement excludes software, but what about data?
41.22	BGE	Disagree	Recommend having 1 inventory for Low, medium and High.
41.23	Hydro One	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.24	ISO New England Inc	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber SystemsRecommend 23.6 High Impact BES Cyber Systems should not be Requireed for Control Center Only
41.25	Northeast Power Coordinating Council	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.26	National Grid	Disagree	Refer to comments in Q. 40.
41.27	San Diego Gas and Electric	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that

#	Organization	Yes or No	Question 41 Comment
	Co.		fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets?
41.28	American Electric Power	Disagree	See comments under question 40.
41.29	MRO's NERC Standards Review Subcommittee	Disagree	See comments under question 40.
41.30	Southern California Edison Company	Disagree	Should be unilateral across all levels.
41.31	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 23.5, 23.6, and 23.7.
41.32	Network & Security Technologies Inc	Disagree	Suggest requiring changes be tested for all High and Medium Impact Cyber Systems. Requirements to use a test environment that models production environment and to document differences could be applied only to High Impact systems in Control Centers.
41.33	Midwest ISO	Disagree	The requirement to document changes to the inventories in R23 is 30 days. The requirement to update inventories CIP-010 R2 is 45 days per CIP-010 R2. These should be consistent and we recommend it should be 60 days per our response in Q5.
41.34	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R23 if our changes proposed in Question 40 are accepted:R23 Table 23.1: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers OnlyR23 Table 23.3: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.4: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers

#	Organization	Yes or No	Question 41 Comment
			OnlyR23 Table 23.5: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.6: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.7: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: Required
41.35	GTC & GSOC	Disagree	We recommend that R23.7 be applicable for control centers only. This requirement is more appropriate for control centers and not for transmission and generations operations. While this requirement may be feasible for certain types of protective relays, this technology generally does not exist for a wide range of devices including certain RTUs and meters. In fact, some RTU's must be taken offline in order to retrieve their configuration. Thus, compliance with this requirement would have a negative reliability benefit.
41.36	Progress Energy (non-Nuclear)	Disagree	We see 23.5 as documented lab and field testing for any change to an existing relay/gateway/etc. configuration. Is this what was intended?Baseline configuration is not clear - does this start with the implementation date of the standard or the original production of the facility/element.Virtual BES is not clear. Please specify intention.

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "sensitive information" that was originally posted as an informal definition adjacent to Requirement R24 in the draft CIP-011-1 was:

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

The primary issue identified with sensitive information was the term itself. Many commenters indicated that this term is already being used by organizations for other purposes, and its inclusion in the NERC CIP standards will cause much confusion. There were several suggestions of alternative terms to use including "CIP-sensitive information" and "protected information." In response to these comments, the drafting team has changed the term to "BES Cyber System Information." The commenters also included numerous suggestions for the improvement of the definition. One commenter indicated that this was not really a definition at all, but rather a list of examples. The drafting team did recognize this as a list of examples, and as such removed it from the requirement language and included the suggestions in the definition of the term BES Cyber System Information.

Several commenters indicated that "floor plans of computing centers" should be removed from the definition. The drafting team agrees that floor plans are problematic as they often are required to be submitted as part of work permits or other items. As such, the drafting team has clarified that only those floor plans that include impact designations of BES Cyber Systems should be identified as BES Cyber System Information, since it is the aggregate data that rises to the level of required protections and not just floor plans alone. This modification was also made to other elements of the definition such as equipment layouts.

A few commenters suggested that the scope of the definition was not broad enough and should be modified by saying "includes but not limited to" or changed entirely to include all data that affects the confidentiality, integrity, and availability of the BES. The drafting team appreciates this suggestion, but sees difficulty in the ability to measure such a broadly scoped definition. Additionally, the drafting team wanted to base the definition on the elements previously defined in CIP-003-3 R4.1 to leverage the investment that Responsible Entities have already made in their existing NERC CIP Information Protection Programs.

The proposed definition of "**BES Cyber System Information**" is:

"Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans."

#	Organization	Yes or No	Question 42 Comment
42.1	Florida Municipal Power Agency	Agree	24.4 - How can a RE "revoke access" from data which may have been copied by personnel?
42.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
42.3	CWLP Electric Transmission, Distribution and Operations Department	Agree	Does network topology or similar diagrams include in-house wiring or plant wiring that may include fiber and Ethernet facilities?
42.4	Exelon Corporation	Agree	Exelon seeks clarification on the following question. Is it the intention of the Standard Drafting Team to include blueprints (schematics and one lines diagrams) for relay and SCADA components in the definition of sensitive information? And, to the extent that such information described large generation facilities or combinations of facilities greater than 2000 MW, then would the electronic record system be considered a High BES Cyber System?
42.5	USACE - Omaha Anchor	Agree	Question - it's difficult to electronically distribute controlled information - however the incident response plan and the recovery plan are supposed to be easily available to all folks. Seems a bit of an oxymoron.

#	Organization	Yes or No	Question 42 Comment
42.6	Northeast Utilities	Agree	The prior version had a concern with user lists, logon-ids, etc. Was applicability to that type of information intentional removed? Also, please clarify whether a recipient of CIP sensitive information must be CIP cleared (PRA & trained).
42.7	Consultant	Disagree	"...network topology or similar diagrams..." should be modified to "network topology that includes BES Cyber Systems" Corporate network topology should not be included in the standards, but this wording would include such diagrams."...floor plans of computing centers that contain BES Cyber Systems..." should be removed, or clarified to specify "floor plans that indicate locations of BES Cbyer Systems". Building floor plans exist in many places that are beyond the control of the Responsible Entities, e.g. architects, landlords, building maintenance companies. A better option might be rewording to qualify the entire list of items as applying to BES Cyber Systems. "... includes (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition should be written as a definition, i.e. Sensitive Information - (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition is NOT 'For the purposes of this standard', it is expected to be included in the next Glossary update after approval of the standard, and the defined term is hidden somewhere in the statement.
42.8	Luminant	Disagree	"floor plans of computing centers that contain BES Cyber Systems" should be changed to "floor plans that specifically identify BES Cyber Systems or their locations". " BES Cyber System disaster recovery plans" should be “BES Cyber System recovery plans"
42.9	Tenaska	Disagree	24.1 should say: Identify sensitive information.24.2 should say: implement procedures protect sensitive information25.1 should say: render sensitive information unusable

#	Organization	Yes or No	Question 42 Comment
			when disposing of documents and equipment that may contain that information.
42.10	Alliant Energy	Disagree	Alliant Energy agrees with EEI on all points and timeframe consistency. Table 24 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
42.11	Dairyland Power Cooperative	Disagree	BES systems actually contain information/data about the BES that is sensitive as well, but are ignored. Definitions for SCADA, electrical network topology, schematics, and other information can also be BES information related to critical infrastructure that requires protection.
42.12	E.ON U.S.	Disagree	CIP-011, R24 The definition of sensitive information should provide examples of what constitutes a “security operational procedure.”
42.13	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes the Responsible Entity should identify and classify data as sensitive information and therefore the definition is too restrictive. CenterPoint Energy recommends it be revised as follows: For the purpose of this standard, sensitive information includes but is not limited to, security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and

#	Organization	Yes or No	Question 42 Comment
			security configuration information.
42.14	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing “contain” to “identify” and adding the phrase “that specifically identify Medium or High Impact components” after the phrase “equipment layout of BES Cyber Systems.” This modification is reflected in the revised definition below: For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that identify BES Cyber Systems, equipment layouts of BES Cyber Systems that specifically identify Medium or High Impact components, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.
42.15	Bonneville Power Administration	Disagree	FERC, NERC and the Regional Entities do not have the information necessary to determine what information is sensitive or not as it regards any Responsible Entity. This is conditional and depends on more that just the types of information involved. The determination of what is sensitive information, and what is not can only be done by the Responsible Entity and under the laws and regulations they must comply with. Floor Plans, network diagrams, equipment layouts and other information may or may not be sensitive depending upon what additional information is provided with it. In addition, legal contracts, Federal, state and municipal laws, regulations, and fiduciary requirements may also govern what information may be protected and what must be released.Recommended Change - For the purpose of this standard, sensitive information may include security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information as determined by the Responsible Entity.
42.16	NextEra Energy Corporate Compliance	Disagree	In R24, is it a requirement to map every user's access privileges to sensitive information?In R24, for every new document that contain security operational procedures, network topology or similar diagrams, floor plans of computing centers

#	Organization	Yes or No	Question 42 Comment
			that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information, do we need to record the explicit authorization of every personnel that has access privileges for each type of documents?In 24.2, does this mean that the handling procedures for hard copies of sensitive information include a documentation for chain-of-custody for High Impact BES Cyber Systems?
42.17	Regulatory Compliance	Disagree	Incident Response plans and Diaster and Recovery plans should not be included as sensitive information - these plans should be psuedo public as long as they have written without security configuration information in them.
42.18	Progress Energy (non-Nuclear)	Disagree	It is not clear if this includes relay device information such as electrical diagrams/schematics.Incident response plans typically do not contain any system specific information. The plans provide the actions that must be taken and must be freely available to many. Will that approach meet the intention of the new standard?
42.19	MidAmerican Energy Company	Disagree	Many entities including MEC use "Sensitive" information as one of the classifications for information that needs to be protected. Calling all information to be protected sensitive will cause confusion. Change the term "sensitive information" to "protected information" in CIP-011.
42.20	Con Edison of New York	Disagree	o R24.3 does the word explicitly mean we cannot say all EMS staff has access to information? Does it need to be by name?
42.21	Network & Security Technologies Inc	Disagree	R24 and/or its sub-requirements should be modified to make it clear they apply sensitive information regardless of media type (including paper copies).24.4 - Revocation of access can be hard to do, and even harder to verify, in cases where an individual has taken either electronic or paper copies of sensitive documents off the Responsible Entity premises (sometime for legitimate reasons). Suggest revising this requirement in a manner that acknowledges this reality - something like “best effort” to retrieve sensitive information the individual may have in his or her possession,

#	Organization	Yes or No	Question 42 Comment
			accompanied by warnings that subsequent unauthorized disclosure of any such information may result in prosecution.
42.22	Hydro One	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.23	ISO New England Inc	Disagree	Recommend that the definition change “includes” to “includes but not limited to”
42.24	Northeast Power Coordinating Council	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.25	US Army Corps of Engineers, Omaha Distirc	Disagree	Remove "floor plans of computing centers"
42.26	Allegheny Energy Supply	Disagree	Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram “similar” (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security

#	Organization	Yes or No	Question 42 Comment
			configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.27	LCEC	Disagree	Sensitive is a classification that is specific to the CIP standards per this definition but is used in organizations as one of the levels of information classification. To differentiate, the term BES Sensitive might be considered.
42.28	Public Service Enterprise Group companies	Disagree	Sensitive should be changed to “protected Information”, the definition is fine.
42.29	Progress Energy - Nuclear Generation	Disagree	Sensitivity levels for information are established for nuclear generation facilities by CFR. This definition should be adjusted to acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
42.30	Southwest Power Pool Regional Entity	Disagree	Should include more than “security” operational procedures. IT-specific operating procedures (“run books”) are very sensitive and could be used to exploit a system. Operations procedures may also be sensitive to some extent if they describe the use of the BES Cyber System.
42.31	San Diego Gas and Electric Co.	Disagree	The "definition" is only a list of examples, not a real definition. SDG&E suggests the following definition: "Sensitive information is defined as any information owned by

#	Organization	Yes or No	Question 42 Comment
			the Responsible Entity, or for which the Responsible Entity is the custodian of, that, if inappropriately disclosed, modified, or rendered unavailable, could adversely impact human safety or the reliability of the BES. Examples include...(their list)"
42.32	APPA Task Force	Disagree	The APPA Task Force would like to comment on the definition of sensitive information: As pointed out in Question 44, the following disclaimer needs to be added to that definition: "To the extent that state/local laws allow"
42.33	Entergy	Disagree	The definition of sensitive information is nearly identical to the one currently being used in version 3. R24.1 and R24.2 explicity allow the Entity to classify and protect "sensitive" information under its own auspice. As long as the classification guidelines are left for the Entity to decide, this definition should prove sufficient.The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Please define "Explicitly Authorize"? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? Is approval documentation all that's required, or is a maintained list required as well?
42.34	Manitoba Hydro	Disagree	The definition should also reference control rooms.
42.35	Southern California Edison Company	Disagree	The definition should clearly distinguish BES operational information and cyber security related information. A smaller subset of the former and larger subset of the latter form potential candidates for "protected information".
42.36	Oncor Electric Delivery LLC	Disagree	The definition should not prescribe items as being "sensitive". The identification and classification process of Requirement 24.1 should do that. "For the purpose of this standard, sensitive information includes procedures, diagrams and any other document which provides proprietary information about BES Cyber Systems or BES

#	Organization	Yes or No	Question 42 Comment
			Cyber System Components."
42.37	Allegheny Power	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.38	EEI	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.39	ReymannGroup, Inc.	Disagree	This definition should be expanded to include the identification and classification of ALL data that affects the confidentiality, integrity, and availability (CIA) of the BES system commensurate with its sensitivity and consequence.
42.40	US Bureau of Reclamation	Disagree	This effort needs to be aligned with the Executive level CUI requirements.
42.41	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
42.42	We Energies	Disagree	We Energies agrees with EEI: There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.We Energies agrees with EEI: Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.We Energies agrees with EEI: The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. We Energies agrees with EEI: A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely

#	Organization	Yes or No	Question 42 Comment
			available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.We Energies agrees with EEI: The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. We Energies agrees with EEI: For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.43	American Transmission Company	Disagree	We propose deleting “floor plans of computer centers” from the definition of sensitive information. Floor plans do not typically include information specific to devices, IP addresses, etc which could be used to compromise a BES Cyber System. Moreover, a computer center is an undefined term which could mean anywhere there was more than one computer.
42.44	LADWP	Disagree	Word sensitive needs to be changed as it can coincide with actual classification used by entities.
42.45	FirstEnergy Corporation	Disagree	Would like to see the definition even more narrow, to focus on information that truly can compromise the BES (e.g. Vulnerability assessments’, mitigation strategies, passwords, and DR plans).

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "media" that was originally posted as an informal definition adjacent to Requirement R25 in draft CIP-011-1 was:

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

The proposed definition of "media" received significant agreement from those entities that chose to respond to this question. The majority of comments on the definition of media indicated that the definition should be expanded to include additional storage types as well as more traditional media types such as paper. The drafting team intends for Responsible Entities to protect media, such as paper, through the required handling procedures included in the Information Protection requirement.

One commenter indicated that USB drives, CDs, and floppy disks should be included in the definition of media. It was the intent of the drafting team that these device types would be considered devices used to perform maintenance and thus treated in accordance with the maintenance requirements. As the maintenance requirements evolved with the inclusion of additional remote access requirements, the drafting team considered expanding the scope of the media definition.

Another commenter made an interesting case regarding the media being "within" a BES Cyber System and suggested that once the media was removed that it no longer met the definition. The drafting team considered this comment and has modified the standard to require sanitization of BES Cyber System Information contained on media. The remaining comments focused primarily on the requirements themselves and not the definition. Specifically, commenters were concerned about the level of sanitization that would be required on the media. Several commenters noted that the level of sanitization should be commensurate with the potential threat to BES reliability, while others suggested that there be a defined minimum acceptable sanitization process, such as an NSA standard. The drafting team understands the need for a minimum acceptable sanitization process. However, the NERC Standards Development Process does not allow the drafting team to simply reference another standard. As such, we have modified the language in the revised standard to require that media be destroyed or other actions taken to prevent unauthorized retrieval.

Given the potential confusion with establishing a NERC Glossary definition for media, the drafting team has elected to define the term within the language of the standard itself.

#	Organization	Yes or No	Question 43 Comment
43.1	Florida Municipal Power Agency		How would one define the process used to render the media unrecoverable? What does unrecoverable mean? Unrecoverable by NSA standards or unrecoverable by means of something like phase transition?
43.2	Black Hills Corporation	Agree	Believe that solid-state mass-storage (flash drives, thumb drives, jump drives, etc,) should be included as examples in the definition.
43.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
43.4	Northeast Utilities	Agree	Suggest that a minimum acceptable sanitization process (i.e., NIST standard) is specified.
43.5	APPA Task Force	Agree	The APPA Task Force agrees with the definition.
43.6	Dairyland Power Cooperative	Agree	With the proliferation of flash memory solutions, the only way to sanitize some media is physical destruction. Many devices use flash memory in a way that is not removable. Is destruction of this equipment intended?
43.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
43.8	FirstEnergy Corporation	Disagree	Believe the definition should not include example because of the quickly changing storage technologies.
43.9	Xcel Energy	Disagree	Further clarification, similar to the definition of Maintenance in R26, is needed to make it clear that media such as hard drives on laptops used for maintenance do not need to be sanitized after temporary connection to BES Cyber Systems.

#	Organization	Yes or No	Question 43 Comment
43.10	LADWP	Disagree	Is portable storage included here?
43.11	Emerson Process Management	Disagree	It should include USB memory stick which is becoming very popular.
43.12	LCEC	Disagree	Media can be removed from the BES Cyber System and it should still be considered media per this requirement. Remove the word "within" and replace with "used by" or "written to by" a BES Cyber System.
43.13	Public Service Enterprise Group companies	Disagree	Media should also include persistent configuration data that is stored in solid state devices (e.g. flash memory, EEPROM (electrically-erasable programmable read-only memory), etc.)
43.14	Southwest Power Pool Regional Entity	Disagree	Portable media, including CD/DVD and USB devices should be included. Basically, anything that sensitive information can be written to.
43.15	Reliability & Compliance Group	Disagree	Recommend removing the word “mass” and instead use the term storage devices.
43.16	USACE - Omaha Anchor	Disagree	Sanitization should only apply to media internal to the devices.
43.17	San Diego Gas and Electric Co.	Disagree	SDG&E notes that the proposed definition does not appear to include "old school" media like paper that is often used to store sensitive information.
43.18	ERCOT ISO	Disagree	Should also specifically address CDs and USB storage devices in the definition.
43.19	Progress Energy (non-Nuclear)	Disagree	Should the definition also clearly state device hard drives?
43.20	Manitoba Hydro	Disagree	The current definition would also require the sanitization of other mass storage devices, such as flash memory, which could render the cyber component unfit for

#	Organization	Yes or No	Question 43 Comment
			reuse outside of the BES Cyber System. The strict sanitization requirement does not permit the return of a failed BES Cyber System or BES Cyber System Component to the vendor for failure analysis. The information protection requirements must provide more flexibility, which may also be achieved through processes and procedures.
43.21	ReliabilityFirst Staff	Disagree	The definition does not need to specify “mass storage devices” and, in fact, should include devices such as flash drives. Media should also be defined to include media types other than electronic such as paper.
43.22	Consultant	Disagree	The definition is technology limited by magnetic and optical technologies. While pervasive, there are and will be other technologies to retain information.Suggest: Media - computer components and recording media that retain digital data used for computing for some interval of time.Might also consider making the definition "Electronic Media" to eliminate books, notebooks, paper, etc. which are also 'information storage media'.
43.23	Entergy	Disagree	The definition of "media" includes the open-ended term "including, but not limited to", which could practically bring anything into scope. A more concise definition with specific examples would remove ambiguity and leave less room for interpretation. The examples of Media in the box should also include flash memory as well.An example of the type of sanitization required should be provided.
43.24	Alberta Electric System Operator	Disagree	The definition states “including, but not limited to,”. The AESO suggests modifiying the definition to explicitly include non-volatile storage to ensure coverage of memory cards and flash drives.
43.25	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
43.26	We Energies	Disagree	We Energies agrees with EEI: When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of

#	Organization	Yes or No	Question 43 Comment
			voltage or frequency does not pose a risk to the BES.
43.27	Allegheny Energy Supply	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperatures does not pose a risk to the BES.
43.28	Allegheny Power	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
43.29	EEI	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns regarding the requirement for information protection centered around the revocation timeline and scope as well as differentiating access to information vs. access to systems. The drafting team is attempting to address the FERC directive that requires the revocation of access to BES Cyber System Information. The drafting team is proposing to address revocation of access to BES Cyber Systems and to BES Cyber System Information all in one place to ensure more consistency in the requirements and their implementation.

There were a number of commenters who raised concerns with the requirement for media sanitization regarding media failure conditions or disposal. The word "sanitization" appeared to cause confusion for a number of commenters and as such has been removed from the revised standard. Additionally, a couple of commenters raised concerns about the burden of proof, compliance requirements, legal issues, and ownership responsibilities.

As with other areas of this standard, there were a significant number of the comments asking for clarity of phraseology and terminology, including words such as consequence, annually, explicitly, acceptable, commensurate, etc. The drafting team eliminated the words, "explicitly, acceptable, commensurate, and annual" from the revised CIP-011-1 standard.

#	Organization	Yes or No	Question 44 Comment
44.1	ISO New England Inc		Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for causeWhat about revoking access for other than cause?Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems"
44.2	Northeast Utilities	Agree	Agree that this requirement covers the key cyber assets but how does this apply to

#	Organization	Yes or No	Question 44 Comment
			protective systems such as the physical access system, firewalls and logging devices?
44.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
44.4	Black Hills Corporation	Agree	Legally Required Release: There may be "legal" situations in which we may be required to share certain information with outside entities, both government and non-government. Examples could include OSHA or MSHA investigations, employee lawsuits (with the associated discovery). There does not appear to be any provision in the regulation to allow this sharing. We could be placed in the position of violating this regulation, or violating some other legal requirement (subpoena, etc)
44.5	Puget Sound Energy	Agree	Puget Sound Energy suggests modifying R24.4 to "Revoke access to media containing sensitive information within 24 hours..." to align with the NERC definition in R25 and to provide clarity around sensitive information in a hardcopy format.
44.6	GTC & GSOC	Agree	We recommend the verbiage and timelines for R24.4 be consistent with tables R5 and R13.
44.7	Independent Electricity System Operator	Disagree	- R24.4 define for cause. Should the wording be involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R24.4 how do you remove access where personnel may have physical copies offsite o
44.8	ERCOT ISO	Disagree	24.2: Recommend: "Implement labeling and handling procedures for sensitive information according to its defined classification level." 24.3: It is unclear whether the requirement includes internal and external personnel. 24.4: Should be combined with other access management requirements (physical, cyber)24.5: Should also address "need to know". The requirement did not address the access control means for protecting information or the access to hard copies of information.
44.9	Duke Energy	Disagree	24.3 - We don't feel it is realistic to explicitly authorize access to paper copies of

#	Organization	Yes or No	Question 44 Comment
			information. Add 'repositories' at the end of the sentence.Include "repository" in 24.4 and 24.5 as well. Requirement 24.3 is particularly burdensome in a nuclear environment where there is already heavy physical security. There are thousands of drawings, for example, available for the plant. There are hundreds of personnel that have a business need to know certain things about the plant that are contained in these drawings. During outages that number often goes above 1000 personnel. Segregating all drawings/manuals/equipment layouts/floor plans/procedures and EXPLICITLY authorizing personnel for access is difficult at best. Certainly, protecting cyber specific information such as firewall rules, group policies, passwords, and other specific cyber information makes sense and is done already.
44.10	Regulatory Compliance	Disagree	24.4 - Strike altogether. Revocation should go back and be included in the scope of System revocation.25.1 - Propose : Sanitize only media containing sensitive information prior to disposal for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.
44.11	Southwest Power Pool Regional Entity	Disagree	24.4: Is this requirement prescribing Information Rights Management? There are many types of access, including access to information no longer under the direct control of the entity. 24.5 is poorly worded. Would be better to require that access is authorized, not that it reflects authorization. 25.1 should require either sanitization or physical destruction.
44.12	American Electric Power	Disagree	25.1: Regarding "Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable", what evidence would be required from an audit perspective? If a USB harddrive is used to copy patches onto a system, would that USB harddrive need to be destroyed with documented evidence if it failed 2 weeks down the road?Suggested rewording:Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which sensitive information is recorded and stored.Rational: Adding sensitive to the "Media" definition will clarify that this is intended to be used

#	Organization	Yes or No	Question 44 Comment
			to protect the inadvertent distribution of protected information, not all media devices that are plugged into a BES Cyber System will need to be sanitized.
44.13	BCTC	Disagree	Â R24.4. We need clarification on revocation of access. We are assuming it is from the point the person departs their job - i.e. access to the BES Cyber System is revoked. Such personnel could have hard copies of information but how would you prove that such documentation was shredded? What about information they have retained within their brain? ï?Š We need some clarity on what the parameters are herePlease provide a concise definition for 'sanitize'. We discussed scenarios such as patching the BES Cyber System via a CD - would compliance require that we 'sanitize' the CD? If yes, seems like overkill from our discussions on the subject. Please provide more concise language to define the scope.over real time to either. Yet, in reading the requirements we could potentially be found non-compliant based on the wording of the version 4 standards - this should not be! FYI, I raised this point at the recent 2 day workshop in Texas and the drafting team was in agreement that our current configuration is an example of excellence ... yet is a potentially non-compliant based on current wording ... this needs to be revisited.
44.14	Progress Energy - Nuclear Generation	Disagree	Agree with R24.1, R24.2 and R25.1. Disagree with R24.3, R24.4 and R24.5 which are governed for nuclear generating facilities by CFR. R24-24 should acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
44.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
44.16	E.ON U.S.	Disagree	CIP-011-1, R24.4 is unnecessary and difficult to impossible to document. At this point, all authorized unescorted physical and electronic access would have been removed per other requirements. E ON U.S. proposes that this requirement be deleted.

#	Organization	Yes or No	Question 44 Comment
44.17	USACE - Omaha Anchor	Disagree	Definition would include external hard drives and other external media. It seems ridiculous if you are installing patches to sanitize the media before going to the next cyber system. You are treating the cyber system as a classified system. This is serious overkill. External media for the most part should be exempt from this requirement unless sensitive information is placed on the media in which case it should follow the rules of R24.
44.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising Requirement R24.1 to read:"Identify and designate controls for protection of sensitive information commensurate with its importance to the security and reliable operation of the associated BES Cyber System."24.3. With the heavy industry reliance on vendors and contractors and the requirements throughout other NERC standards to share data with other entities, it is impractical to "Explicitly authorize personnel for access to sensitive information." For example, when information is sent outside Dominion, it is impossible to know every person who sees it. Moreover it is unlikely that whoever does see it would want to sign an agreement with every entity that can submit information. The controls specified above in the requested revision to 24.1 should cover the requirements for access to the information. Dominion requests that this requirement be removed.24.4. It is possible to revoke electronic access to company-controlled devices containing sensitive information and to revoke physical access to company-controlled areas containing sensitive information within 24 hours. It is not reasonable to identify and retrieve information within 24 hours that may have been taken by an authorized user prior to being terminated for cause and it may not be possible to ever retrieve this information if it has been hidden by the individual. Please restate this requirement to indicate that it covers physical and electronic access as follows:"24.4 Revoke electronic access to company-controlled devices containing sensitive information and physical access to company-controlled areas containing sensitive information within 24 hours."24.5. As stated in Dominion's comment to 24.3, it is impractical to authorize individuals. As applied to this requirement it is also impractical to track individuals. In the example given in the above response to 24.3, any non-company

#	Organization	Yes or No	Question 44 Comment
			personnel that might see sensitive data would need to be authorized by every Registered Entity and their companies would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. Dominion requests that this requirement be removed.Note: At Dallas, the SDT requested input as to requiring training and a PRA for access to sensitive information. Dominion requests that training and a PRA NOT be required. Training and a PRA are not required by versions 1, 2, and 3 of the CIP standards and could be impossible to implement across vendors within the electric industry. In the example given in the above response to 24.3, every vendor or business partner would have to take the training from every Registered Entity or have their training approved by every entity (including annually providing the training program to each RE for approval) and ES-ISAC would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. And then, PRAs would have to be addressed. Registered Entities should be required to have internal requirements for access to sensitive information.
44.19	ReymannGroup, Inc.	Disagree	Expand the list of procedures to include 3rd party data recovery services in accordance with an approved vendor management policy for all impact levels.
44.20	RRI Energy	Disagree	Explicitly define “access” as related to sensitive information. Data can be locally cached on web browsers, remote or personal pc’s, etc. These cannot easily be removed let alone 24 hrs removal.
44.21	Constellation Power Source Generation	Disagree	In R24.1, what classifications for sensitive information should be used? The SDT should develop classifications specifically for CIP. As written, this is not an auditable requirement.
44.22	ReliabilityFirst Staff	Disagree	In row 24.1, what is meant by “consequence”? In Table R24, row 24.5, we suggest the verification of access privileges be performed at least quarterly. To Table R24, add a new row 24.6 stating, “Revoke access to sensitive information within 72 hours for personnel terminated not for cause.” And assign this requirement an impact level of “Required” for both Medium and High Impact BES Cyber Systems. Table R25, row

#	Organization	Yes or No	Question 44 Comment
			25.1; we believe there should be a definition of “sanitize” to eliminate confusion regarding what actions must be taken to comply with this requirement.
44.23	MidAmerican Energy Company	Disagree	It was mentioned in the May workshop that the SDT would consider the necessity for Personnel risk assessments and training required prior to granting access to protected information.Personnel risk assessments and training should not be required prior to granting access to protected information. As an example, entities would have a nearly impossible task of completing personel risk assessments for international employees at global help desks that are allowed view only access to a BES Cyber System.
44.24	WECC	Disagree	Item 24.2 should be made clear that individual hard drives, servers, laptops, etc do not need to be labeled. Perhaps “labeling of media” was meant. Item 24.3 will have great impact on the ability to have technical support from large global vendors such as Cisco. Consider exception to this requirement for maintenance or add something to Maintenance requirement R26 to deal with it.Clarify how sensitivity and consequence are determined.Clarify the requirements for authorization for access to sensitive information (i.e. need to know).
44.25	LCEC	Disagree	Need to clarify the acceptable methods.
44.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes that R24 did not take into consideration access privileges with sensitive information. It does not provide clear guidance and left room for interpretation. The following are the recommended updates:R24.5 Verify at least every 12 months that the access privileges to sensitive information reflect the appropriate need with the personnel roles and responsibilities. Access privileges to sensitive should correspond with the needs and appropriate personnel roles and responsibilities.Regarding CIP-011-1/R25, R25 did not provide a standard to sanitize media. The current language did not provide clear guidance and left room for interpretation. The following is the recommended updates:25.1 - Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using clearing

#	Organization	Yes or No	Question 44 Comment
			utility supporting the Department of Defense clearing and sanitation standard. R24.4 - Requirement covered by revocation of physical and cyber access.Revoking physical and cyber access would revoke access to protected information. Therefore, NextEra suggests removing 24.4
44.27	National Grid	Disagree	o Provide timelines for access revocation for reasons other than "terminated for cause" o Do laptops and devices that maintain the BES Cyber Systems need to be sanitized?
44.28	PacifiCorp	Disagree	PacifiCorp asks that the reference to "at least every 12 months" is modified to read "annuallyonce every calendar year." Allowing responsible entities the flexibility to require trying once every calendar year rather than at least every 12 months would relieve entities of the significant administrative burden of tracking specific training deadlines for each individual employee. At the same time, this change will still ensure that employees are trained at regular enough intervals to achieve the reliability goal of the training requirement.
44.29	Ameren	Disagree	R24.3 - Listing people who have access to information serves no purpose in protecting BES systems from Cyber attack. The list of people with this information is not the same as the list of people that have access to the systems. This requirement should be removed.R24.4 - This requirement is impossible to prove for printed documentation. Suggest removal.
44.30	Liberty Electric Power, LLC	Disagree	R25 appears to require the hard drives of laptops used in relay calibrations to be wiped before leaving site. This is a serious issue for smaller entities, due to almost all of the relay work being done by outside contractors. These contractors often need the data taken to write reports which are required by other NERC standards. This requirement needs to be removed.
44.31	Allegheny Energy Supply	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to

#	Organization	Yes or No	Question 44 Comment
			perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperature does not pose a risk to the BES.
44.32	Allegheny Power	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.33	EEI	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

#	Organization	Yes or No	Question 44 Comment
44.34	Hydro One	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems".
44.35	Northeast Power Coordinating Council	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems".
44.36	Idaho Power Company	Disagree	Revocation of access to sensitive information is virtually impossible if the person terminated has the information in their possession either hard copy or portable media. Access to additional information can be revoke. Consider rewording this requirement to accommodate this reality.
44.37	Southern California Edison Company	Disagree	SCE feels the standard, as written, may be operationally difficult to implement. As such SCE recommends allowing for the revocation of electronic access to sensitive information within 24 hours, or make a written demand (which may be followed up by legal process) for such information within a 24 hour timeframe. This distinction is crucial as not all sensitive information may reside within the physical confines of the registered entity. Business concerns may require registered entities to allow sensitive information (if adequately protected by contractual or employment terms) to leave the confines of the company. For example, employees may have CIP-protected information in company-issued laptops. In some scenarios, it may be impossible to recover those laptops if they were left offsite when the employee was terminated. However, it would be possible to issue a written demand, supported by law, for such

#	Organization	Yes or No	Question 44 Comment
			documents. The drafting team is requested to rephrase R24.4 with a view on implementability, enforceability and auditability.
44.38	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that R24.3 should read "Explicitly authorize role-based access to sensitive information."In R24.4, SDG&E asks how would we do this for hard-copy information?In R24.5, SDG&E suggests changing the wording to read "Verify at least every 12 months that the role-based access privileges to sensitive information reflect authorization."
44.39	Progress Energy (non-Nuclear)	Disagree	Should there be an item in table R25 to identify the media to be sanitized that may be overlooked, i.e. printers/plotters/scanners, relay test sets, etc.
44.40	Consultant	Disagree	Table R24 - Item 24.3 This is an access control requirement, and should be moved to access control requirement table. Access control should cover cyber access, physical access, and information access together, as the process for attaining each type of access is related.Item 24.4 is an access revocation requirement, and should be moved to the access revocation requirement table. Access revocation should cover cyber access, physical access, and information access together, as the process for revoking each type of access is related. The comments related to timeframes in those sections are applicable to information access revocation as well.Item 24.5 is an account management requirement, and should be moved to the account management requirement table. Account Management and reviews should cover cyber access, physical access, and information access together, as the process for reviewing and confirming each type of access is related. The comments related to timeframes in those sections are applicable to information access access review as well.Table R26 - Item 26.1 Replace the word "all" with "BES Cyber System" as a better statement.Item 26.1 If 'media' is a defined term it should be capitalized. (See comments on definition of Media.)
44.41	APPA Task Force	Disagree	The APPA Task Force cautions the drafting team on the information protection requirements in R24. Nearly every state in the United States has a public records law

#	Organization	Yes or No	Question 44 Comment
			that applies to public power systems as units of state or local government (These laws are often referred to as “Government in the Sunshine” laws.). We recommend that the drafting team consult with NERC legal counsel prior to revising this requirement. We do not want public power systems to have to choose between being in noncompliance with the proposed requirements or violating their state open records laws. Rebecca Michaels of NERC Staff is familiar with this issue. If this must move forward as proposed we recommend that the following be added to the requirement: “To the extent that state/local laws allow.”R24.Objective:To prevent unauthorized access to sensitive information associated with BES Cyber SystemsR24. Requirement:To the extent permissible under federal and state laws, each Responsible Entity shall document and implement one or more processes that incorporate the criteria in CIP-011-1 Table R24 - Information Protection.
44.42	Reliability & Compliance Group	Disagree	The method of sanitizing media should be done in an industry accepted manner to provide for auditability of the standard.
44.43	Bonneville Power Administration	Disagree	The objectives of these requirements (“to prevent unauthorized access to sensitive information associated with BES Cyber Systems” and “to prevent the unauthorized dissemination of BES Cyber System information”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R24, Section 24.1. Recommend replacing "classify" and "classification" with "categorize" and "category" and "categorization", . "Classify" and "classification" have very specific meanings to any Federal agency. Those meanings are restricted to the realm of National Security Information and are different from what is presented here. Such information requires storage in General Services Administration-approved safes, transmission using National Security Agency-approved encryption, and can be only be processed on computer systems if those systems are dedicated to such use, totally isolated from any publicly accessible network, and stored in secure facilities when not

#	Organization	Yes or No	Question 44 Comment
			in use. Furthermore, the Federal Agencies do not have the option of using a different definition. In fact, using Regional Entity standard forms marked "Confidential" is problematic for Federal agencies, as such a marking is reserved for a particular level of classified information. Given the large number of Federal organizations to which this standard applies, it would simplify matters to restrict the use of "classify" and similar terms to the realm of National Security Information.Recommend deletion of Table 24, Section 24.3. Requiring formal authorization is a process more stringent to that required to gain access to National Defensed Information at the Confidential and Secret level: A formal determination of trustworthiness, but no formal further formal authorization required for access once the clearance has been granted. For sensitive information other than National Defense Information, Federal agencies are required only to determine the the recipient needs the information to support the activities of the agency. Such a determination can be made informally, by any person with custody of the information. We realize that there seem to be conceptual difficulties about revoking access without formally authorizing it. But, they are resolved when we note that authorizing access is not the same as granting it. Authorizing access is a declaration that the person is allowed to have access. Granting access is giving them the info. It is not clear to which of these "revoke" is intended to apply. However, R24 is only concerned about revocation following termination for cause. In those cases, electronic and physical access to all Entity assets is generally revoked. That would effectively deny access to the information, as well. Thus, revocation can be accomplished even though a formal access authorization is not used.
44.44	US Bureau of Reclamation	Disagree	The use of the term classification is not appropriate, suggest "categoruize" to avoid conflict with other requirements in the federal sector.
44.45	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Requirement 25.1.
44.46	We Energies	Disagree	We Energies agrees with EEI: R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the

#	Organization	Yes or No	Question 44 Comment
			responsible entity is unable to perform sanitization on the media.We Energies agrees with EEI: Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.We Energies agrees with EEI: When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.47	FirstEnergy Corporation	Disagree	We would like to have clearer definition on what is acceptable sanitation methods.
44.48	Entergy	Disagree	What exactly does “Explicitly Authorize” mean? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? If so, it should be stated as such.Is approval documentation all that’s required, or is a periodically maintained list required as well?What is the definition of “Revoking Access”? Does the individual need to be removed from every Cyber System he/she had access to?
44.49	Manitoba Hydro	Disagree	What is the meaning of “consequence” in Requirement R24.1? There is currently no requirement for revocation of access to sensitive information for any other reason than “for cause”. There are no specifics given with respect to “classify” sensitive information in Requirement R24.1 so it is assumed to be at the Responsible Entity’s discretion in terms of criteria, methodology, etc. There are no specifics given with respect to “method” in Requirement R25.1 so it is assumed to be at the Responsible Entity’s discretion.

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns were raised by commenters regarding the applicability of the information protection and media sanitization requirements. The issues centered around the tables being too broad brushed. There was also concern surrounding the differentiation of information sensitivity vs. impact categorization. The drafting team modified the standard to only include information protection for High and Medium Impact BES Cyber Systems and associated Physical Access Control Systems, associated Electronic Access Control or Monitoring Systems, and associated Protected Cyber Assets.

#	Organization	Yes or No	Question 45 Comment
45.1	WECC		Criteria should apply to all impact levels
45.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
45.3	Consultant	Agree	Table R24 - Items 24.3, 24.4, & 24.5 should be moved to their respective subject areas as suggested in the comment on Question 44. (Cyber access, physical access, and information access requirements should be addressed together, as the requirements and processes for each type of access is related.)
45.4	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R24-R25 if it is understood that a blank in the table means N/A.
45.5	PacifiCorp	Disagree	: Lines 24.1 and 24.2 imply that multiple classifications levels for "Sensitive Information" will be required. Need to allow for entities to use one classification for "Sensitive Information".24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct

#	Organization	Yes or No	Question 45 Comment
			access privileges found to be inaccurate once they have been verified.
45.6	Southwest Power Pool Regional Entity	Disagree	24.1, 24.2, and 25.1 should be applicable to all impact categories.
45.7	US Army Corps of Engineers, Omaha Distirc	Disagree	24.3 does a job description constitute "explicit authorization?" Restrictions on media use as written would preclude using media to transfer information to external systems using media. Should be reworded with the intent that the media be sanitized before disposed of or released outside the organization or allowances made for transfering information. Also could be interpreted to mean an update disk used to update BES Cyber System 1 would have to be wiped and could not be used to update system 2.
45.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
45.9	Allegheny Energy Supply	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.10	Allegheny Power	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.11	EEI	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.12	MidAmerican Energy Company	Disagree	Lines 24.1 and 24.2 imply that multiple classifications levels for “Sensitive Information” will be required. Need to allow for entities to use one classification for “Sensitive Information”.24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct access privileges found to be inaccurate once they have been verified.

#	Organization	Yes or No	Question 45 Comment
45.13	American Municipal Power	Disagree	Please provide a little or no impact category
45.14	US Bureau of Reclamation	Disagree	Requirements should be applied to information sensitivity, not the impact level of the system(s).
45.15	Southern California Edison Company	Disagree	SCE feels that R24 and R25 apply regardless of the BES Control System impact level.
45.16	Progress Energy (non-Nuclear)	Disagree	See comment 14.
45.17	LCEC	Disagree	See previous comments
45.18	BCTC	Disagree	See Question 44 response
45.19	Bonneville Power Administration	Disagree	See the response to question 44.Item 24.5 in Table R24 states as follows: "Verify at least once every 12 months that the access privileges to sensitive information reflect authorization". Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently verifications must occur.
45.20	LADWP	Disagree	Should be restricted to high level only.
45.21	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in row 25.1.
45.22	Entergy	Disagree	The requirement indicates that the drafting team believes that protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.
45.23	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 45 Comment
	Affiliates		
45.24	We Energies	Disagree	We Energies agrees with EEI: As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

Summary Consideration:

The definition of "maintenance" that was originally posted as an informal definition adjacent to Requirement R26 in draft CIP-011-1 was:

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

There were questions and concerns raised by commenters about what is included in the scope of maintenance activities. There were comments that the term "maintenance devices" needs to be defined. In addition, there was a question regarding whether remote access is included as maintenance. There were suggestions that the definition of maintenance should be focused on the temporary connections.

One commenter suggested the following definition: "Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the configuration of, or introducing malicious code, to the BES Cyber System." The drafting team considered this feedback, and removed the definition of maintenance from the revised standard, and instead focused on temporarily connecting to a BES Cyber System (such as for maintenance) rather than on the activity being performed. (See proposed CIP-007-5 – System Access Control.)

The requirement for Transient Cyber Assets and media in CIP-007-5 R3.4 is intended to ensure that devices used for temporary access to the BES Cyber System (such as for maintenance) do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. The definition for **Transient Cyber Asset** is as follows:

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

#	Organization	Yes or No	Question 46 Comment
46.1	WECC		Provide a separate definition of maintenance device. The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
46.2	SCE&G	Agree	Are maintenance devices also to be treated as remote access, as it is a device external to the BES cyber system?26.2: TFEs may be necessary for maintenance devices not capable of supporting malicious code prevention.
46.3	Regulatory Compliance	Agree	BUT -Please clarify definition of "not permanently connected"What if you have a device that might be connected for several months?
46.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
46.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
46.6	NextEra Energy Corporate Compliance	Agree	NextEra comments that if a laptop is used to remotely connect to a High Impact Control Center BES Cyber System to debug a problem or view Operator issues by temporarily gaining alarm permissions that are assigned to the Operator, is this considered a maintenance activity?
46.7	Progress Energy - Nuclear Generation	Agree	Nuclear facilities have maintenance programs based on CFR. This definition can be improved by acknowledging 10CFR50.65.
46.8	APPA Task Force	Agree	The APPA Task Force agrees with the definition.

#	Organization	Yes or No	Question 46 Comment
46.9	GTC & GSOC	Agree	We recommend the last sentence in this definition (“Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System”) be removed from R.26 and instead be included as part of the BES Cyber System definition, as suggested in our comment to 1.b. above.
46.10	Consultant	Disagree	"Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches." NONE of these activities are maintenance activities.Configuration changes & software patches are changes covered by change control. Vulnerability assessments are tests covered by vulnerability assessments."Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System." This is not a definition of "Maintenance". This is (or should be) part of the definition of BES Cyber System Component. Suggest both of these statements be removed from the "definition".
46.11	Dairyland Power Cooperative	Disagree	26.2 A definition of a maintenance device seems needed here. I’m presuming this typically would be the computer used by the support staff to access the BES system for maintenance. What if maintenance is being directly performed on a BES system, is there no maintenance device involved in that case?
46.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
46.13	Network & Security Technologies Inc	Disagree	Definition is good overall but should address the question of whether a maintenance device is “external” and must therefore connect via an access point.
46.14	National Grid	Disagree	Does testing the capabilities of the relays part of the maintenance activities?
46.15	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising the definition of Maintenance as follows:”Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the

#	Organization	Yes or No	Question 46 Comment
			configuration of, or introducing malicious code, to the BES Cyber System.”
46.16	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.17	Black Hills Corporation	Disagree	Middle sentence of Maintenance definition should add ... include but are not limited to configuration...
46.18	Minnesota Power	Disagree	Minnesota Power recommends that the following definitions be adopted by the Standards Drafting Team:Maintenance: Maintenance, for the purpose of this standard, is defined as activities associated with the support, testing and upkeep of a BES Cyber System. Maintenance Equipment: Maintenance Equipment, for the purpose of this standard, is defined as any programmable, electronic device used for maintenance activities that are not permanently connected to the BES Cyber System(s). These devices are not considered part of the BES Cyber System(s).
46.19	PacifiCorp	Disagree	PacifiCorp agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.20	Southwest Power Pool Regional Entity	Disagree	Programmable, general purpose devices connected temporarily are a potentially high risk to the BES Cyber System and should have some minimum set of applicable requirements to minimize that risk. An example is the “wandering laptop” that the support staff uses to connect to High impact BES Cyber Systems and also to surf the Internet from a home Internet connection.
46.21	Duke Energy	Disagree	Suggest replacing “Cyber System Maintenance” with “Cyber System Configuration Management”. The definition (first sentence) states: "Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System." There are numerous activities that are associated

#	Organization	Yes or No	Question 46 Comment
			with support, testing, and upkeep of a BES Cyber System that are not related to cyber. This could be tuning, calibrating, etc. and could be done with a screwdriver and a meter. The second sentence includes configuration changes, vulnerability assessments, and software patches. These items are more applicable to the cyber related definition. The suggestion is to combine these sentences:"Maintenance for the purpose of this standard includes the cyber security related activities associated with the support, testing and upkeep of a BES Cyber System, including configuration changes, vulnerability assessments, and software patches."Also, please clarify if non-portable test systems that are connected to BES Cyber Systems thru an access point are included. Otherwise define “permanently connected.”
46.22	BGE	Disagree	Systems used for maintenance should be protected and sanitized per 25.1.
46.23	FirstEnergy Corporation	Disagree	The definition does not clearly specify that the intention is for temporary direct connections.
46.24	Allegheny Energy Supply	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.25	Allegheny Power	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.26	EEI	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.27	Southern California Edison Company	Disagree	The justification of separating end users of BES systems and those involved in maintenance is not consistent with the justification for systems that are used for maintenance. The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. However, a distinct list of maintenance personnel is required to be maintained. The suggestion for the drafting team is to move this requirement to the section dealing with personnel.

#	Organization	Yes or No	Question 46 Comment
46.28	Progress Energy (non-Nuclear)	Disagree	Troubleshooting also needs to be explicitly included as an example.
46.29	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
46.30	We Energies	Disagree	We Energies agrees with EEI: The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.31	LADWP	Disagree	Will require multiple list management. Individual doing maintenance will already be on physical and electronic access list. Now another list is introduced which will also need to be maintained with the same revocation requirements. 26.1 is not necessary.

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters raised concerns about the interaction between the list of personnel in draft CIP-011-1 R26.1 and the lists of those granting authorized electronic and physical access. In addition, commenters were concerned about the interaction with other user/account management requirements. Some commenters suggested that all maintenance devices should be documented in a list. In addition, there were comments regarding the allowance for emergency maintenance situations.

Some commenters suggested that Requirement R26.1 is duplicative of Requirement R8 and should be removed, and that Requirement R26.2 is duplicative of Requirement R23 and should also be removed. The drafting team considered this feedback and has attempted to address these concerns by incorporating the requirements associated with maintenance into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 47 Comment
47.1	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
47.2	National Grid	Agree	Please provide clarification on 26.2.
47.3	Puget Sound Energy	Agree	Puget Sound Energy suggests additional language to clarify if personnel referenced in R26.1 are required to be maintained on the lists associated with Table 5.
47.4	Southern California Edison Company	Agree	SCE requests the Standards Drafting Team combine Requirement R26.1 with other requirements for personnel management and rationalize compliance requirements across personnel.
47.5	APPA Task Force	Agree	The APPA Task Force has no comment on this question.

#	Organization	Yes or No	Question 47 Comment
47.6	Emerson Process Management	Agree	This seems to be a typical task for properly maintaining a cyber (or computer) system. The personnel for doing this task should be already identified in the personnel training, awareness, and risk assessment. This requirement seems to be extra.
47.7	Independent Electricity System Operator	Disagree	- R26.2 define malicious code. Does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- R26.1: suggest using a word other than “personnel”
47.8	Network & Security Technologies Inc	Disagree	26.1 - Should be reworded to distinguish “maintenance” personnel from System Administrators, who in most instances also perform maintenance activities. If the SDT concludes there is really no distinction, this requirement becomes redundant and should be eliminated, as lists of users and the permissions they have (including “System Administrator”) are already required.26.2 - Many test devices are appliances and may not be capable of meeting other CIP-011 requirements, including malicious code protection. Thus, this requirement needs to be eligible for TFEs.
47.9	Dairyland Power Cooperative	Disagree	26.1 This overlaps with the requirement of limits access based on electronic accounts. How can this be blended with user/account management?
47.10	ERCOT ISO	Disagree	26.1: Recommend addressing emergency situations more clearly. How should an entity address listing authorized personnel where support companies use a call center and cannot provide dedicated resources for the entity? This is particularly relevant for after-hours issues.
47.11	Regulatory Compliance	Disagree	26.2 - Propose this phrasing:Insure maintenance devices are free and clear of malicious code prior to the intoduction to the BES System.
47.12	Luminant	Disagree	26.2 should read "Detect and respond to the introduction of malicious code."
47.13	Southwest Power Pool	Disagree	26.2: Requirement is not necessarily applicable to special purpose testing devices, such as Fluke meters. Need to revise to limit the requirement to general purpose

#	Organization	Yes or No	Question 47 Comment
	Regional Entity		devices for which malware prevention is possible.
47.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
47.15	Liberty Electric Power, LLC	Disagree	CIP-026 will penalize entities if malware gets on any device, even if we employ the best available technology and processes to prevent it. This requirement needs to be removed.
47.16	Alberta Electric System Operator	Disagree	Consider revising R26.1 (or creating a new sub-requirement) to include verifying and updating the list of authorized personnel.
47.17	PacifiCorp	Disagree	Devices used for maintenance should also meet the system hardening criteria of R16 and R17.
47.18	MidAmerican Energy Company	Disagree	Devices used for maintenance should meet the system hardening criteria of R16 and R17.
47.19	Dominion Resources Services, Inc.	Disagree	Dominion appreciates the SDT's thoughts in providing this section and its associated exclusions and is very much in favor of this type of requirement. Dominion agrees with the need to protect the BES Cyber System from harm during this process, but is concerned that these requirements are overly broad.26.1. Dominion recommends that this requirement be deleted. All of these actions are covered by other requirements - access controls, change management, training (roles and responsibilities). It adds another layer of administrative paperwork to track every action made by every authorized technician with no corresponding protection to the BES. 26.2. It appears that this requirement intends to allow technicians to connect their personal laptops to relays without having to reformat them afterwards. This requirement has the unintended consequence of including any device used for maintenance (e.g., fluke meters, etc.). A footnote to avoid the necessity of a potential TFE should be added.

#	Organization	Yes or No	Question 47 Comment
47.20	US Bureau of Reclamation	Disagree	Either individuals have access authorization or they don't. This would appear to be an unnecessary tracking requirement.
47.21	RRI Energy	Disagree	Even if a maintenance device is completely up-to-date on all security patches, and also has up-to date virus detection software with the most recently release virus pattern definitions, I can not 100% ensure that malicious code will not accidentally be introduced to a BES cyber system while connected. "Ensure" is a very absolute word that is hard to match in practice. It would be better to "require " that maintenance devices have the same level of virus protection and patch management as BES Cyber Assets which the maintenance devices are being used to maintain.
47.22	ReliabilityFirst Staff	Disagree	How do personnel get authorized for addition to the list in row 26.1 and how often does this list get reviewed and updated. Add requirements for the conduct of a vulnerability assessment and actions to be taken (i.e., mitigation plan) resulting from this vulnerability assessment.
47.23	Western Area Power Administration	Disagree	How do we differentiate between "maintenance" and "administration"? This seems like a new role? This should be worked into Table R10.
47.24	WECC	Disagree	Item 26.1 would have strong impact on the ability to get timely technical support from large global companies such as Cisco Systems. Perhaps there needs to be distinct definitions for "authorized access" vs "maintenance access"? Item 26.2 seems to be covered in previous R15.The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
47.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that Requirement R26 does not provide anytime frame in which the list should be reviewed nor does it take into consideration vendors. The current language does not provide clear guidance and leaves room for interpretation. The following are the recommended updates:26.1 - NextEra suggests maintaining a list of

#	Organization	Yes or No	Question 47 Comment
			personnel authorized to perform maintenance on the BES Cyber System, allow authorized personnel to escort cyber and physical vendors, and allow only authorized personnel to perform maintenance on the BES Cyber System. The list of personnel authorized to perform maintenance of the BES Cyber System should be updated at least annually.Maintenance devices not permanently connected to BES Cyber Systems are not considered part of the BES Cyber System.
47.26	Allegheny Energy Supply	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.27	Allegheny Power	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.28	EEI	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.29	Southern Company	Disagree	R.26.1 If personnel are required to have a PRA, are granted physical access, system usage is logged and the individual has access credentials for cyber systems, the additional list generation should not be required.Vendor personnel supporting systems would need to be added to the personnel listing, these personnel frequently change. The addition of a name to the list would become a common event.
47.30	Consultant	Disagree	R26 - Suggest changing wording to "implement and document"Suggest changing wording to: "Systems and to ensure that" for correct grammar.R26 - Delete the word "accidentally" from the statement. It would appear a better objective is to prevent the introduction of malicious code, "accidentally" or "intentionally" is not relevant to the objective.Table R26 - Item 26.1 This is a new account management requirement. There are account management activities for cyber access, physical access, information access, and now maintenance access. As such this requirement should be moved to the account management requirements table.Item 26.2 This is not a requirement statement, it is a statement of a desired objective. It is not clear what

#	Organization	Yes or No	Question 47 Comment
			requirement or requirements are intended to meet this objective. Please clarify the requirement.
47.31	FirstEnergy Corporation	Disagree	R26 text needs to be more specific that the intention is for temporary direct connections. Otherwise, R26 appears to be covering CIP 7R1 and 7R3.
47.32	Progress Energy (non-Nuclear)	Disagree	R26.1 - do not see need for this requirement. Changes can only be made with cyber access rights which is covered by other requirements.R26.2 - either eliminate this requirement or make additional provisions for the safe use of maintenance components. CIP standards shouldn't mandate malware protection on all test equipment. The BES Cyber Systems components should already be adequately protected from threats as a result of being compliant with the other requirements.We like the use of the footnote earlier in the standard that allowed the use of the highest level of protection the components can support maybe something like that could be used here too.
47.33	Public Service Enterprise Group companies	Disagree	R26.1 requires maintaining another list of personnel who perform maintenance on a BES Cyber System. These individuals are already tracked and documented under other access lists. Seems like a duplication of effort with no benefit and thus the requirement should be deleted.
47.34	Xcel Energy	Disagree	R26.2 - The requirement should be worded to require anti-malware protection on all maintenance devices. The current wording would make it an enforceable violation if, in spite of best efforts, malware was introduced in to a device.
47.35	Hydro One	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.
47.36	Northeast Power Coordinating Council	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.

#	Organization	Yes or No	Question 47 Comment
47.37	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
47.38	LADWP	Disagree	See previous
47.39	BGE	Disagree	Should not have a separate list for maintenance personnel. All personnel should be included on the access control lists created per R7 - R14.
47.40	Duke Energy	Disagree	Suggest replacing "Cyber System Maintenance" with "Cyber System Configuration Management".Requirement 26.1: Please consider adding the word "cyber security related" to make the definition read as follows:Maintain a list of personnel authorized to perform cyber security related maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.Requirement 26.2: Please consider changing as highlighted below:Detect and prevent the introduction and propagation of malicious code on all computer based maintenance devices.Remove 'accidently' from R26. Suggest removing all of R26.26.1 Specify maintenance performed is done with the maintenance device. We interpret 26.1 to be that the maintenance personnel would not have to be background screened and trained. Suggest including screens and trains for these folks. Or remove the requirement with the understanding that these personnel will have electronic or unescorted physical access to the BES Cyber System. This is extra work for no added security.26.2 will need a TFE. Within generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.
47.41	Detroit Edison	Disagree	Table R26.2 only addresses the introduction and propagation of malicious code into

#	Organization	Yes or No	Question 47 Comment
			the BES Cyber System. It is likely however, that a device may be modified not to introduce or propagate code but act as a bridge to another rogue network via wireless, cellular or other medium. This would be akin to introducing an unsecured access point into the boundary if this system is not subject to the same requirements equal to or greater than that of highest impact BES Cyber System component. A possible solution could be to require mitigation for multi-homed or bridged networks for all components used for BES Cyber System maintenance, and/or append R26 to read "...and ensure that systems used for maintenance do not introduce malicious code into the BES Cyber System or act as an unauthorized access point into an Electronic Security Perimeter."
47.42	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidentally introduce malicious code into the BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R26, Section 26.2. It is impossible to prevent the introduction and propagation of malware. This is already addressed in Requirement 15. Recommendation: Delete Section 26.2.
47.43	Manitoba Hydro	Disagree	The personnel authorized to perform maintenance on the BES Cyber System should be identified by roles, not individual names. There are no specifics given with respect to "prevent" in Requirement R26.2 so it is assumed to be at the Responsible Entity's discretion in terms of means, criteria, etc.
47.44	Reliability & Compliance Group	Disagree	There is a possible issue that could occur with this requirement regarding collective bargaining unit rules. It may require that job classifications be created for individuals who work on these systems.

#	Organization	Yes or No	Question 47 Comment
47.45	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.
47.46	Minnesota Power	Disagree	Using the definitions proposed in Question 46, Minnesota Power recommends that Requirement R26 state that "prior to connecting Maintenance Equipment or importing data, patches, code or other electronic files into the BES Cyber System, the device and/or files shall be scanned for malware and up-to-date on security patches."
47.47	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
47.48	We Energies	Disagree	We Energies agrees with EEI: R 26.1 is duplicative of Requirement 8 and should be removedWe Energies agrees with EEI: R 26.2 is duplicative of Requirement 23 and should be removed.
47.49	Florida Municipal Power Agency	Disagree	Why is malware mentioned in 26.2, when it already has been covered in R15? FMPA believes this should be removed.

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Several commenters suggested that the types of connectivity used for temporary connections should be considered. In addition, several commenters suggested that the criteria should be applied to all impact levels. There was also a comment for a no impact category.

The drafting team considered this feedback and attempted to address these concerns by incorporating the requirements associated with maintenance activity into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 48 Comment
48.1	WECC		Criteria should apply to all impact levels
48.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R26 if it is understood that a blank in the table means N/A.
48.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
48.4	Progress Energy - Nuclear Generation	Agree	R26 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
48.5	Allegheny Energy Supply	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.

#	Organization	Yes or No	Question 48 Comment
48.6	Allegheny Power	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.
48.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
48.8	American Municipal Power	Disagree	Please provide a little or no impact category
48.9	BGE	Disagree	Should not be separate requirements for maintenance of BES Cyber Systems.All personnel should be included on the access control lists created per R7 - R14.
48.10	Consultant	Disagree	The comments on Question 47 regarding moving item 26.1 elsewhere, and Item 26.2 not being a requirement statement preclude an evaluation of application to impact categories.
48.11	Duke Energy	Disagree	Require for low when the maintenance device also connects to medium or high systems.
48.12	EEI	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.
48.13	Entergy	Disagree	Basic Maintenance requirements should apply equally for all components of a control system
48.14	FirstEnergy Corporation	Disagree	Until clarity is provided on the above comments (Q46 and Q47), we can not provide a

#	Organization	Yes or No	Question 48 Comment
			response to this question.
48.15	Florida Municipal Power Agency	Disagree	FMPA believes this standard should be removed entirely, as it is already addressed under account control, R7.
48.16	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
48.17	Progress Energy (non-Nuclear)	Disagree	See comment 14.
48.18	Public Service Enterprise Group companies	Disagree	General agreement, but Requirement 26.2 may not be technically feasible for certain types of maintenance devices. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase "where technically feasible".
48.19	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in rows 26.1 and 26.2.
48.20	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
48.21	Southern California Edison Company	Disagree	The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. If this is not the intent of the team, the wording of the standard should be modified to reflect the difference in impact levels.

#	Organization	Yes or No	Question 48 Comment
48.22	Southwest Power Pool Regional Entity	Disagree	26.2 should be applicable to all impact categories.
48.23	US Army Corps of Engineers, Omaha Distirc	Disagree	There needs to be a provision for emergency work. Whether that means talking someone through a fix at 2am or hiring a vendor for additional expertise.
48.24	We Energies	Disagree	We Energies agrees with EEI: R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning.

One of the primary focus areas of the comments concerned coordination with the reporting requirements in CIP 001 and EOP-004 for reporting to the ES-ISAC, and additional guidance in determining incident classifications. The SDT has attempted to coordinate with the drafting team working on revisions to CIP-001 and EOP-004 to ensure the two sets of requirements are coordinated. As the two teams are working in parallel, continued coordination will be necessary.

Several commenters asked for definitions for cyber security incidents and reportable cyber security incidents. The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary.*

The SDT also proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Several requests were made to clarify the periodic timing requirements such as annual, calendar year, and 12 months. The drafting team reviewed the timing elements of all requirements and where there was a reference to "annual" the SDT replaced this with the following:

". . . at least once each calendar year, not to exceed 15 calendar months between. . ."

Some commenters recommended placing all requirements in the table, not in the objective or in the "pre-amble" for cyber incident reporting, and the drafting team has included all mandatory performance in the requirements.

Many commenters requested clarifications for plan testing requirements, operational exercises, test environment, as well as the number of tests required. The drafting team did attempt to add more clarity to plan testing requirements along with operational exercise, test environment, and number of tests required in the revised standard (CIP-008-5).

Guidance was requested regarding review of the results of incident response tests in less than 60 days. The revised standard now requires the review to take place within 30 calendar days and the update, based on lessons learned, to take place within 60 calendar days of the test.

Some commenters asked for clarity on the inclusion of physical breach aspects of cyber security incidents as reportable. The drafting team is coordinating its revisions with the revisions to CIP-001 and EOP-004 underway through Project 2009-01 – Disturbance and Sabotage Reporting.

There were concerns raised as neither logging nor monitoring are required for Low Impact BES Cyber Systems, there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified. The applicability section of the entire suite of CIP Version 5 standards has been revised to provide greater clarity on which BES Cyber Systems (High, Medium, and Low Impact) are applicable to specific requirements.

#	Organization	Yes or No	Question 49 Comment
49.1	National Rural Electric Cooperative Association (NRECA)		In R27.1 a "process" is required, but it is not clear as to how a utility is required to "classify" events. Please provide further clarification as to how one is required to "classify" these events.In R29.1 the requirement is to review the plan once every 12 months. Please provide specificity as to what "once every 12 months" means. If I review the plan on Jan. 15, 2001, am I in compliance if I review it again by Jan. 25, 2002? Please make sure that this is clear in the requirement and in all requirements of CIP-010-1 and CIP-011-1.
49.2	Tenaska		Consider combining 28 and 29
49.3	Black Hills Corporation	Agree	Request that the language in 27.3 be broadened to include contacting appropriate law enforcement authorities, similar to CIP-001.
49.4	FEUS	Agree	Agree with Comments: the drafting should clarify the reporting time requirement for

#	Organization	Yes or No	Question 49 Comment
			27.3, reporting to the ES-ISAC
49.5	Green Country Energy	Agree	I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these requirements.
49.6	SCE&G	Agree	R29 is a good example of an instance where there are a lot of timing requirements embedded in the requirements. It would be helpful to entities if timing requirements were consistently put in the same location in the tables (under the low, medium, and/or high columns) rather than embedded in the text. The SDT should evaluate the number of timed requirements in relation to the low, medium, and high impact categories. Once the requirements are finalized it would be of benefit to entities to have a list of the timeframe type requirements which must be met for each low, med, and high impact system, as these often present some of the greatest administrative burden in documenting these timeframes were met.
49.7	Allegheny Energy Supply	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.8	Allegheny Power	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.9	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
49.10	Ameren	Disagree	R27 would be better suited in CIP-001, Sabotage Reporting.â€,â€,â€,

#	Organization	Yes or No	Question 49 Comment
49.11	American Electric Power	Disagree	27.1 - 27.3: Recommend requiring this for systems with routable external connectivity only. To properly monitor and alert on cyber security events, a trained IT Security Operations staff and dedicated set of monitoring tools are required. If there is no external connectivity, there is no access for the IT teams to monitor these cyber systems.
49.12	APPA Task Force	Disagree	The APPA Task Force supports the drafting team's efforts on incident response. We propose the following edits:The APPA Task Force believes that NERC, as the ES-ISAC, should have a standard process for entities to use in reporting Cyber Security Incidents. Therefore, we propose the following wording for R27 Table 27.3: 27.3: Use the reporting guidance developed by the ES-ISAC for reporting Cyber Security Incidents, either directly or through an intermediary, or develop a process equivalent or superior to that guidance.28.1, recommend changing "once every 12 months" to "Annually."29.1, recommend changing "once every 12 months" to "Annually."
49.13	Bonneville Power Administration	Disagree	The objectives of these requirements ("so that responses to Cyber Security Incidents involving BES Cyber Systems can occur" and "to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table 28, Section 28.1. It's not clear whether testing in January 2010 and June 2011 would satisfy the requirement, since February 2010 through January 2011 would be a 12-month period with no testing. Recommendation: Replace "every 12 months" with "each calendar year". Also, there are other ways to test, as well. Recommendation: "Test the execution of the incident response plan (by recovering from an actual incident, or with a test at least as comprehensive as a paper drill) at ... Table 29, Section 29.1. Same comment as 28.1

#	Organization	Yes or No	Question 49 Comment
49.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
49.15	Consultant	Disagree	R27 - "...so that responses to Cyber Security Incidents involving BES Cyber Systems can occur." should be reworded. Suggest "to identify responsibilities and actions in response to an incident associated with BES Cyber Systems."Table R27 - should specify in each statement that it applies to BES Cyber Systems."Cyber Security Incident" is defined in the Glossary using the terminology from CIP-002 through CIP-009. That definition should be revised by including a new definition in this standard using the terminology associated with CIP-010 and CIP-011.Item 27.3 Not all Cyber Security Incidents are reportable to ES-ISAC as indicated in The Security Guidelines for the Electricity Sector: Threat and Incident Reporting, version 2.0, dated April 1, 2008. Suggest clarifying the statement about reporting.Table R28 - Item 28.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Table R28 - Item 28.1 It is not clear from the table whether one test is required, or two tests (one for High Impact & one for Medium Impact) Suggest some clarification wording in the requirement statement.Table R29 - Item 29.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Item 29.2 - Suggest deleting the word "each" as an unnecessary word.Item 29.3 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 29.5 Suggest deleting the word "all" as an unnecessary word.
49.16	Detroit Edison	Disagree	Table 28.1 and 29.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.

#	Organization	Yes or No	Question 49 Comment
49.17	Dominion Resources Services, Inc.	Disagree	Per R18, neither logging or monitoring are required for Low Impact Systems, hence there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified.
49.18	Duke Energy	Disagree	Requirement 27: The requirements need a definition of a "Cyber Security Incident". This needs to differentiate between a cyber security attack and a mistake that a technician makes in the plant. We don't need to report every time a technician forgets their password.Requirement 28 only has one item and it is related to Requirement 29. Perhaps combine these two?Table 28: 28.1 assumes there is only one incident response plan when R27 allows for multiple plans. We would like to test AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to test all of them. Combine 28 with 29 if the VSL is the same.Table 29: 29.1 We would like to review AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to review all of them.
49.19	E.ON U.S.	Disagree	Comments: CIP-011, R27 The application of this standard to low-impact BES CS's seems inconsistent. There are not requirements for monitoring security events associated with these assets.CIP-011, R29.1 The application of this standard to low-impact BES CS's seems inconsistent with other requirements for monitoring security events associated with these assets.CIP-011, R30.2 Please clarify whether "...identification of the personnel responsible..." require naming individuals, or job functions?
49.20	EEI	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

#	Organization	Yes or No	Question 49 Comment
49.21	Emerson Process Management	Disagree	Without being required to perform tasks in System Security, low impact BES Cyber systems may not be able to easily classify cyber security incidents.
49.22	Entergy	Disagree	The current definition of “Cyber Security Incident” will need to be changed as it references ESPs and PSPs. As such, it may be a good idea to define what this term means here.It is observed that as written there is no longer a requirement to keep documentation associated with a Cyber Security Incident (i.e., akin to CIP-008 R2). Is this the intent?
49.23	ERCOT ISO	Disagree	29.2: Should be 30 days rather than 60 days to align with FERC Order 706.
49.24	FirstEnergy Corporation	Disagree	27.1: From CIP-008 R1.1, what happened to the concept of "reportable"?
49.25	Independent Electricity System Operator	Disagree	- R27.1: note that the word “reportable” has been removed; CIP-008-2, R1.1 stated “Procedures to characterize and classify events as reportable Cyber Security Incidents”- R28.1: modify the sentence to state “Test the execution of the Cyber Sec
49.26	ISO New England Inc	Disagree	see recommendation for review in prior requirements use same for all annual/ 12 month review.
49.27	Manitoba Hydro	Disagree	The wording of Requirement R28.1 should be revised as the phrase “with a paper drill” could be misinterpreted. There are no specifics given with respect to ‘classifying’ events in 27.1 so it is assumed to be at the Responsible Entity’s discretion in terms of criteria, etc.
49.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R27, but recommends that the last phrase be changed from “so that responses to Cyber Security Incidents involving BES Cyber Systems can occur” to “so that responses to Cyber Security Incidents involving BES Cyber Systems follow a defined plan.” Responses can (and will) happen with or without a plan. The purpose of R27 is to define, ahead of time, a process to ensure an orderly response.Minnesota Power

#	Organization	Yes or No	Question 49 Comment
			generally agrees with the proposed Requirements R29, but recommends that this Requirement should be revised to ensure consistency with Requirement R32. For example, Part 29.1 should state "Review the incident response plan(s) at least once every 12 months or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements.") If this language was consistent with Requirement R32, the following issues could be resolved. In addition, the Standards Drafting Team should consider whether or not Parts 29.2 - 29.5 should also be required of Medium Impact Systems (since Part 28.1 requires testing for those systems) with a longer timeframe.
49.29	Network & Security Technologies Inc	Disagree	R27 - should clarify whether cyber security incidents of a physical nature are included and, if so, should tie back to 5.11.29.2 - Sixty days seems like a very long time to wait before evaluating the effectiveness of response actions, esp. if they were taken in response to an actual incident. Suggest revising to require a much more immediate "after action" review, at least for actual incidents. Should be a matter of days - perhaps 7 or less, not months. Even for tests, 60 days seems overly generous. Suggest revising to 30 days.
49.30	Nuclear Energy Institute	Disagree	Does the definition of cyber security incident, as used in this Standard, comport with the definition in Section 215 of the FPA? ("The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.")
49.31	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
49.32	Progress Energy - Nuclear Generation	Disagree	Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security

#	Organization	Yes or No	Question 49 Comment
			Plans for comments for nuclear generating facilities.
49.33	Progress Energy (non-Nuclear)	Disagree	What makes 28.1 and 29.1 different that requires 2 different requirements? If you test the execution every 12 months then you have effectively done a review.
49.34	ReliabilityFirst Staff	Disagree	Problem with auditing the "effectiveness" of R28 without some clear guidelines that would lead to consistent application by all auditors. For R29.4, please clarify what is meant by system, organizational, and technology changes.
49.35	San Diego Gas and Electric Co.	Disagree	SDG&E believes that the Incident Response Plan requirements should only apply to Medium and High impact assets. Including Low impact assets in these requirements seems like overkill. For example, in R27.3, we don't feel that we would necessarily report a "Cyber security incident" on a Low impact item to ES-ISAC.
49.36	Southwest Power Pool Regional Entity	Disagree	27.1: Should be a "reportable" cyber incident. May be appropriate to add as a separate requirement to identify Cyber Security Incidents as "reportable." 27.2: "Communication plans" needs to be defined somewhere. 28.1: Consider changing "Test the execution of the incident response plan" to "Exercise the incident response plan." Clarify that the exercise scenario must involve a covered BES Cyber System and that the exercise must follow (actually exercise) the incident response plan steps. Also need to clarify whether each BES Cyber System, or at least one in each impact category represented, must be included in the exercise. Requiring the inclusion of each BES Cyber System is not recommended due the potential burden; this is a clarification issue to ensure the entities and the auditors have the same understanding. 29.1: Should the 12-month requirement be +/- one month? 29.2: Reviewing an exercise or actual response 60 days after the fact is too long. To keep it fresh in the minds of the responders, 30 days max is suggested, 15 days for High impacting systems is preferred.
49.37	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of

#	Organization	Yes or No	Question 49 Comment
			the previous requirements that did not apply to low systems.
49.38	We Energies	Disagree	We Energies agrees with EEI: Suggested modification to R27.3: “Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).”We Energies agrees with EEI: If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning, and "Cyber Security Incident Response Plan Testing" is addressed in CIP-009-5 - Cyber Security — Recovery Plans for BES Cyber Assets and Systems."

The primary focus areas of the comments received was on impact levels and the concern for coordination with the reporting requirements in CIP 001. The SDT has coordinated with the drafting team working on revisions to CIP-001 to ensure the two sets of requirements are coordinated.

Many commenters requested that Incident Response requirements for Low Impact BES Cyber Assets or non-routable connections be removed along with providing improved consistency between requirements related to impact level. The revised requirements (now contained in CIP-008-5) do not apply to Low Impact BES Cyber Assets. The SDT updated the applicability section of all requirements in the entire suite of CIP Version 5 standards.

It was suggested that Requirement R28.1 should be modified to clarify that test plans should be exercised once each calendar year (vs. every 12 months), and that these tests will be conducted on an overall system basis and not on a per system or per component level basis. This requirement is defined in CIP-009-5 Requirement R2.1, Recovery Plan Implementation and Testing. There were suggestions regarding the clarification of the plan testing requirements, operational exercises, and test environment, and there were comments regarding the addition of guidance on Cyber Security Incident classification by adding glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. The testing requirements, operational exercises, and test environment are described in CIP-009-5, and a couple of terms were added to the NERC Glossary for completeness.

The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

"*A malicious act or suspicious event that:*

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary."*

The drafting team proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

" Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service."

A few comments were directed at reviewing of results of Incident Response tests in less than 60 days, including the physical aspects of Cyber Security Incidents. The SDT modified this requirement and now requires that this review be performed within 30 days of the BES Cyber Security incident or test and to update the BES Cyber System Incident response plan based on lessons learned within 60 calendar days of the BES Cyber Security incident or test.

Issues identified in comments for the SDT to consider for modifications included additional guidance on performing Cyber Security Incident classification. This is now covered in the guidance documentation for CIP-008 and CIP-009..

With Version 5, the drafting team has worked to make the applicability for each requirement very clear.

#	Organization	Yes or No	Question 50 Comment
50.1	Hydro One		Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R27-R29 if it is understood that a blank in the table means N/A.
50.3	Bonneville Power Administration	Agree	Items 28.1 in Table R28 and 29.1 in Table R29 states that the incident response plan shall be tested "at least once every 12 months" and that the incident response plan should be reviewed at least once every 12 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently testing or review must occur.
50.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
50.5	Florida Municipal Power	Agree	FMPA believes "12 months" should be changed to "annual"

#	Organization	Yes or No	Question 50 Comment
	Agency		
50.6	PacifiCorp	Agree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.7	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
50.8	Southern California Edison Company	Agree	SCE recommends that the standards drafting team use the phrase “cyber security incident” or “physical security incident” to differentiate them from the occurrence of system events that may or may not result from the breach of a “cyber” or “physical” control. As the Requirements are currently written, there is no logging and monitoring requirements for low impact systems. It is inconceivable how a registered entity could implement an incident response plan at these facilities when per CIP standards access and use of these facilities is not required. If the drafting team intends for incident response, as it pertains to Sabotage Reporting under CIP 001, they should state it.
50.9	Alberta Electric System Operator	Disagree	In Table R29, for 29.2, consider revising to review results for High Impact systems to within 30 days, and Medium Impact systems to within 60 days.
50.10	Allegheny Energy Supply	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not

#	Organization	Yes or No	Question 50 Comment
			include every possible BES Cyber System.
50.11	Allegheny Power	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
50.13	Ameren	Disagree	R28.1 - Based on the number of Medium Impact Systems this will be labor intensive with no added protection to the BES. Suggest that this requirement only remain for High Impact Systems.
50.14	American Electric Power	Disagree	Please see response to Question 49.
50.15	American Municipal Power	Disagree	Please provide a little or no impact category
50.16	American Transmission Company	Disagree	R27 requires a response to cyber security incident for all Low Impact BES Cyber Systems; however R18 does not require monitoring and/or logging of Low Impact BES Cyber Systems. How do you respond to an incident unless it is being monitored?
50.17	BGE	Disagree	R29 should apply to any BES Cyber System required in R28.
50.18	Black Hills Corporation	Disagree	28.1 and 29.2 should also be required for Low Impact BES Cyber Systems.
50.19	Consultant	Disagree	Table R27 to Table R29 - It doesn't appear to make sense that the Incident Response Plan applies to all impact level categorizations, while testing the plan applies to Medium Impact & High Impact assets, and actions related to updating the plan only apply to High Impact assets.It would seem logical that the columns in this table should indicate the requirements apply to the same impact level assets, which would be either only High Impact assets, or Medium & High Impact assets, but not a mix.
50.20	Dominion Resources	Disagree	29.2 - 29.5 should be required for Medium Impact to be consistent with R28. R29.2 thru R29.5 currently use text to convey numbers (e.g., sixty vs. 60). This is not

#	Organization	Yes or No	Question 50 Comment
	Services, Inc.		consistent with the convention used throughout CIP-011 and is more difficult to read. A single convention using numerical values should be used throughout.
50.21	Duke Energy	Disagree	Requirement 28.1: is this one test of the cyber incident response plan (global) once per 12 months or is this the test of test of the cyber incident response plan for EACH BES cyber system per 12 months? Once globally per 12 months should be plenty.Requirement 29.5: is the communication of updates a broadcast or is specific feedback from each person required? Remove these requirements for Low Impact.
50.22	EEI	Disagree	EEI suggest that R 28.1 should be modified to be clear that test plans should be exercised annually and not at a per system or per component level.
50.23	Entergy	Disagree	These Requirements should apply for all three BES Cyber System/Component Impact categories.
50.24	Garland Power and Light	Disagree	Requirement 27.1, 27.2, 27.3 and 29.1 - remove from “Low Impact” classification
50.25	ISO New England Inc	Disagree	If the Entity’s Incident Response Plan is tested (instead of testing each BES Cyber System), recommend that “Require” should apply for High Impact, Medium Impact, and Low Impact BES Cyber Systems
50.26	LADWP	Disagree	Table 27 - low impact should not be included.
50.27	Manitoba Hydro	Disagree	Cyber Security Incidents for Low Impact BES Cyber System should not require reporting to the ES-ISAC.
50.28	MidAmerican Energy Company	Disagree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency? 29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is

#	Organization	Yes or No	Question 50 Comment
			considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.29	Minnesota Power	Disagree	With the implementation of the changes discussed in Question 49, these impact levels are generally acceptable.
50.30	National Grid	Disagree	o National Grid recommends deleting 27.3 for Low Impact BES CS o National Grid recommends the timeframes for Medium and High Impact in R28 similar to Table R31 31.1 and 31.2 for consistency.
50.31	Network & Security Technologies Inc	Disagree	Table 27 includes Low Impact systems, but Table 18 (event monitoring) does not. Need to change one or the other.
50.32	Northeast Power Coordinating Council	Disagree	Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.33	Oncor Electric Delivery LLC	Disagree	The Incident Response Plan should be required for the entity, not for every High Impact cyber system. Requirement 29.4, update of Incident Response Plan, we suggest these reviews be conducted quarterly.
50.34	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
50.35	Progress Energy (non-Nuclear)	Disagree	Need to clarify the annual/12 month/365 day issue.
50.36	ReliabilityFirst Staff	Disagree	For R29, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems.

#	Organization	Yes or No	Question 50 Comment
50.37	San Diego Gas and Electric Co.	Disagree	SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly
50.38	Southwest Power Pool Regional Entity	Disagree	28.1 should be applicable to all impact categories. An incident response plan should be tested to verify that it will work when needed. 29.2 through 29.5 should be applicable to all impact categories, perhaps with shorter time frame for higher impact systems.
50.39	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of the previous requirements that did not apply to low systems.
50.40	We Energies	Disagree	We Energies agrees with EEI R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.41	WECC	Disagree	All items should be required for medium impact levels in R29Criteria should apply to all impact levels.

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerns with improving the clarity of the periodic timing requirements, the requirement to reinstall and configure any application and system software using its baseline configuration vs. functionality, and the recognition that a large amount of test equipment will be necessary to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ." .

There were suggestions that the testing requirements should only apply to control centers. Additional guidance was requested for operational testing, the use of redundant sites as an acceptable means to address recovery, and for testing of information that is stored on backup media. The SDT added some information about testing in the Rational Box for the proposed CIP-009-5 R1. Testing is necessary to verify the Responsible Entity's Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Recovery Testing – Operational Test every 36 months should count for the annual test. The SDT notes that there is a FERC directive to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was adopted. Areas of opportunity suggested for modification of the standards by the SDT were to provide recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", and incident recovery plan reviews.

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT should consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised

standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

Several commenters suggested adding definitions for terms such as "initially stored," and the SDT believes that these terms do not have a unique meaning when used in the standard and do not require a formal definition. The team has tried to limit its proposed definitions to those terms that either have a unique meaning when used in a NERC Reliability Standard, or when misunderstanding a word may have a material impact to reliability.

#	Organization	Yes or No	Question 51 Comment
51.1	Dairyland Power Cooperative		30.5 does the system test require a test of every element in the recovery plan? If a recovery plan covers multiple systems, must all systems be tested annually? Or is it sufficient to test some scenarios affecting some systems?
51.2	National Rural Electric Cooperative Association (NRECA)		In R31.1 and R31.2 there are references to "once every 24 months" and "once every 12 months." Please ensure these timeline requirements are clear similar to my comments in Question 49 regarding R29.1.
51.3	SCE&G		R31.3: What constitutes and operational exercise? What is the scope of the recovery and systems to be covered (all high impact cyber systems, or one sample system if the same recovery plan is used acroos all)?
51.4	WECC		Item 31.2 looks like it should be two separate items. Consider making a separate item for "Test any information used..." at the same required level for high impact.
51.5	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
51.6	Florida Municipal Power Agency	Agree	30.5 mentions restoring to the previous baseline configuration, without regard to the fact that the baseline may have been the source of the problem. FMPA suggests "prior", giving the RE the flexibility to restore systems based on what they know to be a working system.

#	Organization	Yes or No	Question 51 Comment
51.7	Independent Electricity System Operator	Agree	- R30.1 Please define Recovery Plan. Some regions are not accepting a backup control center, with redundant systems and data as suffice for recovery and think it means building a component from scratch (ie install os, configuration, install application,
51.8	PacifiCorp	Agree	30.4 - Define “protection of information required to successfully restore”.30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define “secure backups” and “functionality”.31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.Define “initially stored”, “useable and current”. This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking. There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.9	Southern California Edison Company	Agree	The standard should clarify that the time line for the operational exercise that is required by R31.3 is not 36 months for every device is scope, but rather than every disaster recovery plan has to be tested on a scheduled basis.The operational impact of protecting backups at par with operational BES systems is substantial. The backup

#	Organization	Yes or No	Question 51 Comment
			does not support real time BES reliability and should be treated as an ancillary system (i.e. climate control, fire prevention etc.) or similar to systems such as access points and boundary protection devices.
51.10	Alberta Electric System Operator	Disagree	In Table R30, for 30.5, consider changing “known secure backups” to “known good backups” since availability and integrity are more important than confidentiality during system recovery.
51.11	Ameren	Disagree	R30.1 - If you miss listing all conditions or you fail to activate your plan if the certain condition is met makes this difficult to provide complete documentation for an audit. Suggest removal or changing the phrase to "List possible conditions that may activate the recovery plan, update these conditions within 30 days of an actual incident that was not included within the scope of the originally documented conditions."
51.12	American Electric Power	Disagree	31.2: Regarding "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current", should this be a separate line item? It seems out of place in 31.2.
51.13	APPA Task Force	Disagree	The APPA Task Force supports the drafting team’s efforts on System Recovery. We propose the following edits:31.2, recommend changing “once every 12 months” to “Annually.”32.1, recommend changing “once every 12 months” to “Annually.”32.4, recommend changing “once every 12 months” to “Annually.”
51.14	BGE	Disagree	Provide definition of “operational exercise”
51.15	Bonneville Power Administration	Disagree	The objectives of these requirements (“so that BES Cyber Systems can be restored to a defined state,” “to verify recovery plan readiness and effectiveness,” and “to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 51 Comment
			appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R30, Section 30.5 is too prescriptive. For example, one way to do backups is to take a complete image of the system. Restoration becomes merely an issue of restoring that image. There is no need to reinstall and reconfigure. Recommendation: Remove 30.5Table R31, Sections 31.1 and 31.2. There are other ways to test, as well. Testing methods should be devised by the RE, not the standard. The frequency may vary based on the Impact status of the system. However, standardization on the middle ground of at least once every 24 months would simplify compliance.
51.16	Con Edison of New York	Disagree	This criterion should be for control centers or SCADA system only. Many cyber systems which would need to comply with CIP-011 do not have back-ups. The BES can be operated effectively even if other cyber systems are down.
51.17	Constellation Energy Control and Dispatch, LLC	Disagree	Provide a definition of operational exercise.
51.18	Constellation Power Source Generation	Disagree	R31.3 uses the term “representative environment.” At the CIP V4 Workshop, the team stated they used this vague term to give entities flexibility in their operational exercises, but this is not auditable.
51.19	Consultant	Disagree	Table R30 Item 30.5 - First bullet - Suggest changing the word "defined" to "documented" or "identified" or "identified and documented". R23 does not define the baseline.Item 30.5 - Second Bullet - Suggest deleting the words "any" & "most" & "known" & "secure" New wording: "Load information from recent backups." Suggest deleting this bullet. Reloading backup date should be an operational decision made based on the conditions that exist at the time of recovery, and not "forced" by a requirement.Table R32 - Item 31.2 This is two requirements. Suggest separating each into it's own line item.Table R32 - The periodicity requirements of this table should be adjusted. The testing and operational exercise statements are not consistent with the

#	Organization	Yes or No	Question 51 Comment
			incident response plan requirements. Suggest making the requirements for incident response plans and recovery plans consistent.Item 32.2 & 32.3 Suggest changing the word "execution" to "occurrence".Item 32.5 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 32.7 Suggest deleting the word "all" as an unnecessary word.
51.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R31.2 the term “current” is not valid if any data has changed since the backup. A backup completed 12 months earlier could never be considered current on an operational system. Consider removing this term.
51.21	Detroit Edison	Disagree	Table 31.2 and 32.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.Table 32.4 should not be an annual update but should be triggered on the required review in 32.2. Consider revising to a sixty day window after the review.Table 32.6 The term "any" is too broad. Consider revising to read "...changes that impact the recovery plan."Table 32.7 Revise "recover" to "recovery"
51.22	Dominion Resources Services, Inc.	Disagree	30.2. The phrase “including identification of the personnel responsible” should be removed from this requirement. Roles and responsibilities should be adequate for the plan. There should not be a need to list 20 relay technicians that could be allowed to recover a substation system. 31.2. The second paragraph of this requirement should be revised to state “Verify BES system can be restored from backup initially and at least annually thereafter”.32.1. The phrase “or when BES Cyber Systems are replaced” should be changed to “or when impacted by BES Cyber System changes.”32.6. The phrase “technology changes” should be changed to “technology changes that impact the recovery plan.” (e.g., not all organizational changes affect the recovery plan.)32.7. The word “recover” should be changed to “recovery”.

#	Organization	Yes or No	Question 51 Comment
51.23	Duke Energy	Disagree	Table 30:30.2 remove “including identification of the personnel”30.3 change ‘personnel responsible’ to “responders”30.5 CIP should not prescribe HOW we restore the system. Suggest removing and adding ‘restoration’ to the list in 30.4Table 31:31.1 multiple plans may be required. Same comment as 28.1 above. Is this once per 12 months per the plan or once per 12 months for each BES cyber system? Suggest allowing 12 months per plan to test.31.2 specify that verifying backup media functionality is an acceptable test.31.3 operational exercises at some generation stations may be unrealistic (unrealistic for availability or costs)Table 32:32.6 this should be part of change managementSuggest allowing 12 months per plan for review.Remove ‘incident’ from 32.2 and 32.3
51.24	EEI	Disagree	Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.25	Emerson Process Management	Disagree	It seems there is a conflict between 31.2 and 31.3. If the operational exercise needs to be donw every 36 months per 31.3, then, it should not be needed again every 12 months per 31.2.
51.26	Entergy	Disagree	Entergy agrees for High and Medium Impact Cyber Systems it is important to be able to recover and demonstrate that the recovery plan and backup media used in the process is sufficient to recover the BES Cyber System however, requirement 31.2 and 31.3 appear to be a little redundant although not completely. In requirement 31.3 the entity is required to demonstrate recovery in a representative environment where 31.2 only the backup media is required to be verified as useable and current. Both of these activities provide validation that data can be recovered from the backup media. Requirement 31.3 should be deleted - testing the plan every 12 months either via paper drill or full operational exercise or actual incident coupled with validating the backup media is readable is sufficient to the demonstrate recovery. Requirement 31.1 should be change to include: “Testing any information used in the recovery of

#	Organization	Yes or No	Question 51 Comment
			the BES systems that is stored on backup media when initially stored and at least every 24 months to ensure that the information is useable and current."
51.27	ERCOT ISO	Disagree	30: Request that the use of redundant sites is an acceptable means to address recovery.30.2: Recommend noting what information is necessary here. Are group notifications considered sufficient (e.g., on-call rotations)? 32.2: Should be 30 days rather than 60 days to align with FERC Order 706.
51.28	FirstEnergy Corporation	Disagree	R31 - 31.3 - Need clarity on what is meant by 'Operational' exercise. We believe the intent was business operations, not IT system operations and related DR plan recovery. A business operational exercise is a business continuity planning issue. (example: EMS Operation hot-site testing) Sub-requirement 31.3 would need to be answered by each business unit and not within an IT DR Team response as business operational (BCP) tests are not performed for DR Plans. DR Plans have physical and media type testing which it appears to be what the intent was for 31.1 and 31.2. Need clarity on ownership. It seems like 31.1 and 31.2 are owned by IT, and 31.3 is owned by business units. R32 - 32.6 - We do not agree with changing names in individual recovery plans except during the annual review. Normally organization changes affect the recovery plan approvers list and if changed, would require re-approval of the DR plan. Given the complexity of our critical DR plans, this requirement is not reasonable, and certainly not within a 30 day window - especially if the new name is for someone just starting in a position. We agree that interim organizational changes could be made for call trees of 'personnel expected to respond to/perform a recovery using the recovery plans', but call trees are not part of the individual recovery plans and are instead part of an overall recovery plan. R32 - 32.7 - Recovery is misspelled ('communicate all recover plan...')
51.29	Garland Power and Light	Disagree	Requirement R30 requires the implementation of the plan to be in compliance - Concern is that for some business reason (perhaps a certain business strategy or the economy) some system or facility might not need to be rebuilt. There should be a provision for the Responsible Entity to provide justification to Regional Entity for not

#	Organization	Yes or No	Question 51 Comment
			rebuilding and not be in violation for not implementing and actually rebuilding the "whatever" that failed.
51.30	GE Energy	Disagree	36 months is too long between operational recovery exercises. This should be at maximum 24 months, and should require re-validation if a large system configuration change is made, such as hardware changes, version upgrades, or 3rd party software upgrades.
51.31	GTC & GSOC	Disagree	We recommend R32.1 be changed to the following: "Review and update recovery plan(s) at least once every 12 months or when a Cyber Security Incident recovery of BES Cyber System(s) does not effectively proceed according to the documented plan."We recommend the word "incident" be replaced throughout R30 through R32 with the words "Cyber Security Incident"
51.32	Hydro One	Disagree	Recommend changing the bullets for 30.5 to start with "plans for". The first bullet should be "install" not "reinstall." The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.33	ISO New England Inc	Disagree	31.2 - "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. "impossible to test " - is this to test if your backup works and is usable? Realtime data is never restored - clarification on information and is this test your media for usability? "Test when initially stored"?? Not feasible. More appropriate Verify backup completed successfully, not verify data that was backed up. Control Centers utilize full functioning backup facilities for recovery from the main center being compromised and or rendered unavailable, so for control centers the recovery should be to run from the backup control center once a year. The media should be tested on an annual base to make sure that the data from the offline storage is still recoverable. For facilities that do not have a backup BES cyber systems then I would agree that they need to recover in the way stated. Recommend changing 30.5 bullets to start with "plans for". The first bullet should be "install" not

#	Organization	Yes or No	Question 51 Comment
			"reinstall." Recommend that the recovery plan does not need to include non-BES Cyber Systems. Recommend that the third bullet should test the BES Cyber System Component(s).
51.34	LADWP	Disagree	CIP-011-1 R30 Cyber System Recovery (CSR) should not require to document identification of the personnel responsible for recovery effort (R30.2) within the CSR. Identification of specific personnel will lead to revision of the document when personnel are reassigned.
51.35	Manitoba Hydro	Disagree	The wording of Requirement R31.1 should be revised as the phrase "with a paper drill" could be misinterpreted. There are no specifics given with respect to the Requirements of R30 (in terms of "conditions", "roles and responsibilities", etc., so it assumed to be at the Responsible Entity's discretion in terms of criteria, etc. Consider whether Requirement R31.2 should be two separate Requirements - R31.2 with respect to "Conduct a test..." and R31.3 with respect to "Test any information...". There are no specifics given with respect to "demonstrates readiness" in Requirement R31.3 so it assumed to be at the Responsible Entity's discretion as to whether the test has demonstrated readiness or not. The word "recover" in Requirement R32.7 should be "recovery".
51.36	MidAmerican Energy Company	Disagree	Define "protection of information required to successfully restore".30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define "secure backups" and "functionality".Define "initially stored", "useable and current". This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is

#	Organization	Yes or No	Question 51 Comment
			introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R30, but recommends that the Standards Drafting Team consider defining the term "known secure backups" as it is not currently defined in the Standard and is open to interpretation. Part 31.2 requires that data be "tested" at the time of backup and every 12 months to ensure that it is "useable and current" and to ensure consistency with that requirement, Minnesota Power recommends that the Standards Drafting Team replace "known secure" with "useable". Minnesota Power generally agrees with the proposed Requirements R31, but recommends that the Standards Drafting Team further define what is meant by "test" data stored on backup media to "ensure that the information is useable and current" in Part 31.2. While testing usability can be done by verifying one can read the tapes' contents, how does one test that data is current? This would require more of a manual verification or comparison function than a test, correct? In addition, is R31.3 requiring a full restoration, or is it requiring that each scenario documented in the Restoration Plan be fully tested every 36 months? Minnesota Power recommends that the Standards Drafting Team revise the wording of Part 31.3 to eliminate confusion regarding their intent.Minnesota Power generally agrees with the proposed Requirements R32, but to be consistent with the "update" portion R32, Minnesota Power recommends that Part 32.1 be modified to state "Review the recovery plan(s) at least once every 12 months, or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements."Minnesota Power generally agrees with the proposed Requirements R32, but recommends that the term "recover" be

#	Organization	Yes or No	Question 51 Comment
			changed to “recovery” for Part 32.7.
51.38	National Grid	Disagree	National Grid recommends changing 30.5 bullets to start with “plans for”. The first bullet should be “install” not “reinstall.” Also recommends that the recovery plan does not need to include non-BES Cyber Systems and that the third bullet should test the BES Cyber System Component(s).
51.39	Network & Security Technologies Inc	Disagree	30.5 - Suggest revising to require use of either baseline configuration or most recent known “good” configuration. Covers the possibility a (new) baseline configuration is causing problems (can and does happen - even if tests pass).30.5 - Need to define what “secure” backup means.31.2 - Requirement to test information “when initially stored” may be extremely burdensome in some environments, depending on backup mechanisms used. Some types of backup systems use on-the-fly techniques to verify a copy/write operation is “good” but SDT should use language that is less prescriptive. Should also drop the word, “current.” Certain types of operational data will cease to be “current” moments after it is copied. Only real-time mirroring can satisfy this requirement and entities should not be compelled to implement it.
51.40	NextEra Energy Corporate Compliance	Disagree	NextEra believes the CIP-011-1 Table R30 - Recovery Plan Specifications so that BES Cyber Systems can be restored to a defined state did not provide enough guidance and left room for interpretations.The following are the recommended updates:30.1 - The Responsible Entity shall define conditions for activation of the recovery plan(s).30.4 - Processes and procedures for the backup, storage and protection of information required to successfully restore a BES Cyber System30.5 - Implement a test plan to identify the processes and procedures for the restoration of BES Cyber Systems to include the following: o Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, o Load any information from the most recent, known secure backups, o Conduct a system test to verify functionalityModified the wording and additional guidance should be provided by NERC on the minimum conditions which would activate the plan.NextEra also believes that Table R31 - Recovery Plan Testing Specifications to verify recovery

#	Organization	Yes or No	Question 51 Comment
			plan readiness and effectiveness did not talk about documenting test resultsThere should be documentation of test results to validate that it was performed. The following are the recommended updates:31.1 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months. All testing results shall be documented.31.2 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. All testing results shall be documented.31.3 - Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness. All testing results shall be documented.In 30.5, the recovery plan expands the current backup and restore of any application and system software using its baseline configuration. Is the definition of baseline the current or previous version of an application and system software?In 31.2, does the testing of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored to ensure that the information is useable and current require the Responsible Entity to "load back" the data that is stored on backup media to an operational system to prove usability? Is loading it back to a test environment sufficient?In 31.2, "Test any information used in the recovery of BES Cyber systems." Does the requirement imply that in the case of protective relays at a BES Transmission Facilities, the backup settings file for every protective relay at High Impact facilities should be tested every 12 months?
51.41	Northeast Power Coordinating Council	Disagree	Recommend changing the bullets for 30.5 to start with “plans for”. The first bullet should be “install” not “reinstall.” The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.42	Oncor Electric Delivery LLC	Disagree	These requirements are unnecessarily burdensome. Entities have been recovering from man-made and natural disasters for many years without these requirements.

#	Organization	Yes or No	Question 51 Comment
			Entities should be able to leverage Business Continuity, High Availability architectures and Standardization to demonstrate their ability to recover from unforeseen events. Requirement 32.6, update of Recovery Plan, we suggest this review be conducted quarterly.
51.43	Progress Energy - Nuclear Generation	Disagree	Agree with R30 and R31. Disagree with R32. Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments for consistency in regulation for R30-32.
51.44	Progress Energy (non-Nuclear)	Disagree	R30.5 the first bullet should not be a requirement based on the second bullet.
51.45	Regulatory Compliance	Disagree	30.5 - STTRKE all the bullet points. Recovery plan should be system wide. Test restoration annually - document processes.31.2 - Make the second item a separate criteria line item - it's too confusing the way it is currently written. "Required" for High Impact.32.2 - "Annually" review the results.....
51.46	ReliabilityFirst Staff	Disagree	For R30, change “or failure” to “failure, or destruction.” For 30.4, please clarify what is meant by “successfully restore”. For R30.5, please clarify what is meant by “known secure backups”. For R31.3, change “incident response” to “activation of the recovery plan”. For R32, delete “relevant” so all changes are communicated. For R32.7, change “recover” to “recovery”.
51.47	ReymannGroup, Inc.	Disagree	R30.4 should be expanded to include processes for the recovery, restoration, and protection of data from a damaged or failed BES Cyber System. R30.5 should be expanded to include a review to ensure that malicious code has not been installed on the recovered files or device.
51.48	RRI Energy	Disagree	What constitutes a representative environment?

#	Organization	Yes or No	Question 51 Comment
51.49	San Diego Gas and Electric Co.	Disagree	R30 - R32 were originally covered in CIP-009-3. Referencing Table R30 - SDG&E suggests that R30.4 and R30.5 be removed. The IT Disaster Recovery Plan covers this and it would not normally be part of our Business Continuity Recovery Plan. The Responsible Entity (RE) should not be required to develop Recovery Plans with detailed IT processes for storage, backup, protection and reinstallation of software, etc. Referencing Table R31 criteria 31.3, SDG&E suggests that this wording be changed. CIP-009-3 R2 provides the RE with more options for "exercising" the recovery plan and we prefer the way the Requirement is worded in CIP-009. Referencing Table R32, CIP-009-3 R3 provides the RE more options when developing plans and procedures to comply with the Requirements. The new table seems to hold the Entities (both Medium and High) to several compliance timetables that are extremely restrictive. SDG&E suggests that we utilize the same wording for this Requirement from CIP-009-3 R3.
51.50	Southwest Power Pool Regional Entity	Disagree	R30: Is a recovery plan required for each BS Cyber System or is a generic plan acceptable? Recovery plans need to range from device component failure to catastrophic failure (e.g. physical facility disaster). 30.2: Is the identification by individual name or by position title? 30.5: What is meant by "secure" backups? Encrypted? Securely stored? Something else? Also, the backup and restoration processes should be "as applicable." Not all recovered systems are restored from a "backup." 31.2: Does the requirement to test backup media when initially stored apply to every daily backup, or only after BES Cyber System updates? Does the test include a restoration to an offline environment to verify the backup is not only readable but also complete? 31.3: Clarify that the operational exercise is more than a system or site fail over (NERC Standard EOP-008 exercise) but must also include performing the necessary steps to recover from the failure and restore the failed systems to normal operation by following the steps of the plan. 32.1: Include BES Cyber Systems that are significantly updated / upgraded requiring an update to the recovery plan. 32.4: Require the update within a much shorter time following determination of the need through the methods defined in the criteria. Delayed

#	Organization	Yes or No	Question 51 Comment
			updates are at risk of being overlooked and out of date plans pose a risk to the entity's ability to quickly recover. 60 days is recommended.
51.51	USACE - Omaha Anchor	Disagree	A) 30.5 - how often must system test be conducted? B) 31.2 Clarify "initially stored" is this the first time the tape is used?C) 32.6 - this could be interpreted to require a change in the recovery plan every time a software change occurs. This is very extensive - and unrealistic. Potential verbiage could be 'whenever system, organizational, or technology changes effect the recovery plan.'
51.52	We Energies	Disagree	We Energies agrees with EEI: Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.53	Xcel Energy	Disagree	Definition is needed as to what constitutes an "operational Exercise". Is this a table top drill, or something more.

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerned improving the clarity of the periodic timing requirements and the large amount of test equipment it would take to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ."

There were suggestions that the testing requirements should only apply to control centers as Recovery Plans apply to Medium & High Impact Level categorizations, while some aspects of the recovery plan may only apply to High Impact assets. Additional guidance was requested for operational testing and for testing of information that is stored on backup media. The SDT added some information about testing in the Rationale Box for Requirement R1 in the revised CIP-009-5. Testing is necessary to verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Issues identified in comments for SDT consideration were Recovery Testing – Operational Test every 36 months should count for the annual test, recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", coordination of physical aspects of Cyber Security Incidents, and incident recovery plan reviews. The SDT notes that there are FERC directives (e.g., P686, P687, P725) to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was not adopted. (CIP-009-5 R2)

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

	Organization	Yes or No	Question 52 Comment
52.1	Alberta Electric System Operator	Agree	There appears to be a typo in 32.7 - "Communicate all recover plan updates" - recover should be recovery.
52.2	Emerson Process Management	Agree	In reality, it would be a good practice to exercise recovery plan during or toward the end of each scheduled unit outage for generation.
52.3	Florida Municipal Power Agency	Agree	FMPA suggests changing “12 months” to “annual” and “24 months” to “biennial”
52.4	PacifiCorp	Agree	31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.
52.5	American Municipal Power	Disagree	Please provide a little or no impact category
52.6	American Transmission Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.7	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on impact levels and therefore proposes the following changes:R31 Table 31.3: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyThe APPA Task Force agrees with the impact levels for the rest of R30-R32 if it is understood that a blank in the table means N/A.
52.8	BGE	Disagree	R30 - R32 should synchronized with R29 to include both Low and medium impacted

	Organization	Yes or No	Question 52 Comment
			BES Cyber Systems.
52.9	Black Hills Corporation	Disagree	30.4 should also apply to Medium Impact systems. Without this basic information, recovery would have to start from scratch.
52.10	Bonneville Power Administration	Disagree	Table R32Sections 32.2 and 32.3. Both should allow 60 days for review.Section 32.4: 12 months is too long. No more than 6 months should be allowed. Items 31.1 through 31.3 in Table R31 and 32.1 and 32.4 in Table R32 states certain events must occur "at least once every 12, 24, or 36 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently the events referenced above must occur.
52.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
52.12	Con Edison of New York	Disagree	See 51
52.13	Consultant	Disagree	Table R30 - It doesn't appear to make sense that the Recovery Plans applies to Medium & High impact level categorizations, while aspects of the recovery plan only applies to High Impact assets.Table R31 & R32 - How many test and exercises are required? The structure here will create an administrative burden to track what was done when that has no corresponding risk reduction.Mixed requirements would force multiple recovery plans based on categorization of assets, which could mean two recovery plans for the same asset type where the application of each asset has a different impact categorization. This does not appear to be a sensible approach to recovery plans.Suggest deciding on a consistent set of requirements that can be applied equally to High Impact and Medium Impact assets.
52.14	CWLP Electric Transmission, Distribution	Disagree	R32.6. In order to meet the required change management process in R23 this window should be extended to 60 days.

	Organization	Yes or No	Question 52 Comment
	and Operations Department		
52.15	ERCOT ISO	Disagree	All requirements should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
52.16	FirstEnergy Corporation	Disagree	R32 - Combine R32.5 and R32.6 and eliminate the word 'organizational'.
52.17	Garland Power and Light	Disagree	Requirements 30.1 & 30.2 - remove Medium Impact classification
52.18	ISO New England Inc	Disagree	32.6 - clarification on scope of "any" technology and system change scope. (organizational change is fine). R32.7 spelling "recover" should be recovery? CIP Standard use of the term "annual": The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next.
52.19	LADWP	Disagree	Medium Impact should not be a factor.
52.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
52.21	Manitoba Hydro	Disagree	Medium Impact BES Cyber System should be included as "Required" in sections 30.3 to 30.5
52.22	MidAmerican Energy Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous

	Organization	Yes or No	Question 52 Comment
			disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.23	MRO's NERC Standards Review Subcommittee	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.24	Oncor Electric Delivery LLC	Disagree	Verification of the entity's Recovery Plan for High Cyber Systems every 12 months should cover Requirement 31.1. This should require only one test for the entity - remove low/medium/high)
52.25	Progress Energy (non-Nuclear)	Disagree	See comment 14.What is meant by an operational exercise in a representative environment? Does it mean individual components that can be easily tested for recovery plans?
52.26	ReliabilityFirst Staff	Disagree	For R30, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems. For R32.6, should be "Required" for "Medium".
52.27	San Diego Gas and Electric Co.	Disagree	SDG&E would agree with Table R30 if item 30.5 were to be removed. Similarly, SDG&E would agree with Table R31 if item 31.3 were to be removed. Referencing Table R32 - SDG&E prefers the wording in CIP-009 R3 in this area because it provides more flexibility for the Entities while still covering the issues.
52.28	Southern California Edison Company	Disagree	The drafting team should state in CIP 010 that back-up systems should be treated at par with system key to real time BES reliability if the intent of this requirement is that CIP-011 be applied to all BES systems.
52.29	Southwest Power Pool	Disagree	30.3, 30.4, and 30.5 should be applicable to Medium impact systems. 32.6 should be

	Organization	Yes or No	Question 52 Comment
	Regional Entity		applicable to Medium impact systems with perhaps a 60-day update timeframe.
52.30	The Empire District Electric Company	Disagree	Comments: Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.31	WECC	Disagree	All items should be required for medium impact levels in R30Criteria should apply to all impact levels.

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

Summary Consideration:

Some commenters stated that the requirements should be written around the specific device types. The drafting team considered this option, but believes that it becomes problematic for entities and auditors to determine when a device is multi-purpose versus purpose-built. Some purpose-built devices can be considered multi-purpose depending on how the device was manufactured and implemented.

A variety of comments were received regarding the TFE process and its applicability to the specific CIP Cyber Security requirements. While the TFE process itself was outside the scope of the drafting team's work, commenters stated that TFEs should be allowed for passwords, malicious code monitoring, system hardening, system event monitoring, wireless and remote access, as well as for communications and data integrity. The drafting team considered these comments and revised the requirement text where necessary to allow entities more flexibility in implementing these requirements thereby reducing the need for TFEs. In some cases, the requirement was removed or written at a system level to prevent the need for TFEs.

#	Organization	Question 53 Comment
53.1	Detroit Edison	14.4, 17.1, 17.2, 16.2, 10.1-10.8 should retain TFE status.
53.2	Network & Security Technologies Inc	19.1 (see comments on Question 35), 26.2 (see comments on Question 47)
53.3	ISO New England Inc	Actual language on several requirements need to be clarified, many are still open to interpretation which may lead to TFE's.
53.4	EEI	Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.

#	Organization	Question 53 Comment
53.5	Progress Energy - Nuclear Generation	All CIP 011-1 Requirements should contain provisions similar to NIST 800-53, Regulatory Guide (RG) 5.71, and NEI 08-09, Revision 6, CIP standards should provide for nuclear facilities' use of alternative methods which implement security controls equivalent to those required by CIP. Nuclear programs, required by regulation, currently in place at nuclear facilities provide these alternate methods. Technical Feasibility Evaluations (TFE) should not be required with such documentation. One example is that nuclear facilities have one of the most effective Physical Security Programs of Critical Infrastructures. CIP-011-1 requirements R5 and R6 should acknowledge nuclear generating station physical security programs.
53.6	Ameren	All of the following requirements would need a TFE o R10 for passwords complexity o R14.4 for user banners o R15 for malicious code protection o R16 for installing patches o R18 for logging security events o R19 for validating data inbound o R23.7 for monitoring changes to a baseline configuration.
53.7	US Army Corps of Engineers, Omaha Distirc	All requirements that require existing hardware and software be capable of performing any function should allow for the possibility of TFE's. Sections R10, R15, R17, R18, R19, & R23 have requirements that are likely to require TFE's.
53.8	Southwest Power Pool Regional Entity	Any time a requirement specifies "continuous", "all", or prescribes a specific solution or characteristics of a technical solution, a TFE may be necessary. Try to avoid specific technology requirements as discussed elsewhere in these submitted comments.
53.9	The Empire District Electric Company	Comments: See comments under questions 34, 35, and 37.
53.10	RRI Energy	Cyber assets that are not on your standard IT equipment list are the most likely devices to need TFEs. This list could include meters, vibration monitors, PLCs, DCS, RTUs, cpu based test equipment.
53.11	E.ON U.S.	E.ON U.S. believes that many of the requirements remain ambiguous and additional clarity is needed. Absent such clarity it is difficult to ascertain where TFE ability can be eliminated. In fact, the proposal to provide greater compliance flexibility for responsible entities makes this determination even more difficult. As the requirements currently read, E.ON U.S. believes that more, not less, TFE requests will

#	Organization	Question 53 Comment
		result. Areas where responsible entities have requested additional clarity need to be addressed prior to issuance of a final industry draft. The informal comment period does not provide an adequate forum to identify all areas of concern and suggest specific replacement language.
53.12	Cogeneration Association of California and Energy Producers & Users Coalition	Entities should be able to use TFEs for any instance where unsupported technology is in place that may not be compliant with CIP-011 requirements due to age or vendor proprietary technology. Patches, updates, virus scanning, or firewalls may not be available for older, unsupported technology. An entity should not be required to upgrade or replace a system that currently satisfies the needs of the entity. The entity should be able to use other mitigation methods to protect a system if patches, updates, virus scanning, or firewalls cannot be applied.
53.13	Northeast Utilities	Equipment that never has security software patches or virus protection should be exempt. Also, those cyber assets that do not have user authentication capabilities should be exempt from password requirements.
53.14	ERCOT ISO	ERCOT ISO supports the proposed form of combining all requirements into a single reliability standard. The use of a single standard will eliminate the need for cross-referencing to other reliability standards. ERCOT ISO does request a realignment of some requirements. All requirements for access authorization, revocation, and review should be combined to eliminate confusion of how access should be managed.The timing of updates to documentation should be consistent throughout the requirements. Recommend the use of 30 days to be in compliance with the directives of FERC Order 706.
53.15	Bonneville Power Administration	If the standards present the overall security controls required, and do not attempt to dictate how those controls are accomplished, there should be no need for TFEs.If there is a need:First, the TFE process as presently constituted has shown to be cumbersome, not well understood, and inflexible. Neither NERC nor The Regional Entities have the detailed internal system knowledge or manpower to do make an intelligent judgment. At best, they can make a broad, industry best guess. The TFE approval process belongs within the Responsible Entity, at a technical level where there are people who know the environment, the systems, and their capabilities can evaluate them. They should be audited as part of the normal compliance audit.Second, if a system will not, or can not perform a

#	Organization	Question 53 Comment
		required function, it should be up to the RE to determine what steps should be taken to meet the standard. Third, because there are so many ways to accomplish the security of systems, the only time a TFE should be necessary is when all methods have been exhausted that could provide a level of protection required.That being said - Any time a situation arises where for technical reasons, or because implementation of security features may present BES reliability issues, or where application of one security measure would compromise others, the RE should have the authority to choose how to proceed. If this is called a TFE, the RE should approve it and document it as part of the overall security planEven if TFEs with approval required by the REs or NERC are used under CIP-010 and CIP-011, the process needs to be revised. As examples:1. There needs to be an opportunity for entities to appeal or request reconsideration of a rejection of the initial submission. Under the current, at best they can resubmit one time to correct errors.2. It should be possible to submit TFEs under multiple justifications.3. There are claims that the regional entities have been instructed to reject any TFEs other than those based on legacy equipment. If true, this violates the process, which allows TFEs for both new and legacy systems. It is also unreasonable: there are still systems today, and will be for the foreseeable future, that may be the best overall solution for reliable operation of the grid but which do not allow full compliance. Having said that:10.6 may not be possible for all systems. For overly simplistic example, routers intended for small office/home office use often allow either full access or no access. If all that is necessary is to review a log, full administrative access is overkill. To avoid the need for a TFE, recommend "To the extent possible for the particular device or system, require that authorized..."10.8. Same comment as 10.6.14.2. Unless the definitions of external connectivity and/or remote access or change, 14.2 may not be possible in every instance. For example, consider a legacy multi-user system in a Control Center that is not capable of multi-factor authentication. Any access from a system not part of the BES Cyber System containng the legacy system would constitute remote access and require multi-factor authentication for a High Impact system. It is not clear from R14 whether that multi-factor authentication is required at the BES Cyber System itself or at the access point. If it is required at the system itself, then a TFE would be required. Recommendation: Redefine external connectivity and remote access as described above. Multi-factor could then be required clearly at the external access point.14.4. It is not always possible to display an appropriate use banner under such circumstances. As an example, consider remote connection using a VPN. The access point in that case would the device at the endbound end of the encrypted tunnel. The user never sees a

#	Organization	Question 53 Comment
		screen on that access point, and therefore sees no such banner. Recommendation: See the suggested revisions to 14.4 R19. For both 19.1 and 19.2, validation might not be possible. In particular, commercial off the shelf software (COTS) may or may not provide such validation. If the COTS is the best solution otherwise, a TFE would be required.
53.16	Public Service Enterprise Group companies	Implementation of requirements 10 (Response to Question 24), 13(Response to Question 32), 23.7 (Response to Question 40) and 26.2 (Response to Question 48) may not be feasible in all situations. Please see comments in the questions that relate to these requirements for description of the potential infeasibility.
53.17	Idaho Power Company	In R19, data validation and encryption may in some control center applications, introduce a data latency that renders the application degraded or useless and may result in a more secure environment but less reliability. In R19.2, I am unaware of technology that can determine whether invalid data has been maliciously compromised. Most EMS/SCADA systems which would be the most common BES cyber system in a control center filter or ignore invalid data anyway and I do not see that the benefit of this requirement outweighs the technology investment needed to meet this requirement.The ability to alert on unauthorized access attempts may require a TFE depending on the boundary device that is protecting the system. Some boundary devices do not lend themselves to providing alerting and may require a TFE until they are replaced with a device that can meet this requirement.
53.18	Lincoln Electric System	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
53.19	MidAmerican Energy Company	MidAmerican Energy agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.20	Minnesota Power	Minnesota Power recommends that the following requirements should still be eligible for Technical Feasibility Exceptions:Requirement 8, Part 8.3:Depending on the definition of “monitor the use,” it may be impossible to do this for many devices. For example, for Windows computers, how does one monitor the use of someone when much of the interaction involves mouse clicks? Will software be

#	Organization	Question 53 Comment
		required to log, not just keystrokes, but mouse clicks? Further, certain devices do not even maintain an audit trail of logins/logouts (e.g.: networked KVMs for remote console access to servers to allow for efficient system administration).Requirement 10, Part 10.2:While this is certainly good IT Security practice, implementing this on every BES Cyber System could very well put the reliability of the BES at greater risk. Since there is no way to change all passwords in all the various devices simultaneously, especially in a utility that is geographically distributed and remote, this will result in a continual need to change passwords. As a result, it could become commonplace for technicians and engineers to not know/remember what password to use on what device. Not only will this keep them from accessing devices at potentially critical times to perform needed maintenance, but EVERY failed login attempt will then have to be investigated in detail. This could be minimized by requiring this for only Medium and High Impact systems.Requirement 10, Parts 10.4 and 10.5:It is quite probable that devices exist that cannot meet these requirements.Requirement 10, Parts 10.8:It is quite probable that devices exist that do not allow for the creation of accounts, whereby all functions must be performed from the system/admin account(s).Requirement 15:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the installation of malware-prevention software, Requirement R15 would be not technically feasible.Requirement 18:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the security event logging, R18 would be not technically feasible.Requirement 19:The way this is written, the requirement is likely technically infeasible for most any system. To correct, Part 19.1 could be changed by replacing the word “Validate” with “Encrypt”.Requirement 23, Part 23.7:This implies detecting changes that have occurred outside of the approved methods of Parts 23.3-23.6. As such, not all devices may support the installation of software that would allow for such monitoring.
53.21	Progress Energy (non-Nuclear)	Need to include language that allows for procedural controls - example as for password requirements which cannot typically be enforced technologically.
53.22	WECC	No requirements should be so prescriptive to required a TFE. The SDT has done a good job in rewriting requirements to describe WHAT is required without describing HOW it must be achieved.It is impossible to draft standards language that anticipates all possible limitations for implementation.

#	Organization	Question 53 Comment
		The standards, or Rules of Procedure should allow for exceptions to any requirement if an entity could provide justifiable basis and acceptable alternative controls.
53.23	Nuclear Energy Institute	Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.24	PacifiCorp	PacifiCorp agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.R10 - equipment still exists in the field that cannot meet the requirement of a 6 character password. R14 - equipment still exists in the field that cannot meet the requirements.
53.25	Dominion Resources Services, Inc.	Please see Dominion's responses above suggesting the addition of footnotes to avoid required TFEs for requirements 10.8, 14.4, 15.2, 15.3, 18.2, 26.2.
53.26	Puget Sound Energy	Puget Sound Energy suggests Table 10, Table 18, and Table 22 as inclusive for TFE eligibility for the following reasons (also stated in those sections):Table 10 - Puget Sound Energy suggests including "Where Technically Feasible" to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing "continuous security monitoring that issues alerts".Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.
53.27	FEUS	R10: Access Controls; some legacy systems do not allow for default factory accounts to be changed; some legacy systems only allow for a single level of access.R14: For systems not connected to an external network that use Dial-Up access for remote support multifactor authentication may not be technically feasible. Keeping some systems/networks separate from an external cooperate network can reduce cyber vulnerabilities.

#	Organization	Question 53 Comment
53.28	Southern California Edison Company	R7.2: Enforcing this control may be limited by the technical capability of a SCADA device. A device such a PLC that has preset accounts forces the RE to develop acceptable use for a set of accounts retroactively rather than have the capability to limit the account types.R10.4 and R10.5: There are SCADA devices in service that are not at the end of their service life that do not offer this capability. R15.1, 15.2 and 15.3: While these capabilities may be possible at the electronic boundary, individual SCADA devices may not support this functionality. Strict compliance is restricted by technical limitation.R17.1: The mitigation plan that is suggested should be a part of a formal technical feasibility exception program.R28.1: The phrase "or a full operational exercise" is expected to result in technical feasibility exceptions since this will require test data/ setting to be loaded onto in-service SCADA systems.
53.29	Alliant Energy	Recommended changes for any TFE program implemented:Security patch TFEs should be programmatic and not based on individual patch releases.Cyber Asset counts should be stricken. Approved changes to the environment create an immediate ad-hoc obligation for TFE update to the RRO for what is already a burdensome process.Quarterly updates should be removed and replaced by re-approval on an annual basis by the Sr. Manager or delegate.NERC should create a standard Class-Type list as originally proposed.
53.30	USACE HQ	Requirements 10, 14.4, 15 and 17, among others, should have a TFE.
53.31	San Diego Gas and Electric Co.	SDG&E recommends that the TFE processes be changed and incorporated into the Vulnerability Management Process; where the Entity would identify, track, and mitigate any TFEs as a Vulnerability. This methodology will streamline and enhance the TFE process and thereby 1) allow Entities to manage their TFE's internally, 2) reduce Entity, NERC, Reliability Coordinators and Regional Reliability Organization resource requirements, 3) reduce paperwork, resources, and overhead, 4) reduce the potential for errors or leakage of secured information, 5) enhance the audit process and 6) standardize and clarify the process across all Entities.
53.32	BGE	See comments for R13 under Q31-31 and R23 comments under Q40-41.

#	Organization	Question 53 Comment
53.33	MRO's NERC Standards Review Subcommittee	See comments under questions 17, 34, 35, and 37.
53.34	American Transmission Company	See comments under questions 34, 35, and 37.
53.35	Florida Municipal Power Agency	See comments under R7, R14, R16, R23, R20
53.36	CenterPoint Energy	See references to possible TFE issues in comments above.
53.37	SCE&G	Similar to RG 5.71 and NEI 08-09, allowances should be provided for use of alternatives to the required security controls. Alternate controls would be justified and documented that the Threat Vector has been mitigated. TFEs are administartively burdomesome and currently require annual certification and ultimate elimination. The scope of equipment eligible for TFEs will drastically increase the number of filed TFEs, especially for eligble requirements with low impact categories. The SDT needs to consider the feasibility and practicality of implementing the current TFE process with these standards.
53.38	ReliabilityFirst Staff	Table R10, requirements 10.1 and 10.2, Table R14, requirement 14.4, requirement R15, Table R19, requirement 19.2.
53.39	Consultant	Technical Feasibility Exceptions should be allow for any requirement. There are about 2,000 registered entities. Trying to address every configuration of every asset across that spectrum would result in either the requirements being written in a convoluted and confusing manner to address the multiple configurations or being written with little detail to allow the multiple configurations, neither of which could even approach a "bright lines" concept of the requirements. The Technical Feasibility Exception should include a technical basis that shows implementing the specific requirement as stated would not achieve the requirement objective, or improve the security position as it relates to the requirement objective.The Technical Feasibility Exception process probably needs to be improved to deal with exceptions as described here.

#	Organization	Question 53 Comment
53.40	Kansas City Power & Light	TFE should continue to be allowed. Unsure of all the requirements that this may apply to at this point. Recommend the Drafting Team at least consider a direct translation from the CIP version 2 requirements to these CIP-011 requirements at a minimum since CIP-011 is intended to be a translation but less prescriptive.
53.41	USACE - Omaha Anchor	TFE's will still be required in several standards - I've addressed the requirement for TFE in applicable standards.
53.42	Allegheny Energy Supply	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.43	Allegheny Power	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.44	National Grid	TFEs related to Password and Appropriate Use Banner.
53.45	CWLP Electric Transmission, Distribution and Operations Department	TFEs should be allowed for requirements R10, R13, R14, R15, R16, R17, R18, R19, and R23.
53.46	Reliability & Compliance Group	The best thing that could be done for this Standard is to ensure that everything is well defined so that there is no ambiguity when it comes to identifying BES Cyber Systems and also categorizing their impact.
53.47	Manitoba Hydro	The language or the requirements should be written such that there should be no need for TFE submissions. The standards should allow for compensating measures. For all instances where it is not technically possible to meet strict compliance with a requirement, the Responsible Entity should apply compensating controls which are documented and approved by the senior manager or delegate, similar to the policy exception process in CIP-003-1. The current TFE process creates a enormous administrative burden on the electric industry which provides no additional value to the reliability of

#	Organization	Question 53 Comment
		the Bulk Electric System.
53.48	LADWP	The need for TFEs still exist as certain control systems are legacy systems that may not have current update or patch capability (e.g. SCADA systems). Removal of TFEs for these systems would result in non-compliance as replacement or upgrade of these systems must be done on a planned and scheduled manner.
53.49	Garland Power and Light	There are 2 requirements specifically listed below that need TFE's but there should be provision for any equipment that cannot be made strictly compliant with any requirement that either a TFE or a mitigation plan can be written and implemented such as is stated in 16.1 or 17.1.Requirement R10 - Unless the requirement is rewritten to allow for procedural controls to suffice for compliance or the language in the footnote is actually included in the requirement, a TFE is needed for this requirementRequirement R14 - A printed circuit board (with a network connection) in most cases will not allow for any process to be loaded onto it to protect against malicious software - need a TFE for this requirement
53.50	GE Energy	These changes should eliminate the need for the vast majority of TFEs. There may still be a requirement for TFEs on systems that cannot enforce the password complexity rules.
53.51	FirstEnergy Corporation	This question should be postponed until the Standards are in a more final state so that entities can better see how the new requirements would apply to specific devices, etc. It appears that R20 would necessitate new TFEs.
53.52	NextEra Energy Corporate Compliance	Though NextEra believes TFEs are very important part of the CIP process, given the number of changes proposed, NextEra will wait until the next draft to comment on TFEs.
53.53	Oncor Electric Delivery LLC	To eliminate the need for TFE’s the standard will have to be more granular. Many legacy systems are immune to cyber attacks, yet cannot satisfy the requirements of this standard. R8.3 as an example, there is no system to monitor access at the physical port of relays. R10 - legacy devices do not support account management.

#	Organization	Question 53 Comment
53.54	American Electric Power	We encourage the SDT efforts in drafting requirements in such a manner that will eliminate the need for a TFE. The TFE process should be standardized between the Regional Entities. Currently, Responsible Entities are required to submit multiple forms and varying information for the TFE process depending on the Regional Entity. AEP suggests standardizing on a single submission form and process and have all TFE data submitted to a single source maintained by NERC that can be used by all Regional Entities. This will allow Responsible Entities to submit and/or modify TFE data once and have it available to all Regional Entities on a consistently.See comments under questions 24 and 35.
53.55	We Energies	We Energies agrees with EEI: Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.56	Regulatory Compliance	We feel that TFE's should still be considered for the following tables:R10 - Account Access Control SpecificationsR14 - Wireless and Remote Access ControlsR16 - Security Patch ManagementR17 - System HardeningR18 - Security Event MonitoringR19 - Communications and Data IntegrityR20 - Electronic Boundary ProtectionR23 - Configuration Change Management
53.57	BCTC	We have embedded this information in our individual responses to previosu questions.
53.58	US Bureau of Reclamation	We have not had an opportunity to assess which requirements may require a TFE yet. We will evaluate the requirements during the next evaluation period.
53.59	Duke Energy	We prefer that all of the requirements allow for an exception. Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.60	GTC & GSOC	We recommend that TFEs should be considered for all requirements with the exception R1 because of the ability of the regional entity and NERC to review the appropriateness of the TFE. We recommend adding language to the requirements on acceptable use banners and passwords to clarify that they do not require TFEs.If our recommendation to allow TFEs for all requirements is not viable then the following requirements should allow an entity to request a TFE. (R5, R6, R8, R9, R10, R13, R14, R15,

#	Organization	Question 53 Comment
		R16, R17, R18, R19, R21, R22, R23, R26)Example justifications are as follows:R5: BES Cyber Systems where physical security cannot reasonably be provided such as devices that are physically hung on a transmission line such (i.e. transmission line fault detectors). R6: While physical protection of the physical security systems should be feasible in most instances, there may still be instances where mitigation measures need the oversight provided by the TFE process.R8: The majority of substation devices use the concept of "shared" accounts. While an entity can add a device to facilitate logging into substation devices, there is not a feasible way to "monitor" these accounts on the purpose built devices themselves such as protective relays. R9: Depending on the method chosen to physically protect the BES Cyber System, it may not be technically feasible to revoke physical access to every location within 24 hours for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R10: There are numerous examples of legacy devices which cannot meet the requirement of a 6 character password, or a password with special characters, etc.R13: Depending on the method chosen to electronically protect remote access to the BES Cyber System, it may not be technically feasible to revoke remote access to every location within 1 hour for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R14: There are rare instances where remote access may be needed without 2-factor authentication such as for the administration of the device that authenticates the remote access itself. There are also instances where a display of appropriate use banner is not technically feasible.R15: While this requirement should greatly reduce the number of TFE's submitted based on the existing CIP v3 malware requirement, there will still be existing legacy purpose built BES Cyber Systems that do not have the ability to detect and respond to the introduction of malicious code. Specifically, consider the case of a protective relay with no external connectivity.R16: The allowance for TFE's should carry over from the existing CIP-007-3 R3.R17: Based upon the existing TFE framework, the language "shall document and implement a mitigation plan" from row 17.1 would necessitate that a TFE be filed.R18: There exists no such tool or process to monitor for system events related to cyber security on protective relays with no external connectivity.R19: Not all data protocols include a checksum. Whereas most SCADA protocols do contain this data error detection functionality, this requirement (19.1) is not limited to those inbound SCADA connections. There are a number of reasons, supported by the DHS Catalog of Control System Security itself, where an entity may choose not to encrypt all data inbound to a BES Cyber System (19.2).R21: There may be shared

#	Organization	Question 53 Comment
		cyber system components between BES Cyber Systems that do not provide logical separation. Clarification of this requirement may resolve the need for a TFE allowance on R21.R22: The TFE allowance justification for R22 carries over from the justifications for R14, R16, R18, and R23.R23: There are a number of devices for which there exist no such tool to monitor changes to the baseline configuration (23.7). In addition, it will not be feasible to monitor and detect changes for those systems with no external connectivity.R26: There are maintenance devices for which there are no known methods to detect and prevent the introduction and propagation of malicious code. Examples include devices such as data analyzers, birdogs, etc.
53.61	Constellation Energy Commodities Group Inc.	We support the effort to reduce the need for TFEs; however, the complexity and variability of systems across industry make it difficult and inappropriate to expect one-size-fits-all requirements.The password complexity requirements should either be written so as to avoid the need for TFE's, or clarified to specify that the use of maximum complexity allowed by the device is sufficient.
53.62	Entergy	Where the need for TFE has been obvious to us we have noted as such in comment to the respective requirements. We will be more thorough during the formal comment period.
53.63	Con Edison of New York	Will Technical Feasibility Exceptions still be accepted, required or will this process no longer be enforced? The Password requirements would still drive the need for TFE's. TFE's may be avoidable if the standard allows for internal documentation and approval of exceptions. There will be many TFE required because the net has been cast on so many different unique type systems that are located on the power system. Many of these systems are 20 to 30 years old. The CIP is written to address concerns for new technology computer network systems. Much of the equipment used on the power system is uniquely built and not designs with a full wide area network design.It would be a much better approach to address the SCADA systems (remote control and indications) & EMS systems and pay less attention to trying to force all the other unique (less critical) equipment in the same square hole.

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

Summary Consideration:

Many of the commenters stated that the Standards need additional clarity. Define what is meant by words like monitor and review and remove potential ambiguity. Make clear the intent or objective of each requirement. The timing requirements of the standards need to be clearly defined. In response to these comments, the drafting team has made several steps to improve the clarity of the standards. These steps include moving to a Results-Based Standard approach, where the reliability objective must be specified for each requirement. Also the Drafting Team reviewed these standards with regional CIP auditors, with FERC, and with industry representatives ahead of the NERC Quality Review process to gain additional clarity in the requirements. The Drafting Team agrees and has made efforts to eliminate inconsistent terms and phrases and to consistently and unambigouously use timing phrases throughout the standards.

Commenters stated that the Implementation Plan should address the significant amount of effort required to comply with the standards for the many new cyber systems that will be in scope. Significant time should be included in the Implementation Plan for the categorization of BES Cyber Assets and for the transition from previous versions of the CIP standards to the Version 5 standards. The Drafting Team is proposing to allow 2 years for the Responsible Entities become compliant with all of the CIP standards and to allow entities the option to become compliant earlier if they choose to bypass Version 4 compliance.

Many commenters expressed a common theme to remove or minimize requirements for Low Impact BES Cyber Systems. Since the overarching objective is to provide for some level of security for all BES Cyber Assets, the Drafting Team has kept the requirements for physical and electronic boundary protection as well as basic security program elements such as policy, awareness and incident response, for the Low Impact BES Cyber Systems.

#	Organization	Question 54 Comment
54.1	Independent Electricity System Operator	- Specify calendar or business days when referring to a time frame- Issue with the bundled approach-- if you violate more than 3 in the same standard, this affects the VSL? need to look at NERCs governing procedure on VSLs- Strongly suggest that standards
54.2	Consultant	1. Each requirement should have a unique title. Currently the requirements are grouped by the subject area, but the requirements typically are just a statement. This makes it difficult to reference requirements except by number. What will really happen is everyone will develop their own "short title" for each requirement number, and it will not be consistent across the industry, and will result in

#	Organization	Question 54 Comment
		confusion.2. There should be consistency for the requirement title, the associated table name, & the requirements column heading for each requirement. Currently these three items are not necessarily consistent, and in some cases there doesn't seem to be a connection or relationship in the terminology in these locations.3. If the Requirements Groups are going to stay in the standard then they should be numbered in order to facilitate cross referencing the groups.4. The word "criteria" in the requirement statement should be change to "requirements" where it occurs. The tables list requirements, not criteria. (Multiple instances throughout CIP-011)5. There is different sentence structure and grammatical structure throughout CIP-011. While it is a good idea to combine the requirements in a single standard, it still appears to be written by multiple authors. There are still access control and account management requirements scattered across multiple requirement groups, and each is a bit different. Another example, the incident response and the recovery plan requirements groups should be very similar, but are, in fact, very different in the requirement and the wording of the requirements, much like the differences noted in CIP-008 and CIP-009. The structure of the "local definitions" is different throughout.Suggest a "wide area" review to make the standard appear to be written by a single author rather than multiple authors.6. The definitions should be written as definitions. [Defined Term - Definition statement.] The wording "for the purpose of this standard" is not correct, and thus unnecessary. The glossary collects definitions from the standards when the glossary is updated. The next update should add the terms defined in these standards, and therefor they are not "for the purposes of this standard". Also, the words "is defined as" are redundant as it is a definition.7. Data retention requirements should be included as requirements. Moving data retention to Section D isn't logical. If there is no requirement for data retention, then it isn't a viable compliance activity. At the workshop it was stated that this was a NERC format. In this case NERC is wrong and needs to correct the format, both for these standards and for the other reliability standards. 8. Suggest dropping all requirements for assets categorized as Low Impact. They are after all, low impact on the BES. Based on the discussion at the workshop, looking at a 10 year implementation timeline for low impact assets is effectively the same as no implementation. Many things will change in 10 years, and expenditure of resources in the low impact is unlikely to have any increase in BES security. The Low Impact category needs to remain as part of the categorization process in order to include all BES assets in that process.9. There are multiple requirements that differentiate between types of facilities in the requirements tables. This is an indication that the categorization criteria is incomplete or incorrect, or

#	Organization	Question 54 Comment
		that the requirements are not properly stated. If a requirement currently indicates in the High Impact column that it applies to Control Centers only, then either (1) the transmission, generation, and special systems are not "High Impact", or (2) the requirement statement doesn't properly address all asset classes.The categorization criteria should properly place each asset in each asset class in the appropriate category with "bright lines" to eliminate adding categorization in the requirements.10. While this format for commenting and collecting comments seems good, there should be a mechanism to complete the form 'non-sequentially'. For example, as comments are made through the form's current sequence, if a 'general' comment arises, the only method to enter that comment is to page through to the end, save the comments, and then reopen and page back to the location where you started. This is not very user friendly.11.The commenting tool should have a "Save and Continue" option to allow saving work in progress without exiting and re-entering the tool.12. An improvement to the "status bar" of the commenting tool would be a table of the questions with an indication for each question if a response has been entered.
54.3	Con Edison of New York	A few general questions:Will there be an implementation plan? The document for comments indicates there will be an implementation schedule that will take into consideration existing BES Systems (CCA's) and newly defined BES Systems (CCA's). In order to be able to meet the requirements in CIP-011, the devices on secured networks that are not currently CCA's by definition but are "treated as" since they are on the same network need to be considered as part of the implementation plan. The inheritance rules may require newly defined CCA's in order to allow the time that we be needed to address these additions. If they are considered existing since they are "treated as" a short implementation period could be an issue.Is there a six-wall physical boundary requirement in this version of the standards? Suggested additional defined terms:"BES Cyber System Failure": should be defined to serve as shorthand for the long list of items currently used in the draft CIP-010/011 Reliability Standards.Current Wording: "disruption, compromise or failure of BES Cyber Systems""if destroyed, degraded, misused or otherwise rendered unavailable"Proposed Wording:The term 'failure' when used in conjunction with the terms BES Cyber Component and/or BES Cyber System shall encompass the meanings 'malfunction, disruption, compromise, failure, destruction, degradation, misuse or unavailability' of those.Suggest replacing term "affect" with already defined term "adverse reliability impact". The drafting team (DT) uses the terms "affect" and/or "affects" without providing any specific meaning, system impacts, or other bounding explanation to describe that term. Proposed

#	Organization	Question 54 Comment
		Alternative Wording:NERC Glossary of Terms - Substitute definition for BES Cyber System "affect" or "affects." [Causes] Adverse Reliability Impact - The impact of an event that results in o frequency-related instability; o unplanned tripping of load or generation; or o uncontrolled separation or cascading outages, that affects a widespread area of the Interconnection.
54.4	Allegheny Energy Supply	A lot of work went into the prepration of the existing CIP-002 through CIP-009 standards. This new CIP-011 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to helping to refine the CIP-003 through CIP-009 drafts and to create and implement the current compliance plans and related software systems. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES.Suggest that the standard require physical security controls for BES Cyber Systems that no more stringent than other requirements for the BES equipment that the BES Cyber System controls, protects, or monitors.Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.- Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
54.5	Allegheny Power	Allegheny Power does not understand the need to eliminate and combine CIP-003 thru CIP-009 into a new standard CIP-011. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP standards are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP standards and not force changes in terms, concepts and numbering schemes

#	Organization	Question 54 Comment
		which would essentially force all entities to start their CIP compliance efforts over from the beginning. AP would like the SDT to abandon the concept of completely rewriting the CIP standards in favor of incrementally revising the existing standards to accomplish the same objectives.
54.6	Lincoln Electric System	Although much of the standard seems very practical, LES believes it was written with routable systems in mind. When applied to systems with only non-routable connections, or even no connections, many of the requirements are not very applicable, and would set the stage for numerous TFE's within the industry. LES believes this either needs to be addressed requirement-by-requirement, as in the approach taken by the MRO NERC Standards Review Subcommittee (MRO NSRS), or there should be a blanket statement that removes non-routable systems from the requirements that are not applicable. Either way, LES believes this differentiation is extremely important, since non-routable connections (or even better, no connections) are inherently more secure against, and limit potential damage from, remote attacks, and by default eliminate the threat of propagating localized attacks to other facilities.
54.7	Oncor Electric Delivery LLC	As the tables of CIP-011-1 specify certain requirements for "Control Center Only" or "External Connectivity", the additional requirement of "Routable Communication or Dial-up Only". Many requirements do not even make sense without integral communications being part of the cyber systems. If there isn't communication involved, the cyber system should be excluded from a requirement.
54.8	Garland Power and Light	At the CIP workshop, there were several comments that were made that were "depends" or "our intent was" o The "depends" requirements need to be reworded so that requirement is clear. o The "intents" need to be expressed clearly in the document because it is almost guaranteed that the will be many different interpretations if they are not expressed.
54.9	Constellation Power Source Generation	At the workshop, it was stated that an assumption of the SDT that High Impact BES Cyber Systems were most likely already Critical Cyber Assets per the older standard. This is false. Non routable protocols and other criteria used by Registered Entities have excluded certain assets at critical locations from being critical cyber assets. A 3 year timeframe should be implemented for High BES Cyber Systems to be fully compliant if it was previously not classified as a CCA. Another suggestion for implementation is to make the procedural requirements auditable first, and then implementing the

#	Organization	Question 54 Comment
		other requirements in stages. Furthermore, as stated in the workshop, allowing an entity to declare advanced implementation for audits would be of great benefit, as compliance with the new standard will take years to implement. The blank boxes found in the requirements tables of CIP-011 are implying that a high/medium/low BES Cyber System does not need to comply with that requirement's particular control, but that is not written anywhere. A blanket statement in the beginning of CIP-011 needs to state that the intent of an empty box to avoid confusion. An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for auditees in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.
54.10	E.ON U.S.	Because Distribution Providers are for the first time made subject to CIP standards they may need additional time to come into compliance
54.11	ReliabilityFirst Staff	Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
54.12	Reliability & Compliance Group	By dividing up the Standards and just revising CIP-002 through CIP-009, it makes it easier for the Registered Entities to update their existing documentation. It allows for the creation of a "crosswalk" document that helps examine the changes. While it may not be able to be done requirement by requirement and sub-requirement by sub-requirement, it can be done Standard by Standard. Where possible, it would be good to create a change crosswalk document that lists the version 3 requirements and the points to where they are now covered in the version 4 standards and note that

#	Organization	Question 54 Comment
		there is either a major change or a minor change.
54.13	LADWP	CIP-011-1 R16 The patch management does not specify a required time for installation of patch. The entity should be given the ability to determine the schedule as systems vary on when they can be brought down to install a patch. The language in R16.2 addresses the issue and no additional language to restrict the installation time needs to be included.
54.14	City Utilities of Springfield, Missouri	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
54.15	US Army Corps of Engineers	Definitions within the standard need to be improved so they are less ambiguous.Statements like those found in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", are confusing. What is the standard trying to say here?
54.16	USACE HQ	Definitions within the standard need to be more direct and narrower scope. Also, the relocation of all of them to a separate attachment would help too.
54.17	Dominion Resources Services, Inc.	Dominion recommends placing all requirements into a requirements table. It is sometimes difficult to distinguish requirements mixed into the preambles.Using a single standard for all requirements is preferred; however the format internal to the single standard is inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
54.18	EEI	EEI would like to thank the members of the Drafting Team for their significant efforts on this important issue.
54.19	Black Hills Corporation	Emergency Response: Emergency Response provisions are limited to R3 & R4, and address training and risk assessment controls. There are many possible scenarios that could be identified which would

#	Organization	Question 54 Comment
		require emergency exceptions to most of the requirements of CIP-011. There should be a general emergency clause that allows appropriate response to many possible emergency situations.Outside Vendors: There is no mention in the rules how the use of outside vendors should be addressed. A common solution could be to have the responsible entity extend the necessary requirements of these regulations to the third party via contract. (Example from other regulatory efforts includes the HIPAA regulations and their business associate requirement). An example of this in action could be the requirement that a contractor conduct the personal risk assessment, according to the requirements specified in CIP regulations.
54.20	Exelon Corporation	Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format.. Each change in itself represents a significant “change management” issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon’s continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us “starting from square one” to implement. Policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards.Specifically, Exelon

#	Organization	Question 54 Comment
		would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity.This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.Compliance with NERC cyber security standards should be re-scheduled for nuclear generation. That is, nuclear generation is currently in the process of compliance with Version 3 of CIP-002 thru -009 by September, 2011. However, it appears that compliance with Version 4 of the standards may be required by 2013. In terms of resource expenditures, ultimately borne by consumers of electricity, it seems wasteful to build a program for nuclear generators based on CIP-002 thru 009 that will be scrapped roughly two years later to be compliant with CIP-010 and CIP-011. Such scheduling will result in maintenance of a program based on CIP-002 thru -009, including audit support, and purchasing and installing equipment during refueling outages, at the same time a new program built on CIP-010 and -011 is being constructed. This new Version 4 program will include doing away with the concept of Critical Assets so that purchase and installation of the equipment previously installed may no longer be required. The existing cyber security programs and regulations in place or in process to protect nuclear generators, e.g., NEI-04-04 and 10CFR73.54, the limited contribution of nuclear generation to the BES (roughly 20%), and the limited time until Version 4 of the NERC Standards are expected to be in force all limit the cyber vulnerability of nuclear units. It is recommended that the implementation of Version 3 of CIP-002 thru -009 for nuclear units be deferred, and compliance with NERC cyber security standards for nuclear generation be re-scheduled for Version 4.
54.21	BGE	General - The wording was changed to “at least every 12 months” instead of “annually” in previous CIP versions. Can the exercise or test occur in the same month each year or must it be 11 months 29 days or less from the previous exercise/test?
54.22	Network & Security Technologies Inc	Good start! Strive for clarity. Ask both individuals responsible for compliance and auditors for their interpretation of every requirement. Be explicit about what’s required (e.g., documentation of, records to demonstrate compliance with, etc.). It’s okay to not be very prescriptive but try to avoid

#	Organization	Question 54 Comment
		implied requirements - they will be a source of endless debate.
54.23	CWLP Electric Transmission, Distribution and Operations Department	Guidance documents should be available before balloting these standards. All terms used should be defined in the NERC Glossary of Terms or in the standard.
54.24	Green Country Energy	I really like the way the standard is developing it is a huge improvement and hopefully with industry comments it will develop into a fine standard that meets everyones expectations.I would like to see a Guidance Document, footnotes, measures and VSLs etc to make compliance and auditability a lot clearer and less subjective.
54.25	US Bureau of Reclamation	It seems that the standards are applying a postage stamp level of security to Cyber elements involved in BES reliability. Multifunction relays or Solid State relays which are programmable must now have eletronic access attributes which are normally associated with BES computer control systems. The SDT should reexamine the true nature and scope of these types of systems before lumping these deviced together with traditional computer control systems. Lumping everything into one standard will make adminstration by the Responsible Entities and Reliability Entities difficult and may add to confusion with respect to individual table elements.While the tables applied to requirements in CIP-011 are an excellent way to establish security requirements for the 3 levels of system impact addressed, the empty fields should be avoided as they lead to confusion on the part of readers. All blocked fields should indicate something, even if it is an indication that the requirement is “Not Applicable,” “Not Required,” “Addressed under Requirement xx.x, above,” or “In accordance with entity policy.” Further, all requirements should include the 3-level requirement application table, even if the requirement applies equally to all three levels. This will further avoid confusion when reading the Standards.Appreciate the “blocked-out” area-specific definitions, but the drafting team must ensure that this feature is only used for area-specific needs and not global definitions. If the scope of the definition extends beyond a specific section there could be problems with sub-dividing the document to simplify what is handed over to organizational components with different functional responsibilities, particularly if the definitions do not also appear in the NERC glossary.The use of “objective statements” is very much appreciated, both as a guide to entities addressing

#	Organization	Question 54 Comment
		implementation and also (we would assume) to reviewers and audit staff addressing compliance. We encourage the drafting team(s) to continue this direction and to strengthen and refine the objective statements in order to provide clear direction for Standards users, including down to the sub-requirement level (as applicable).
54.26	Luminant	Measures need to be defined
54.27	Minnesota Power	Minnesota Power believes that, for all requirements which specify that something must be completed within X hours, the Standards Drafting Team consider using the following statement:"As soon as practical, but not exceed x business days from the date reported."This would preserve the spirit of the requirement, but also allow for more practical time frames.With so many auditable elements included in these Draft Standards, Minnesota Power believes that the VSL's cannot be written with the current zero-defect mentality. It would be more practical to allow for minor issues to be identified and scheduled for corrective action without representing immediate non-compliance which will result in extended investigations and settlement proceedings.Minnesota Power recommends that the Standards Drafting Team consider using a technical writer and/or solicit feedback from multiple proofreaders who have not been involved in the creation of this Standard to ensure that the following items are addressed: o any interpretable vocabulary is defined o grammar is correct o punctuation is correct o meaning is clear and does not require any guessing as to the intention of the Standards Drafting Team.This should be done prior to the official comment period, so that the Industry can concentrate on technical aspects of the review, rather than spending time on interpretation. The ability of Registered Entities to properly interpret the Requirements is highly dependant upon clear wording, good grammar and proper punctuation. This has been one of the greatest problems with the version 1 through 3 CIP standards. Minnesota Power requests that the Standards Drafting Team ensure that improper writing does not change or hide the intended meaning. The misuse of
54.28	Progress Energy (non-Nuclear)	More examples of requirement application to the real world would aid auditors and the industry.In CIP-011 If the record keeping and retention for compliance is similar to previous standards this standard significantly increases the record keeping administrative burden on utilities and compliance authorities due to the number of devices which are now to be declared without actually increasing security of BES.Implementation plan (when developed) needs to consider how it will overlap existing

#	Organization	Question 54 Comment
		standards compliance record-keeping and documentation, then establish a phased-in approach of the new standards to eliminate double record-keeping and double documentation across audit compliance periods.Implementation schedule needs to be developed that allowsHigh - 4 yearsMedium - 4 yearsLow - 4 yearsNeed clearer definitions of annual, quarterly, etc.Need to resolve issues/questions with current standards:How is communication/wiring covered by the standards? This becomes even more of a question when a BES Cyber System could be defined as a SCADA system including all of the RTU's which support it.Within ESPBetween ESP'sInto/Out of ESPPassword strength/management. Improvement has been made here, but it is still not clear if requirements must be enforced by the assets in question or if policies are sufficient. For instance, regarding the requirement to change passwords at least once every 12 months, must the device force this password change, or is it sufficient for an entity to have a policy requiring compliance along with documentation to attest that the policy was followed?Timeframe for revocation of access for expired training/background checks. NERC CIP Training is required at least every 12 months. It can be assumed that if the training is not completed in the allowed timeframe that access must be revoked; however, it isn't clear if this revocation must be done immediately, within 24 hours, 36 hours, 72 hours.There is currently no provision for moving cyber systems from one ESP to another (such as between a primary and backup ECC). Although this type of even will need to happen from time-to-time, it is left up to each entity to determine how that can be accomplished within the standards.There is no clear distinction between various types of Access control. It is obvious that the standards apply to network facing logins for BES Cyber System Components;however there are other types of access that are not clearly addressed or excluded such as-Access to configuration controls for something like a time standard which are only available to someone with physical access to the front of the device-Access to the BIOS on a typical PC-Access to various functions/programs on a machine - some of which may require special login - others which don't.How 7 year background checks are handled for someone under the age of 25 since juvenile records prior to the age of 18 may not be legally searched in many cases.Will the TFE process continue? What a TFE is, where it is/is not allowed, how it is to be handled (regarding documentation, approvals, submittals, periodic reviews, etc)
54.29	Michigan Public Power Agency	MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities,

#	Organization	Question 54 Comment
		" between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
54.30	ISO New England Inc	Need more precise, well-defined language. Several requirements are measures, not standard requirements to measure against. Provide examples, FAQ, what is the actual risk/ driving requirement - what are we trying to protect against? Understanding the background to the requirement will help to define defenses to perceived threats that this standard is trying to protect. Clearer definitions of Cyber Systems, Cyber System Components, Control Center. Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional pageRequest that the tables and time constraints be consistentEliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32)Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.31	WECC	Need to have consistency in spelling out time periods versus numerically showing them (ie thirty-six months vs 36 months). Also need consistency in use of the tables as some say "criteria" and others say "procedures" or "processes". In many cases when a requirement states that you should have a process or a procedure it might be easier for audit purposes to instead require a program that addresses many of the processes or procedures required. A single requirement for a program or plan that meets a table of criteria might reduce the number of requirements and ease audits. For instance "Wireless Security Program covering the following risks" "Remote Access Program addressing the risks in Table X" "Maintenance Program addressing the criteria in Table X" "Physical Security Program addressing the criteria in Table X"
54.32	US Army Corps of Engineers, Omaha Distirc	Next draft should include the measurement criteria. Standards are very computer center centric.
54.33	Regulatory Compliance	NRG Energy Inc. is concerned with some of the impact criteria in Attachment II related to transmission and generation Facilities. To base impact on "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows.

#	Organization	Question 54 Comment
		Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: Â· High Impact (has the potential to cause an Adverse Reliability Impact) Â· Medium Impact (has the potential to require planned/controlled loss of load) Â· Low impact (has no potential to cause loss of load)
54.34	National Grid	o There is inconsistency in using “processes” or “one or more processes” in several requirements. For example R25 states that Each Responsible Entity shall document and implement one or more processes...” while R26 states that Each Responsible Entity shall document and implement processes...”. National Grid recommends using “one or more processes”. o Request that the tables and time constraints be consistent o Eliminate confusion caused by two 3.1’s. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32) o Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.35	Southwest Power Pool Regional Entity	Overall auditing issue: The requirements need to consider issues of sufficiency (adequacy of the entity solution) without being prescriptive in the solution. Where possible, clearly define the objective and do not prescribe technical solutions. Also, avoid the use of adjectives in defining the objective and / or specific requirement. Terms such as “adequate”, “sufficient”, and the like are very difficult to objectively audit. Overall observation: The implementation plan concept presented at the May 19-20 workshop in Dallas, coupled with the proposed applicability matrix for Medium and Low impact BES Cyber Systems will likely reduce, not improve the overall cyber security protection afforded the BES Cyber Systems today. A good number of existing Critical Cyber Assets will fall out of the High impact category, many becoming Low impact, with the resultant relaxation of protections. The applicability matrix as it appears today does not define a reasonable baseline of protections for Low and Medium impact systems. Re-categorization of BES Cyber Systems: While this will hopefully not happen very often, a BES Cyber System that sits on the cusp between two categories could find itself being re-categorized more than necessary unless some sort of a dead-band is introduced that would preclude re-categorization as a result of a small change. Implementation Plan: There needs to be a consistent

#	Organization	Question 54 Comment
		implementation plan for any BES Cyber Systems represented under today's standards as Critical Cyber Assets regardless of their ultimate categorization. Any existing Critical Cyber Asset should be afforded a very short timeframe to achieve compliance under the new standard(s) as it can be reasonably be expected to be already compliant. This is similar to the Table 1 entities concept for Version 1 of the existing standards where entities subject to the UA 1200 standard were given the shortest timeframe to comply. Consideration needs to be given to how an entity will migrate from compliance with the existing standards to the new standards. A piecemeal approach will be very difficult for the entity to maintain and for an auditor to evaluate compliance.
54.36	Alliant Energy	Per previous comments, all occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement. Per previous comments, all instances where 12 calendar months are used as the outside allowance for renewal a rolling creeping calendar is introduced. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.
54.37	FirstEnergy Corporation	Please see our response to Question 1 for the FE Summary view of the proposed CIP V4 standards.The new format, tables, information boxes is a good change o We question whether the new format (low-to-high impact, in particular) will encourage us to categorize more as high so we track things in a similar way. It seems like an administrative burden to try to track things at three levels. It is hard enough to track everything now with just one level. This 'administrative burden' issue crops up in

#	Organization	Question 54 Comment
		several places.
54.38	PacifiCorp	Procedural exceptions are onerous to manager operationally; the standards would be more effective if less differences in revocation of access were implemented across the BES system and criteria.The term "Annual" is not defined. "Annual" requirements were changed to 12 months in most cases (not consistently). The 12 month requirement causes "schedule creep". Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual" or, preferably, use the definition of annual defined for the NERC FERC Standards of Conduct (calendar year). The following FERC Directives need to be addressed with version of of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Don't wait. Address the following FERC Directives in version 1 of of CIP-010 and CIP-011.
54.39	Southern California Edison Company	SCE recommends revising the numbering of CIP-0011-1. Between CIP-010 and CIP-011 the drafts should indicate the intention of the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. Otherwise, the gap of unused numbers between CIP-001 and CIP-010 will potentially cause confusion. SCE also suggests rearranging the structure of these new requirements. for example, by breaking up CIP 011 into functional areas such as Governance & Personnel, System Security & Boundary Protection (with Incident response since “incidents” are cyber security incidents), Access Management (Physical, Electronic and Information), and Disaster Recovery Planning & Capability. From a policy formulation perspective, this would result in fewer policies than CIP 011 as it is currently structured. For example, combining physical access controls with electronic access controls provide the means of utilizing a combination of both to determine sufficient total security. Providing secure physical access controls and disconnecting routable communications such as gateways and/or modems.Finally, separate and apart from the recommendations made above, SCE also recommends allowing use of local definitions as in-line guidance at the requirement level. The use of local

#	Organization	Question 54 Comment
		definitions in addition to the NERC glossary is good approach. The text of each requirement objective should be such that it is only a objective and not a control statement. A control should reside within the impact level table. For instance, R11, R12, R18 contains control statements within the objective.
54.40	San Diego Gas and Electric Co.	SDG&E notes that it appears the drafting team took the approach of defining the details and then working up to the bigger picture items, i.e., BES Cyber Systems Component to BES Cyber System. SDG&E feels that there is risk associated with taking this "bottom up" approach to the standard setting process vs. the "top down" as used in the previous three versions of the standards. The risk is that components posing no significant risk to the BES system can get "swept up" into BES Cyber System definition and require protection commensurate with components that are correctly required to have strong security measures.SDG&E feels that part of the issue with Versions 1-3 of the CIP standards was that the "top down" approach to critical asset identification was not started high enough; it was started at the Responsible Entity level rather than at the Region / Reliability Coordinator level. If that level is deemed too high, even a sub-region level would be more appropriate. In SDG&E's case, it has a view of its assets in the context of its service territory that serves 1.4 million retail customers. Independent generators on the other hand don't have that regional view. In Southern California, for instance, congestion is high in some places and regulatory mandates for incorporating renewable energy are growing. Thus, the risk to the BES can only be fully evaluated when considering sources (generation - fossil and renewable) and uses of energy (load) in the region as well as the adequacy of transmission to balance and move power. In such a scenario, the assets critical to BES stability and/or restoration are much easier to identify and so too are the BES Cyber Systems that support them. For those entities that do not have a region or sub-region view, perhaps the Regional Entity, Reliability Coordinator or Balancing Authority could be responsible for identifying which assets are critical.
54.41	Manitoba Hydro	Section D Compliance: 1.4 Data Retention should include all documentation, inventories, logs, etc that are mentioned throughout the Requirements, or include a "catch all" requirement for data retention for all other documentation referenced by the Requirements.General Comments: The language in Requirement R1 indicates that each Responsible Party shall "develop, implement and annually review one or more formal, documented cyber security policies" addressing the listed Requirements. This should be clarified to confirm whether a formal written policy is required for each of the listed Requirements or only for selected Requirements. From the language of the specific Requirements one

#	Organization	Question 54 Comment
		could assume that those Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, while those Requirements that indicate only "implement" do not. Then there are those Requirements that require the Responsible Entity to "create, document and implement" - it is not clear if this would require something different than "document and implement". There are also those Requirements that simply require that certain criteria be applied which would seem to indicate that no documentation is necessary. If the Responsible Entity is to assume that the Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, it is assumed that there may be one master policy covering all elements of the Requirements that must be documented given the language in Requirement R1 "one of more formal documented cyber security policies" and that separate documented policies for each of the Requirements requiring documentation are not necessary. Certain references to "review" in the Requirements should be clarified to indicate on what basis the review is to be conducted, what criteria should be applied, what the Responsible Entity should do with the results, etc. i.e. Requirements R5-5.6, R12-12.1, R18 -18.4. The same comment applies for certain references to "monitor" (i.e. Requirements R8-R8.3) and "verify" (i.e. Requirements R24-R24.5). Where no review or monitoring of developed protections or processes is specified, is it to be assumed that no review or monitoring is required? (Requirements R15 and R16) Each of the Requirements seems to provide a reason or justification for their inclusion i.e. Requirement R2 ".....to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems." Consider whether it is necessary to state the justification for each Requirement, especially if it could be that the objectives achieved by the Requirement are not exactly as specified or if the Requirement does not necessarily meet the objective as set out. It would be preferable to just have the broad purpose statement in the introduction which is stated to apply to each of the Requirements that follow. What is the purpose of the Measures in these standards? If they are to re-state the wording of the Requirement, they provide no value and create opportunities for legal interpretation if the wording in the measure does not exactly match the wording in the specific requirement. Entities should be allowed to employ multiple layers and tailor their approaches to cyber security to meet the intent of the requirement, such as including the inherent security benefits provided by private entity owned and managed communication networks. Manitoba Hydro is also concerned that the multiple layers of physical and electronic security directed by FERC Order 706 are

#	Organization	Question 54 Comment
		not included in this proposed version of the CIP-010 and CIP-011. While we understand that these directives were not included at this time for the sake of expediency, there is a risk that the electric industry may expend considerable resources to meet the requirements these proposed standards, only to revisit the electronic and physical security issues and expend more resources in the near future. Implementing physical security changes for electric facilities is proving to be a monumental task. This standard does a disservice to the industry if it does not provide the complete scope of the physical security changes required. If the entire scope of the physical security requirements, including the directives in FERC Order 706, cannot be provided to the industry in this proposed version of the standard, then all the requirements for physical security should be removed at this time and submitted to the industry, in its entirety, at a later date.
54.42	Alberta Electric System Operator	Specifying the units of measure (e.g. business vs. calendar days) and exact ordinal amounts ("365 days from date of implementation" vs. "annually") might help resolve some ambiguity surrounding some of the criteria.
54.43	Northeast Power Coordinating Council	Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.Situational awareness displays currently in use at the Regions and FERC should not be included in the applicability of these standards. No operational actions or decisions are being made based on the information on those displays.
54.44	Nuclear Energy Institute	Terms should be clearly defined and unambiguous. Examples of items covered by the term and not covered by the term should be given. CIP-011-1 is a vast change from the prior CIP-003 through CIP-009, and clear definitions with examples will be valuable.

#	Organization	Question 54 Comment
54.45	Puget Sound Energy	The amount of work relative to CIP-010 is almost as much as CIP-010 because of the broad application of BES Cyber Systems. It would be prefereable to be able to manage this scope better up front so that entities don't have to evaluate and record so much to then only focus possibly a much smaller pool of work as more defined by CIP-011. It still not clear how to evaluate a system for "misuse" effectively and defensibly. Further guidance would be appreciated. Lastly their should be some grace period and easier interpretation process when these versions become effective in order to more quickly flush out interpretations of concepts once implementation starts. To date the interpretation is a lengthy process or determined in an audit as a result of a violation when the entity may have been well intended.
54.46	APPA Task Force	The APPA Task Force commends the drafting team on the overall development of CIP-011-1. We believe this document is another step in the right direction of cyber system protection. We did, however, notice a theme throughout the requirements that caused us some concern. There is an IT focus to a number of the requirements. The drafting team seemed to be focusing on control centers when developing requirements to protect critical facilities. As a result, a number of the requirements are not practical for remote substations and generation stations, that may be owned by many entities and operated by only one of them, or another entity. What may be simple in a control center environment may be next to impossible for a transmission substation or a generator.
54.47	Constellation Energy Commodities Group Inc.	The blank boxes in CIP-011 tables need to be filled in. While the intent appears to be that if the box is blank the control is not required, by leaving it blank, liability questions could be raised. Compensatory measures should be allowed in the compliance structure. Entities may find that alternative, but comparable protection measures will better fit the circumstances of their system.An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance

#	Organization	Question 54 Comment
		documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for being audited in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.The Implementation Plan should allow for sufficient time to complete the comprehensive task of identifying and categorizing BES cyber systems.The R3 and R4 tables should address each requirement. All tables should be completed in full stating either not applicable or required.
54.48	Midwest ISO	The categorization approach in CIP-010 appears to require any BES Cyber System that touches the BES in any way to be included no matter how minimal the impact of the Cyber System on the BES, we are concerned that the Midwest ISO energy and ancillary services markets will be impacted. We believe that market portals could become High, Medium or Low Impact facilities and, thus, require application of the CIP standards or modification of the systems to isolate them so that CIP standards don't apply. Our conservative estimate is that we could easily spend in excess of $10 million dollars without anywhere close to this impact because our existing processes would prevent the market from negatively impacting reliability. We request that the drafting team make clear that market systems should not be included per NERC standard development tenets. In some cases, drawing in market systems could present impossible challenges. For instance, if a market portal becomes a High Impact BES Cyber System, CIP-011 R4 appears to require that we would have to conduct personnel risk assessments on all users which would include thousands of employees from market participants submitting bids and offers. State laws make this impossible. The drafting team could help solve this problem by making clear that personnel does not include market participants/customers who already have significant financial incentive to enter good bid and offer data. Opportunity costs do not appear to be considered in the development of these standards. All business resources are limited. Requiring registered entities to focus on these specific issues may divert attention away from other important cyber and physical security initiatives and work that offer greater improvements to reliability.We are also concerned that cyber and physical security could initially be compromised as entities focus on becoming compliant for Low and Medium impact cyber systems. Likely, High Impact Cyber systems will meet the new requirements because they were likely Critical Cyber Assets under the existing CIP standards. Thus, their reliability could degrade as entities may lose focus on the High Impact BES

#	Organization	Question 54 Comment
		Cyber Systems.
54.49	Florida Municipal Power Agency	The drafting team seems to have added an objective into the requirements which adds ambiguity to the requirement. For instance, R2 adds the phrase “to ensure that personnel maintain awareness ...” which adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? If the drafting team wishes to add an objective to each of the requirements, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished.Throughout the standard, there is confusion among the terms “grant” and “authorize”. “Authorize” is senior manager approval, “grant” is giving the person a key, keycard, or user account. The requirements should keep these two concepts clear. For instance, in 5.5, “authorize” should be changed to something like: “Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized such access”.Overall, added complexity to the cyber systems will reduce the reliability of the BES, so this needs to be kept in mind when drafting these standards.Almost all of the standards need to have stronger language in them to remove ambiguity and give specific guidelines as to what it expected.
54.50	NextEra Energy Corporate Compliance	The following are specific language changes for clarity:1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To provide clear understanding of the protections that are to be applied to BES Cyber System Components identified as a result of the applicable of CIP-010-1 to the Responsible Entity’s BES.Also, for clarity, this section should be re-written as follows:R2. Each Responsible Entity shall reinforce sound security practices to all employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access to a BES Cyber System Component reinforcements in sound security practices at the beginning of each quarter. The Responsible Entity also has the discretion to reinforce sound security practices at any time, it deems appropriate. The reinforcement may be delivered via e-mail, intranet, posters, classes or other educations methods. .R3. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall ensure the personnel requesting access completes cyber security training consistent with that required in. CIP-011-1 Table R3 - Cyber Security Training,.3.1. For employees and contractor personnel requesting

#	Organization	Question 54 Comment
		authorized cyber access, this cyber security training shall cover the following: o The proper use of BES Cyber Systems o Physical access controls to BES Cyber Systems o Visitor control program o The proper handling of BES Cyber Systems information and storage media o Identification and reporting of a Cyber Security Incident For employees and contractor personnel requesting only unescorted physical access, this cyber security training shall cover the following: Procedures for not intervening with a BES Cyber System ComponentVisitor control programIdentification and reporting of a Cyber Security Incident 3.2. For employees and contractors personnel who engage in the operation or control of the BES via authorized cyber access to a BES Cyber System Component, cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber System Components and BES Cyber Systems. 3.3. For employees and contractor personnel who have a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures.3.4. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures. 3.5. Each Responsible Entity shall maintain document for each employee and contractor personnel required to take cyber security training as required in R3 and its sub-requirements that the training was conducted at least once every 12 months plus or minus one month. R4. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall perform or have performed a personnel risk assessment on the employee or contractor personnel requesting access consistent with CIP-011-1 Table R4 - Personnel Risk Assessment, expect as prohibited or limited by federal, state, provincial, and local laws, and existing collective bargaining unit agreements. 4.1. This personnel risk assessment program shall at a minimum include: o Identity verification via photographic identification documentation issued by a government agency (i.e., Federal, State or Provincial); and o A seven year criminal history screened against specific criteria developed and documented by the Responsible Entity. The seven year criminal history shall include a records check that covers all locations where, during the previous seven years up to date the check was performed, the subject has resided, been employed, and/or attended school for six months or more, including

#	Organization	Question 54 Comment
		current residence regardless of duration. 4.2. Each Responsible Entity shall document the results of each personnel risk assessment. 4.3. Each Responsible Entity shall update or have updated each personnel risk assessment at least once every seven years after the initial personnel risk assessment.
54.51	Entergy	The industry has now had experience grappling with a one-size-fits-all set of cyber security standards' requirements for its grid and generation control systems. At a high level of abstraction the problems with this approach are manifest in two major ways. The first concerns the age of the control system components we have at work relative to cyber vulnerabilities, threats, and hence risk. In brief, our control host systems and operator consoles by and large today use mainstream "IT" commercial off the shelf computer (COTS) hardware, operating systems, and application code bases. These are the very same networked-computing systems components that are widely hacked on the Internet and within mainstream commercial businesses around the world, and accordingly represent highest risk to reliable grid operation from cyber malfunction or nefarious attack. If hacked, they provide the ability for perpetrators to commandeer and use the systems against us - which represents the worst case scenario (e.g., a widespread unplanned "load shedding event" - trip all). On the other far extreme, we have often decades-old computing equipment still widely used "in the field" at substations, switching stations, hydro dams, etc. Increasingly these field sites are connected to control hosts over ("Internet") routable protocol communications networks, and increasingly emergent wireless communications transmission technologies. But there also remains very high dependency on "legacy serial" and "POTS" dial-up communications. So, we have both very old and very new networked-computing control systems technology woven together that requires some kind of cyber security protection. The second major distinction is the physical orientation of control host and generating plant sites on the one hand, and the far flung field assets on the other. The former are typically referred to in security circles as "bastion sites," in that they can be defended in much the same way as castles of old using concentric rings of physical defenses, complimented by armed guards. The field sites on the other hand have more in common with gas and oil pipelines, rail infrastructure, and the like that are characterized by long stretches of geographical separation between sites. These are hard to physically defend economically, and, through use of protocols that by design enable "network navigation" akin to being able to telephone-dial anyone in the country on demand, provide an attack vector path back to control hosts, and therewith also creating opportunities for "island hoping" from one organizational network to another. Given these two decidedly different continuums of variables that the industry needs to

#	Organization	Question 54 Comment
		defend, “one size fits all” standards’ requirements result in situations where the requirements are expensive overkill in one circumstance, and if watered-down to ease this burden do not provide robust enough protections for the circumstance at the other end of the spectrum. The only standards-writing approach that affords appropriate cost-effective security is to define granular sets of standards that are specific to the real vulnerabilities and threats incumbent to each scenario. From this perspective, specific recommendations for improving the current Version 4 draft CIP Standards are outlined below.The SDT was directed in Order 706 to consider adaptation of the NIST Security Risk Management Framework, especially noting SP800-53. This comment is neither about the individual requirements themselves nor the fact that most of the specific CIP-011-1 requirement language was drawn from the DHS Catalog of Controls. Rather, this comment focuses on the fact that the SDT has diverged from FERC directive in not employing a major foundational construct of SP800-53. Specifically, the SDT has developed a single set of requirements, and then through use of sub-requirement tables indicate in binary fashion whether or not each (sub)requirement of note is applicable or not, based strictly on the high-medium-low “impact categorization” based exclusively upon a facility’s size (electrical operating characteristics). Contrast this with the SP800-53 paradigm, where there are three graduated, hierarchical layers of cyber security control and countermeasure requirements. First, there is a baseline set of requirements, which applies for all cyber systems, and these are the only requirements applicable for low-impact-on-mission cyber systems. Then, there is a second and third set of requirements that apply cumulatively for medium and high mission-impact cyber systems respectively. The SP800-53 approach is responsive to the stated FERC preference that there be a baseline set of requirements that must apply for all grid BES Cyber Systems/Components. Draft CIP-010-1 is not responsive to FERC Order 706 - many requirements as stated in the Standards’ language simply do not apply for BES Cyber Systems/Components in use at low and medium-sized grid sites.Recommendation: A) Modify the categorization of grid assets (Attachment II) into two groups:i) “Bastion Installations” consisting of data centers, control centers, and generation sites. Rationale: At least the ‘data center’ part tends to employ mainstream IT COTS HW/OS/and to some degree appl code; and, physical security measures can be used to greater advantage as compensating measures where cyber security measures may be difficult to implement for a variety of reasonsii) “Grid Field Assets” consisting of any physical site that does not have a control host/control center within their physical perimeters, regardless of what protocols are in use. The distinction again revolves around

#	Organization	Question 54 Comment
		physical security, in this case the difficulty in physically securing far flung field sites.B) Create layers of requirements akin to the SP800-53 paradigm, labeled 'a-z': i) The lowest enumerations being baseline requirements; e.g., 'a' could be associated with bastion installations, and 'b' could pertain for field grid asset sites. Important distinctions at the baseline can pertain for each site type.ii) Similarly, create appropriate sets of succeeding requirements applicable specifically to each column (bastion/field) depending on the type of data networking communications employed. This way appropriate requirements - not more nor less than necessary - and be specified for the unique characteristics and attack surfaces posed by each technology. As technologies are retired, e.g., serial legacy, POTS dial-up, so can entire categories of requirements.C) Create a "Scoping Table" consisting of: i) Two columns: Bastion/Field - #1 above); and,ii) X number of rows: #2 above - list of different communications technologies, i.e., routed, legacy serial, dial-up, non-routed LAN, non-routed wireless, etc., as the SDT deems appropriate. D) Apply requirements sets (a-z) as appropriate within each box on the grid.2) Entergy submits that NERC's intention to address the following FERC Order 706 directives in action subsequent to adoption of CIP Version 4 will create undue hardship for the industry. The following Order 706 directives are central to implementation of any organizational cyber security program, and it is unreasonable, inefficient, and potentially financially wasteful to require the industry to implement one approach per Version 4 Requirements, and then be made to re-visit entire cyber security programs in order to comply with post Version 4 changes. Entergy submits that the entire puzzle should be addressed at once, i.e., including the following FERC Order 706 directives, at the same time while recasting the CIP Standards under Version 4:...develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter... a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.... consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... revise the Reliability Standard to require two or more defensive measures.... modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years... that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a

#	Organization	Question 54 Comment
		physical security perimeter around critical cyber assets.... consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.... to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.... to revise CIP-009-1 to require data collection, as provided in the Blackout Report.... proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.Entergy recommends that NERC appeal to FERC for permission to extend the deadline for final Version 4 drafting a modest amount of time necessary for the entire puzzle to be grappled at once. The industry is now hardly complete in implementation of CIP V1-V3 Standards' Requirements. The prospect of having to endure adaptation to two more waves of fundamental change to the tenets of these standards is not only onerous, but also not responsive to the imperative to provide service at lowest reasonable cost to ratepayers. We didn't build our national electric infrastructure overnight, and apt response to relatively recent emergence of cyber security threats will not be accomplished overnight either.
54.52	IRC Standards Review Committee	The organization of the 32 requirements and all of the subrequirements is lesser of a concern to us, although separate standards that group similar requirements allows for better administration. The greater concern is the degree of specificity of many of these standards. As discussed in the response to Q #8, many of these requirements go into exacting detail specific to technology and may duplicate either other industry standards or practices already employed. Many of these requirements can be elevated to "higher level" requirements that requires certain types of protections, e.g. - require user access identification, rather than specific password practices. For examples, the list of criteria that are included in Requirements Table R9, the details in the Tables for R10 and R11, and the specific treatment of wireless access in R12, to name a few.
54.53	Public Service Enterprise	The requirements for wireless and remote access (R11 to R14) are not well integrated with other

#	Organization	Question 54 Comment
	Group companies	requirements for access to BES Cyber Security Systems (R7 to R10).
54.54	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	The table format is great, makes it very easy to see what applies.If we say “CIP-011-1 R3.1” do you know what we am referring to? There is a sub-requirement 3.1 as well as a line 3.1 in Table R3. This could lead to confusion. Suggest extending the table to cover all sub-requirements, or otherwise avoid repeating numbers. This occurs only in R3 and R4.Regarding R21, no definitions have been provided for “other cyber systems” and “Cyber System Components” (without “BES” in the phrase.) Note that “Cyber System Components” is capitalized as if it was defined, but no definition exists or is proposed. While “other cyber systems” is not capitalized, it should also be defined to avoid any ambiguity over what the SDT intends. We appreciate the objectives that the SDT has included in the requirements, since this will help us to see the SDT’s intent. There is the risk, however, that auditors will see this as more than guidance when placed in the requirement. For example, an auditor might read R5 and R6 as requiring the prevention and/or detection of all unauthorized physical access, and find an entity non-compliant for an undetected or un-prevented intrusion. We suggest the objectives (“to prevent..”, “to ensure..”, etc.) be placed in the guidance document, or otherwise be removed from the requirements. Note that some of these objectives when read as requirements are absolute, such as R14; “..to ensure no unauthorized access is allowed.
54.55	MidAmerican Energy Company	The term "Annual" is not defined. Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual".The following provides a summary of the reasons for using a definition of “12 months not to exceed 15 months.” o It does not force “creep.” A definition of 365 days or 12 months, without a “not to exceed” clause means that work must be planned to be done enough before the 365 days to allow time for unexpected situations. This can result in doing “annual” requirements every 10 months or less to ensure compliance is not jeopardized. o It does not jeopardize compliance for either delivery or supply due to current implementation plans. A calendar year definition could unintentionally jeopardize compliance if delivery did not complete a task between June 30 and Dec. 31, 2009. o There is no effect of leap years, which could be a problem with a definition of 365 days._____Requirements that are defined to be completed within x hours are impractical and unnecessary. Entities do not currently document the precise hour that (as an example) a termination takes place. Thus hourly requirements are impractical to measure or audit.

#	Organization	Question 54 Comment
		Convert all hourly requirement as follows: o Convert 1 Hour requirements to "As soon as possible not to exceed date reported". o Convert 4 Hour requirements to "As soon as possible not to exceed date reported". o Convert 6 Hour requirements to "As soon as possible not to exceed date reported". o Convert 12 Hour requirements to "As soon as possible not to exceed date reported". o Convert 24 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 36 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 48 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 72 Hour requirements to "As soon as possible not to exceed second day from date reported"._____The following FERC Directives need to be addressed with version 1 of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Entities will be required to make additional expenditures at greater cost if these issues are resolved in later versions. NERC should ask FERC for more time to implement version 1 if necessary.
54.56	Dairyland Power Cooperative	There are very few requirements that apply to low impact systems and many that do not apply to medium impact systems. Considering that many high impact systems will connect with lower impact systems, how will data integrity be adequately implemented? Consider a large RTO/ISO connecting a shared communications system to all entities in a region, regardless of impact to the BES.The standard basically excludes serial communications from being governed. This not only does not address protecting serial systems, but it introduces oddities and ambiguities about routable connections in relation to serial connections. There are security questions, as well as questions as to how such connections will be viewed by an auditor. Serial communications should not be ignored.
54.57	Ameren	These standards will require a substantional amount of effort to implement for entities while also maintianing compliance with the previous versions of the CIP standards, how will the implementation schedule address this? Will their be a period were the entity does not have to comply with the old

#	Organization	Question 54 Comment
		standards while implementing the new standards, for examle 30 days to 90 days while the entity is updating systems or updating/revising procedures for the new standards. Also, the local definitions should be included in the NERC glossary of terms rather than by the standard to which they apply.
54.58	Bonneville Power Administration	This is far better than the current standards. The requirements are more straight forward by not cross referencing each other in separate standards. Much time is spent "mapping" out how the standards relate to each other and under what specific requirements. If misinterpreted it could lead to potential violations. This is a much better approach. Not directly relating to the newly proposed standards but still a concern is the time for implementation. Numerous resources have been extended and significant dollars spent to meet the current requirements. There needs to be sufficient time to review the new standards, identify Cyber Systems and allow for proper prior planning to physically protect these systems. Depending on the category, low-high, significantly more dollars could be spent. There needs to be sufficient time to address the new standards and implement in a manner that is cost effective. The overall approach is superb: target the standards only at systems that can actually affect the BES in near-real time, include other systems only to the minimum extent necessary, require outcomes rather than specify actions. However, this draft has some wording issues that apparently have inadvertently broadened the scope far beyond the intent of the SDT, or even practicality. As described above, correcting these errors will produce a set of standards that enforce security where it needs to be, but do not waste time, money, and people addressing tasks that do not improve the security of the BES. In particular, we find that the following questions address issues that must be corrected before the standards could be acceptable:- Q5, addressing CIP-010 Table R3 Section 3.2- Q12, addressing CIP-011 Table R3 Section 3.2- Q13, addressing the the definition of "External Connectivity". Note that several other questions rely upon changing this definition.- Q16, addressing CIP-011 Table R5, sections 5.8 and 5.9- Q22 and Q23, addressing revocation time limits- Q24, addressing authentication schemes- Q27, definition of "Remote Access"- Q32, addressing revocation of remote access- Q33, addressing Table R14 Sections 13.2 and 14.4- Q35, addressing Table R16, Section 16.2 and patch risk assessment- Q35, addressing Table R17, Section 17.2 and disabling of physical ports- Q35, addressing Table R18, Sections 18.1, 18.2, 18.3, and 18.4- Q37, addressing Table R20, Sections 20.1, 20.2, 20.3, 20.6- Q37, addressing Table R21, Section 21.1- Q38, addressing the second part of the definition of electronic access point. This is the most serious flaw in the standard. It must be corrected.- Q40, addressing Table R23 section 23.7- Q42, addressing the definition of

#	Organization	Question 54 Comment
		sensitive information- Q44, addressing Table R24, Section 24.1 and 24.3- Q47, addressing Table R26, section 26.2- Q51, addressing Table R30, Section 30.5- Q51, addressing Table R31, sections 31.1 and 31.2- Q53, addressing TFEs Overall, an excellent start. Here are some additional suggestions:1. In all cases - Write the standards to identify the outcome of the requirement. Never say how to do something, say what you intend for it to accomplish. Let the Responsible Entities figure out the "how".2. Use Industry Standard wording wherever possible. For example, the term "Hardened" means one thing in IT and another in a substation.3. Define any terms that may present confusion - Example - Ports and services. There is a common IT understanding when you hear that term. It is almost always assumed to mean logical ports 0 to 65535 and the networking services they support. However, it can also mean physical ports like Ethernet jacks, RJ45, Serial connectors, parallel connections etc. If there is a question, put it in the definitions.4. Wherever possible, include all the elements of a standard into one standard. Only break requirements apart where it makes real sense to do so. So If you get to R32 and find that something there seems to fit in 20, go back and put it there rather than making a reference back. 5. Keep paring this down in size. It is so much better.6. If any of your experts know that equipment used in the electrical generation and distribution industry cannot perform specific functions, don't write the standards to say they have to.7. There were questions in the May webinar about the meaning of "revocation". Our suggestion is this: revocation is the act of ensuring that a person can no longer gain access to a system, physical area, or information. It can be accomplished directly or indirectly. For instance, if a cyber asset is only accessible from within a physical facility, then denying physical access to the facility also denies cyber access to the cyber asset. If sensitive information on a system resides only in electronic form on particular servers, then denying cyber access to those servers denies access to the information. The emphasis should be on the denial of access, not how that denial is accomplished.Definition of "annual" or "annually": There are numerous occurrences of these terms in the Requirements. Also now, Requirements state that activities must occur “at least once every 12, 24, or 36 months.” Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. “/A/t least once every 12 months” could lead to some confusion. Let’s assume that the event occurred on July 15, 2010, and again on March 15, 2011. That is “at least once every 12 months.” But it raises the question of when the next activity or compliance event must occur. Is it no later than July 15, 2011, or no later than March 15, 2012? The exact questions could be asked for events that are supposed to occur “at

#	Organization	Question 54 Comment
		least once every 24 or 36 months."Following on to comment 1 immediately above, there are two other phrases that could be used depending on what NERC intends. o "every 12 months" - in this case, the event would occur on the same date each year. This would be virtually impossible. Same concern with "every 24 or 36 months." o "within 12 months of" the event - in this case let's assume that the event occurred on March 15, 2010. The next event would have to occur no later than March 15, 2011, but could occur earlier (let's say it occurred on December 15, 2010). If it occurred on December 15, 2010, the next event would have to occur no later than December 15, 2011. The same example with different dates would work for "at least once every 24 or 36 months."The SDT should be very specific as to what it means for how frequently the events referenced above must occur. BPA appreciates the opportunity to provide comments. Thank you.
54.59	MRO's NERC Standards Review Subcommittee	We believe all of the requirements that specify something to be completed within X hours would be better suited to the following language: "As soon as practical, but not to exceed x business days from the date reported". This would maintain the spirit of the requirement, while also allowing for more practical time frames.With so many auditable elements included within the requirements, we believe the VSL's cannot be written with the current zero-defect mentality. We feel a practical approach is required, where minor issues are allowed to be addressed without representing immediate non-compliance and associated investigations and settlement proceedings, but instead are identified and scheduled for corrective action.We understand the burden on the drafting team to meet FERC's deadlines, but we would propose that all outstanding FERC directives be addressed as part of the current process, as opposed to leaving some items for a later date.
54.60	Idaho Power Company	We commend the SDT on its efforts to draft a standard that meets the FERC directives but is feasible for the industry to implement. That is an extremely difficult assignment. This version will greatly expand the number of cyber assets that are impacted by the CIP requirements and represents a major shift in the identification and classification of an entities BES cyber systems. We are certainly willing to implement the standards because we understand the impact of failure to do so. However, the standards must be accompanied by as much guidance documentation as possible along with realistic implementation plans that take into account the technology required, time required to realistically implement the controls, the fact that registered entities must first assess the financial impact and then

#	Organization	Question 54 Comment
		budget appropriately, and the massive volume of work that implementation represents.
54.61	Xcel Energy	We do not agree that Low impact systems should have mandatory, enforceable cyber security standards. By their very definition, Low impact systems have very little potential to impact the BES. As such, cyber security controls on these systems is best left to the business judgment of each individual entity. The terms defined throughout the standard have not followed the convention of being capitalized. They should be capitalized so that it is clear to the reader that they are defined terms when they are used later in the standard. The Standard would be enhanced if it were to differentiate between software based versus firmware based devices.The Standard would also be enhanced if it were to separately define requirements for Control Centers, Substations, and Generation Facilities. The cyber security issues between these different types of facilities are vastly different. Transmission Control Centers are typically fully digital control systems with the ability to have wide area impacts. On the other extreme, where Generation facilities typically have digital systems are for retrofits to older, analog systems controlling individual components within the facility, such as digital feedwater or digital turbine controls. These are much different that Transmission Control Centers as they have only limited, local impact. Additionally, they typically have mechanical controls that can override the digital systems providing limited, if any benefit from protecting the digital aspects of the system from malicious attacks.
54.62	We Energies	We Energies agrees with EEI: Please see the earlier discussion about identification of a rational and understandable threat basis that should be used when constructing security requirements. The requirements should focus on the highest probability risks that will have the most negative impact. The requirements should not treat all threats and impacts equally.
54.63	Duke Energy	We had previously gone a long way towards getting common understanding on terms such as “Critical Assets”, Critical Cyber Assets”, “Electronic Security Perimeter” and Physical Security Perimeter”. Moving away from these terms in the current Version 4 draft creates uncertainty.Tables and subrequirements should have different numbering schemes so that, for example, there are not two 3.1 listings.If the standard is broken into smaller standards, please provide separate measures for each standard.

#	Organization	Question 54 Comment
54.64	Hydro One	We noticed that combined CIP-011-4 standard excluded vulnerability management program. We'd like to know what the rationale was behind this decision and if this might be considered in the next draft.Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.
54.65	GTC & GSOC	We recommend a local definition of "Implement" should be added to CIP 011: "Implement means to put into place and consistently utilize. An entity has implemented a policy, procedure, or plan when it has created such policy, procedure or plan and consistently uses it in appropriate circumstances."Throughout the standards the inclusion of the words "for external connectivity only" in the tables is redundant and confusing. If used at all, the qualifier should be on "access" in the text of the standard rather than in the table.We recommend Annual be defined as recurring at least once every Calendar year and at least once within any thirteen (13) consecutive calendar months. Otherwise, annual training will necessarily have to take place earlier each calendar year to ensure all personnel are trained within twelve (12) months.We appreciate the significant effort that the NERC Cyber Security Order 706 Standards Drafting Team has put into developing these proposed standards and communicating them to the industry, especially the CIP Workshop held in Grapevine, TX. We are in full support of the NERC standards development process for the development of reliability standards to secure and protect North America's critical electric infrastructure. In particular, we appreciate the multiple opportunities to guide the development of the CIP standards through both informal and formal comment periods. We are supportive of the proposed standards. We believe these standards are a significant step forward in terms of being able to clearly understand the expectations that are placed upon the entity as well as the security that they provide for the Bulk Electric System.

#	Organization	Question 54 Comment
54.66	PNM Resources, Inc.	We suggest not removing explicit examples from the language of the standards. The incorporation of examples provides clarity and brightline guidance that improves a Responsible Entity's opportunity to comply with the standard. The introduction of new and additional "flexibility" can lead to ambiguity and differences of opinion between the entities and auditors and creatr more opportunities for Regional Entities to allege violations.
54.67	MWDSC	When looking at logical tasks to mitigate risk, e.g., malicious code propagation, could a malicious code in one cyber component affect another component and result in a change in the impact categorization, e.g., low vs medium?
54.68	Progress Energy - Nuclear Generation	Yes, see comments a - f below.a. Comments: Attachment 1 included in responses above follows this question. To obtain full benefit of this review, see Attachment 1.b. The security controls in CIP-011-1 should provide for acceptance of Common Controls as defined by NIST 800-53. CIP-011-1 would offer a more consistent approach in cyber security regulation by considering the mature physical security programs, engineering control programs, emergency plans and physical segregation programs within the nuclear industry that offer alternative countermeasures. These countermeasures provide at least the same degree of cyber security protection as the corresponding cyber security control. c. NIST 800-53 establishes provision for tailoring security controls and states that the level of detail required in documenting tailoring decisions in the security control selection process is strictly at the discretion of the organization consistent with the impact level of the information system. CIP-010-1 and CIP-011-1 should allow use of this provision in the nuclear industry consistent with acceptance by nuclear regulators.d. Nuclear applicability is specified in CIP-010-1, Section 4.2.1. The following comments are based on applicability to nuclear generating facilities: o Definitions for Bulk Electrical System (BES) Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the NRC in NEI 08-09, Revision 6, for Critical System and Critical Digital Asset. Recommend, that for nuclear systems subject to FERC Order 706-B, that definitions for FERC and NRC regulated systems be consistent. o CIP-010-1 requirement R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? o The implementation schedule for CIP-010-1 and CIP-011-1 versus CIPs 002 through 009 requires doing the same reviews twice and is an unnecessary burden on

#	Organization	Question 54 Comment
		nuclear licensees as well as other FERC critical assets.e. Several requirements include periodic review of controls (e.g., R8.2, R12.1). This CIP should contain a provision that permits nuclear facilities to use the periodicities in its NRC approved Cyber Security Program in lieu of those in the CIP standards. This allowance would minimize the administrative burden of having two sets of requirements for the same Cyber Security programmatic element so that plant digital systems that support safety, security, EP or BOP functions are not regulated differently. The following are used to establish frequency or periodicity for security controls with identified durations: o NRC Regulations, Orders o Operating License Requirements (e.g., Technical Specifications) o Site operating history o Industry operating experience o Experience with security control o Guidance in generally accepted standards (e.g., NIST, IEEE, ISO) o Audits and Assessments o Benchmarking o Availability of new technologies. f. R27.1 - The definition of "Cyber Security Incident" should be revisited in light of current definitions, especially NRC and NEI, and revised to align with the definition of "Cyber Attack." It is not on the list of terms to be defined. From NERC Glossary of Terms used in NERC Reliability Standards updated April 20, 2010, the "Cyber Security Incident" definition is: o Any malicious act or suspicious event that:o Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,o Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.o It is unclear what NERC does with cyber incident reports and whether these reports are consistent with those required by the NRC in the event of a "cyber attack." Progress Energy Nuclear Generation Group CommentsCIP- 011-1ATTACHMENT 1NIST Security Control Description NIST 800-53 NEI 08-09 NEI 08-09 Description CIP-011-1 CIP-011 Description NRC CommentsSecurity Planning Policy and Procedures PL-1 N/A N/A R1 Security Governance and Policy 50 App B 50 App E73.5473.5573.56 The development and implementation of cyber security policies that address the requirements identified in R1 are mandated for nuclear by one or more Code of Federal Regulations (CFR). This requirement duplicates and/or is not consistent with the CFR and could lead to regulatory uncertainty. Review of cyber security is mandated by 73.55(m) and R1 conflicts with its duration. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Awareness AT-2 E9.2 Awareness Training R2 Personnel Training, Awareness and Risk Assessment 73.5450 App B Training requirements for nuclear personnel are established by CFR. R 3.3.2 would result in personnel without a need to know becoming knowledgeable in technical aspects of digital equipment. R3.3.4 is not required for users to perform

#	Organization	Question 54 Comment
		their job. This conflicts with 73.54 requirements that personnel are trained to the extent necessary to perform their assigned duties. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Training AT-3 N/A N/A R3 Personnel Training, Awareness and Risk Assessment 73.5473.55 Physical and logical access to plant digital systems is governed by CFR. Personnel who are granted access to these systems are required to complete training that result in their receiving formal and documented Qualifications. Requalification is at established intervals required by plant procedures. Whether the plant system performs functions associated with safety, security, emergency preparedness or BOP, the requirements are the same. Additional training and duration not consistent with established mature training programs would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant. R4 Personnel Risk Assessment 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. Results are documented and stored in Records. The requirements in R4 conflict with the requirements in the CFR that nuclear personnel supporting plant system performs functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from requirement R4. R5.1 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. The nuclear plant is protected by armed security officers and other protective strategy that restricts access. The requirements in R5.1-3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.2 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.2 are covered by the CFR for restricting physical access for all plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.3 Physical Security for BES Cyber

#	Organization	Question 54 Comment
		Systems 73.55 Nuclear personnel must pass through security access points before being granted physical access to nuclear plants. Automated scanning records entry. The requirements in R5.3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.4 Physical Security for BES Cyber Systems 73.55 Visitors must receive approval prior to arriving at the security access points and are subject to search before being granted physical access to nuclear plants. Entry and exit are documented. The requirements in R5.4 are covered by the CFR for nuclear visitors supporting plant systems performing functions associated with safety, security, emergency preparedness, BOP or other. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Authorizations PE-2 E5.4 Physical Access Authorizations R5.5 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.5 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Control PE-3 E5.5 Physical Access Control R5.6 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to annual retraining in order to maintain unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.6 conflict with the CFR that cover access authorization for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.7 Physical Security for BES Cyber Systems Part 2673.56 Requirements for nuclear personnel terminated for cause are covered by the CFR. The requirements in R5.7 conflict with the CFR that direct termination for cause of nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting

#	Organization	Question 54 Comment
		nuclear facilities from this requirement. R5.8 Physical Security for BES Cyber Systems 73.55 N/A to nuclear - applicable to Control Center R5.9 Physical Security for BES Cyber Systems 73.55 Requirements for nuclear personnel who no longer require physical access are covered by CFR. The requirements in R5.9 conflict with the CFR that covers removing physical access for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.10 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are trained and qualified to provide continuous escort for visitors while they are granted physical access to nuclear plants. The requirements in R5.10 are covered by the CFR for nuclear personnel who escort visitors supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R5.11 Physical Security for BES Cyber Systems 73.55 Unauthorized physical access is handled by armed security officers in nuclear security. The requirements in R5.11 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R6.1 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.1 are covered by the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.2 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.2 are addressed in the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.3 Physical Access Control Systems 73.55 Physical access control systems are maintained and tested per CFR requirements. The requirements in R6.3 are addressed in the CFR. Therefore, this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement.Account Management AC2 D1.2 Account Management R7 Account Management Specifications Consistent with nuclear cyber security plan.Least Privilege AC6 D1.6 Least Privilege R8.1 Account Management Implementation Consistent with nuclear cyber security plan.Account Management AC2 D1.2 Account Management R8.2 Account Management Implementation Duration is inconsistent with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP.Account

#	Organization	Question 54 Comment
		Management AC2 D1.2 Account Management R8.3 Account Management Implementation Consistent with nuclear cyber security plan. R9.1 Personnel Terminated for Cause Part 2673.56 Duration is inconsistent with nuclear requirements.N/A N/A N/A N/A R9.2 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R9.3 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterAccount Management AC2 D1.2 Account Management R9.4 Access Revocation Duration is inconsistent for removal of access for personnel who no longer require access with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP. Identification and Authentication (Non-Organizational Users) IA-8 D4.2 Identification and Authentication (Non-Organizational Users) R10.1-5 Account Access Control Specifications The control of passwords contained in R10.1 - 8 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should include the provision contained in note 1 for digital assets that are not technically capable of supporting some of the password requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Least Privilege AC6 D1.6 Least Privilege R10.6 Account Access Control Specifications The control of passwords contained in R10.6 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Access Enforcement AC3 D1.3 Access Enforcement R10.7 Account Access Control Specifications The control of passwords contained in R10.7 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as system and security administrative accounts. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by

#	Organization	Question 54 Comment
		nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Separation of Duties AC5 D1.5 Separation of Functions R10.8 Account Access Control Specifications The control of passwords, contained in R10.8, is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Wireless Access AC18 D1.17 Wireless Access Restrictions R11.1 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.2 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.3 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R12 Wireless and Remote Electronic Access Management 73.5573.56 Duration is inconsistent with nuclear requirements for reviewing remote access. Other physical security and access authorization nuclear regulation ensures personnel who have remote access are trustworthy and reliable therefore this type of review is not justified.N/A N/A N/A N/A R13.1 Remote Access Revocation (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R13.2 Remote Access Revocation (Transmission) N/A to nuclear - applicable to TransmissionRemote Access AC17 D.1.1 Access Control Policy and Procedures R13.3 Remote Access Revocation Part 26 73.56 Duration is established in nuclear requirements for removal of access for personnel who no longer require remote access.Remote Access AC17 D.1.1 Access Control Policy and Procedures R14.1-3 Wireless and Remote Electronic Access Control Consistent with nuclear requirements.System Use Notification AC8 D.1.8 System Use Notification R14.4 Wireless and Remote Electronic Access Control Inconsistent with nuclear requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. Add provision for this requirement to be implemented if technically supported.Malicious Code Protection SI-3 E3.3 Malicious Code Protection R15 Malicious Code Consistent with nuclear regulation.N/A N/A

#	Organization	Question 54 Comment
		D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.1 Security Patch Management Duration is inconsistent with nuclear regulation otherwise requirements are consistent. D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.2 Security Patch Management Consistent with nuclear regulation.N/A N/A D5.4 Hardware Configuration R17 System Hardening Consistent with nuclear requirements.Information System Monitoring SI-4 E3.4 Monitoring Tools and Techniques R18.1 Security Event Monitoring Consistent with nuclear requirements.Information System Documentation SA-5 E6 Defense-In-Depth R18.2 Security Event Monitoring Consistent with nuclear requirements.Incident Monitoring IR-5 E7.5 Incident Monitoring R18.2 Security Event Monitoring Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R18.4 Security Event Monitoring Duration for maintaining logs is inconsistent with nuclear requirements. The duration for maintaining logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A E6 Defense-In-Depth R18.4 Security Event Monitoring Duration for review of logs is inconsistent with nuclear requirements. The duration for reviewing logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R19 Communication and Data Integrity in a Control Center N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R20 Electronic Boundary Protection Consistent with nuclear regulation other than duration. The duration for reviewing alerts and logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R21.1 System Boundary Protection N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R21.2 System Boundary Protection 73.54 Consistent with nuclear requirements. R22 Protective Cyber Systems (duplicate of R14,16,18,23) Duplicate - (duplicate of R14,16,18,23); Remove not neededInformation System Component Inventory CM-8 E10.9 Component Inventory R23.1 Configuration Change Management 73.54 Consistent with nuclear regulation.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.2 Configuration Change Management 73.5450 App B Consistent with nuclear regulation.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.3 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be

#	Organization	Question 54 Comment
		regulated differently.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.5 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.6 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Information System Component Inventory CM-8 E10.9 Component Inventory R23.7 Configuration Change Management 73.54 Consistent with nuclear requirements.Media Protection Policy and Procedures MP-1 E 1.1 Media Protection Policy and Procedures (SGI, Non-SGI, 2.390) R24.1 Information Protection Consistent with nuclear requirements.Information Output Handling and Retention SI-12 E3.10 Information Output handling and Retention R24.2 Information Protection Consistent with nuclear requirements. R24.3 Information Protection 73.56 The requirements in R24.3 are covered by the CFR for authorization to view security sensitive information for plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.4 Information Protection 73.56 The requirements in R24.4 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.5 Information Protection 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. to ensure their trustworthiness and reliability. This requirement is not necessary for nuclear personnel. Consider exempting nuclear facilities from this requirement.Media Sanitation MP-6 E 1.6 Media Sanitation and Disposal R25 Media Sanitation Consistent with nuclear requirements.Maintenance

#	Organization	Question 54 Comment
		Personnel MA-5 E4.3 Personnel Performing Maintenance and Testing Activities R26.1 Maintenance Consistent with nuclear requirements.Maintenance Tools MA-3 E4.2 Maintenance Tools R26.2 Maintenance 50 App B Consistent with nuclear requirements.Incident Handling IR-4 E7.1 Incident Handling R27.1 Cyber Security Incident Response Plan Specifications DG-501950 App B50 App E The requirements in R27.1 are covered by the CFR for classifying events as Cyber Incidents whether the plant systems performing functions associated with safety, security, EP or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently.Incident Handling IR-4 E7.4 Incident Handling R27.2 Cyber Security Incident Response Plan Specifications 73.54 Consistent with nuclear regulation.Incident Reporting IR-6 N/A N/A R27.3 Cyber Security Incident Response Plan Specifications 73.5473 Appendix GDG 5019 This requirement should be addressed by NRC and FERC/NERC to ensure consistency in reportability requirements.Incident Response Testing and Exercises IR-3 E7.3 Incident Response Testing and Drills R28 Cyber Security Incident Response Plan Testing Specifications 73.54 Nuclear testing of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently. Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R29 Cyber Security Incident Response Plan Review, Update and Communication Specifications 73.5450 App E Duration is inconsistent with nuclear regulation. Nuclear review and updating of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently.Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R30.1 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan CP-2 E8.1 Contingency Plan R30.2 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Recovery and Reconstitution CP-10 E8.6 Recovery and Reconstitution R30.3 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.4 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.5 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan Testing and Exercises CP-4 E8.2 Contingency Plan Test R31 Recovery Plan Testing Specifications 73.54 Duration is inconsistent with nuclear regulation. Nuclear tests and exercises for recovery for plant digital systems that support safety, security, EP or BOP functions

#	Organization	Question 54 Comment
		should not be regulated differently. R32 Recovery Plan Review, Update, and Communications Specifications Neither nuclear regulation nor NIST 800-53 contain expectations reviews, updates and communication of recovery plans at the frequencies established by R32. The bases for R32 requirements are unclear and consideration should be given to removing it.

END OF REPORT

Project 2008-06 Cyber Security Order 706

Consideration of Issues and Directives — DRAFT

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 25 We direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences is the divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost two hundred different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected.
		This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		features of the NIST Risk Management Framework were incorporated into version 5 NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable and therefore this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System Reliability. The NIST security control catalogue in 800-53 revision 3 was also used as a reference in addressing many of the FERC directives in Order 706.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 252 "Para 258. As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Para 252. Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commission's concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT approach would provide the industry with more certainty in implementing the CIP Reliability Standards."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Risk-based approaches to applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions.
Para 282 The Commission directs the ERO to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets.	FERC Order 706	The definition of BES Cyber Asset as used in CIP-002-5 requires Responsible Entities to consider misuse of the Cyber Assets in identifying BES Cyber Systems.
Para 285 The Commission directs the ERO to consider the comment from	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5 and added as a

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].		scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring and alerting, etc.).
Para 321 "Para 321. SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to “bright line” criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.
Para 376 “the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.”	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.
Para 386 The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities are required to revoke access to BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		production environment to aid in identifying any accidental consequences of the change.
Para 433 “we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.”	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, Requirement R2
Para 434 “The Commission adopts the CIP NOPR’s proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.”	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (item 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 “Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.”	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer based training (CBT). As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.
Para 446 "Para 446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by establishing criteria for personnel risk assessments.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."		
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (item 7.1) or by the end of the calendar day in cases of transfers or reassignments (item 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (item 7.2) from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (item 7.4) augments the requirements in items 7.1 and 7.2 that respond to the directive. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (item 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	FERC Order 706	CIP-004-5, Requirement R5 (item 5.1), requires a personnel risk assessment as a condition of being granted access, with exceptions only for specific CIP Exceptional Circumstances which are outlined in the proposed glossary definition of the aforementioned term.
Para 473 The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets.	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the Standards.
Para 476 We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions	FERC Order 706	Guidance in CIP-002-5 advises the owning Responsible Entities determine who is responsible for complying with the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
determinations above.		
Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter"	FERC Order 706	The proposed requirement requires a Responsible Entity to deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection). The drafting team addresses this in CIP-005-5, Requirement R1 (item 1.4). Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.
Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.
Paras 525, 526, 528, and 628 Para 525. "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 526. "the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments. The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs." Para 528. "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system. In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
or filtered logs." Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"		requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.
Paras 541, 542, and 547 Para 541. we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments." Para 542. "the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems." Para 547. "we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 544 "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification." "we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergoes an active vulnerability assessment. • An exception is made for specified CIP Exceptional

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
assessment”		Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (item 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment to ensure that required security controls are not adversely affected.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (item 1.3) for High Impact BES Cyber Assets
Para 581 “The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years.”	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (item 3.1) by changing the frequency to a 24 month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.
Paras 609, 610, and 611 Para 609. “We therefore direct the ERO to develop requirements addressing what constitutes a “representative system” and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.” Para 610. “we direct the ERO to revise the Reliability Standard to	FERC Order 706	CIP-010-1, Requirement R1 (item 1.4), provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. • The SDT proposes to require a “representative system” or test system for those High Impact Control Centers to use for the purposes of testing proposed

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above." Para 611. "the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."		changes and performing active vulnerability assessments. • The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system. • To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."
Paras 620 and 622 Para 620. "The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622. "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.		• The SDT rewrote the requirement as a competency based requirement that does not prescribe technology. • The SDT added Maintenance to cover malware on removable media. The drafting team also created a new requirement, CIP-007-5, Requirement R3 (item 3.4), to protect against personnel introducing malicious code when temporarily connecting to a BES Cyber Asset for Maintenance purposes. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (item 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks.
Paras 633 and 635	FERC Order 706	The SDT addresses these directives in CIP-011-1,

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633. "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it." Para 635. "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."		Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from media. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal.
Para 643 "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	In CIP-010-1, R3 (item 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment. In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 661 "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include as a minimum any Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."	FERC Order 706	In CIP-008-5, R3 (items 3.3 and 3.4), the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		NERC Reliability Standards.
Para 694 “For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard”	FERC Order 706	The SDT added in CIP-009-5, R1, a requirement to implement the recovery plan
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term “forensics” due to the legal interpretations associated with the term.
Para 710 and 706 "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (item 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (item 2.2), the SDT requires an initial and once every calendar year test of the data at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706 NERC Alert regarding remote access VPN vulnerabilities	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully. Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.
Para 13. "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	The SDT addressed this issue in CIP-007-5, R1, by having a requirement to disable or restrict use of physical I/O ports. The SDT changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan For Version 5 CIP Cyber Security Standards

November 7, 2011

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards[1]," are covered by this Implementation Plan:

CIP–002–5 —Cyber Security — BES Cyber System Identification
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 —Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management
CIP–011–1 — Cyber Security — Information Protection
"Definitions of Terms Used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards*.

These standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1 in addition to CIP-002-5 through CIP-009-5 because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

- Interchange Authority
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- Distribution Provider
- NERC
- Regional Entity

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows:

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were planned and implemented by the Responsible Entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5 Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must therefore be in Compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were not planned by the Responsible Entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5 Attachment 1. Then, later, an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified, changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, and that unchanged BES Cyber System may become a Medium Impact BES Cyber System based on the CIP-002-5 Attachment 1 criteria. The actions that cause the change in power flows would have been performed by a neighboring entity and would result in a change in impact level the of the affected BES Cyber System.

For *planned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1

For *unplanned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards according to the following timelines following the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1:

Scenario of Unplanned Changes	Compliance Implementation
New High Impact BES Cyber System	12 months
New Medium Impact BES Cyber System	12 months
Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System	12 months for new requirements
Newly categorized Medium Impact BES Cyber System	12 months
Responsible Entity Identifies first Medium or High Impact BES Cyber System	Add 12 months from time above

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability

and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1

November 7, 2011

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	DELETED	Critical Asset Identification – Removed this requirement because new Standard identifies and categorizes BES Cyber Systems directly without declaring assets as critical.
CIP-002-4 R2.	CIP-002-5 R1	Critical Cyber Asset Identification – New Standard identifies BES Cyber Systems as a grouping of Critical Cyber Assets because it allows entities to apply some requirements at a system rather than asset level. BES Cyber Systems are also identified using BES Reliability Operating Services, which provides more detail on what it means for a Cyber Asset to be critical to reliable operation.
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption or cyber assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g. training, response, recovery, etc.). Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R2.	DELETED	Control Center – No longer applicable since R2 has been deleted.
CIP-002-4 R2.	DELETED	Dial-up Accessible – No longer applicable since R2 has been deleted.
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes.
NEW	CIP-002-5 1.1	Update and re-categorize for changes to BES – Specifies timeframe for complying with all categorization and associated security requirements following a planned change.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R2	Cyber Security Policy – Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R2, 2.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order 706 paragraph 443.
CIP-003-4 R1.2.	CIP-003-5 R4	The cyber security policy is readily available – The Responsible Entity only needs to make individuals aware of elements of the cyber security policy related to their job function. This was in response to general confusion around the term "readily available". Examples of how to make individuals aware are listed in the Measures.
CIP-003-4 R1.3.	CIP-003-5 R3	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 R1	Single senior manager – Created a definition of CIP Senior Manager to prevent cross referencing across Standards.
CIP-003-4 R2.1.	CIP-003-5 R1	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within thirty calendar days of the change.

CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that the CIP Senior Manager can delegate the ability to delegate. For example, a senior manager can delegate the ability to further delegate responsibility for a plant control system to a plant manager.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.1.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. Removed language to “protect” information and replaced with “Implement handling and access control” to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – Replace this requirement with the defined term BES Cyber System Information.

CIP-003-4 R4.2.	CIP-011-1 1.1	Classification – Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-1 1.3	Assessment – No significant changes.
CIP-003-4 R5.	CIP-004-5 6.3, CIP-011-1 1.2	Authorize personnel for access to protected information – Clarified the "program for managing access" included the authorization of access as well as handling and access control procedures.
CIP-003-4 R5.1.	DELETED	Authorizing personnel – Personnel are still required to have authorization, and the CIP Senior Manager authorizes or delegates this responsibility. So the additional requirement to have and maintain a list is considered duplicative and unnecessary.
CIP-003-4 R5.1.1.	DELETED	Personnel shall be identified – 5.1 is deleted.
CIP-003-4 R5.1.2.	DELETED	Verification – 5.1 is deleted.
CIP-003-4 R5.2.	CIP-004-5 6.6	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.

CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate Standard because of the additional requirements necessary for satisfying FERC directives and the subject matter is currently spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material and moved example mechanisms to guidance..
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order 706-directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 2.2	Proper use of CCAs – Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 2.3,2.4	Physical and electronic access controls training – No significant changes.
CIP-004-4 R2.2.3.	CIP-004-5 2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media
CIP-004-4 R2.2.4.	CIP-004-5 2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order 706 paragraph 413.

CIP-004-4 R2.3.	CIP-004-5 3.2	Annual training – Replaced Annually with calendar year, not to exceed 15 months. .
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment –Split into two requirements, R4 to define the PRA program and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 4.1, 4.2	Identification and 7 year criminal check – Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment. Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 5.2	Perform the PRA every 7 years.– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 4.4	Addresses the contractor or vendor performed PRA.
CIP-004-4 R4.	CIP-004-5 6.1, 6.2	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 6.4	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 2.1	Added to help facilitate understanding what roles the entity has to support the role based training program.
NEW	CIP-004-5 2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should have be part of the core training per FERC Order 706 - paragraph 432.
NEW	CIP-004-5 2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order 706 - paragraph 434.
NEW	CIP-004-5 4.3	PRA failure criteria – There should be documented criteria or a process used to evaluate personnel risk assessments.

NEW	CIP-004-5 7.2	Transfers – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 7.3	Completion of revocation – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 7.4	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.4.	Applicability	Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring cyber assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have an ESP.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.

CIP-005-4a R2.1.	CIP-005-5 1.2	Deny access by default - Changes include referring to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP. The requirement explicitly states the network admission control includes both inbound and outbound connections.
CIP-005-4a R2.2.	CIP-007-5 1.1	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 1.3	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of “secure”, which is that the BES Cyber System should not be directly accessible with a phone number only
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. - Evidence requirements are considered as part of the measure.

CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.
CIP-005-4a R4.2.	CIP-010-1 3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.

CIP-005-4a R4.3.	CIP-010-1 3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.4.	CIP-010-1 3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.5.	CIP-010-1 3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order 706 para 643.
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 4.5	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4

NEW	CIP-005-5 1.6	Inspect & detect potential malicious communications – Per FERC Order 706, paragraph 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 2.1,2.2	Remote Access: intermediate device and encryption– This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for Senior Management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physically security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 1.2, 1.3	Physical Security Perimeter - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary.
CIP-006-4c R1.2.	DELETED	No longer requires identifing physical access points and controls at them to reflect the change from Physical Security Perimeter to Defined Physical Boundary
CIP-006-4c R1.3.	CIP-006-5 1.4	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in table row 1.4, which replaces the monitoring term. Otherwise, no significant change.
CIP-006-4c R1.4.	CIP-004-5 2.3	Appropriate use of access controls – The term “appropriate’ is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

CIP-006-4c R1.6.1.	CIP-006-5 2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the applicability section of each security requirement and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement. For this particular requirement see CIP-006-5 item 1.1
CIP-006-4c R2.2.	Applicability	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement.
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the applicability section of each security requirement.

CIP-006-4c R4.	CIP-006-5 1.2, 1.3	Physical Access Controls - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary. Also addressed FERC Order 706 defense in depth. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R5.	CIP-006-5 1.4, 1.5, 1.6	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 1.7	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the Defined Physical Boundary. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R7.	CIP-008-5 Evidence Retention	Retain relevant incident related log information is addressed in CIP-008-5
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing
CIP-006-4c R8.1.	CIP-006-5 3.1	Physical access control system 3 yr. testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order 706 paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of item 3.1.
CIP-006-4c R8.3.	CIP-006-5 3.2	Retain outage records – No significant changes.
NEW	CIP-006-5 1.1	Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 1.4	Assess security controls following changes - Provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order ,paragraphs 397, 609, 610, and 611
CIP-007-4 R1.1.	CIP-010-1 1.4	Test procedures – See description and justification for CIP-007-4 R1.
CIP-007-4 R1.2.	CIP-010-1 1.4	Testing reflects production environment - See description and justification for CIP-007-4 R1.
CIP-007-4 R1.3.	CIP-010-1 1.4	The Responsible Entity shall document test results. - See description and justification for CIP-007-4 R1.
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.1.	CIP-007-5 1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording or CIP-007-4 R3, R3.1, and R3.2 was separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.
CIP-007-4 R3.1.	CIP-007-5 2.2	Assess patches – Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.
CIP-007-4 R3.2.	CIP-007-5 2.3	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3, 3.4, 3.5	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…" In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.
CIP-007-4 R4.1.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malware prevention tools – See description and justification for CIP-007-4 R4.
CIP-007-4 R4.2.	CIP-007-5 3.4	Update malicious code detections – See description and justification for CIP-007-4 R4.

CIP-007-4 R5.	CIP-007-5 5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.
CIP-007-4 R5.1.	CIP-004-5 6.1	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5	Access authorization – CIP-003-5 R5 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.
CIP-007-4 R5.1.2.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R5.1.3.	CIP-004-5 6.5	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.
CIP-007-4 R5.2.1.	CIP-007-5 5.4	Change default vendor passwords – The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 5.2	Identify account types and determine acceptable use
CIP-007-4 R5.2.3.	CIP-007-5 5.3	Identify account types and determine acceptable use – No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

CIP-007-4 R5.3.	CIP-007-5 5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters . The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 5.5	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.
CIP-007-4 R6.1.	CIP-007-5 4.1	Identify security events – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R6.2.	CIP-007-5 4.2	Identify security events for real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 4.4	Retain relevant log information – No significant changes.
CIP-007-4 R6.5.	CIP-007-5 4.3	Review logs – Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 2.1	Erase media no longer needed to store protected information – Consistent with FERC Order 706, paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Removed requirement explicitly requiring records of destruction/redeployment because this was implied as a measure of compliance.
CIP-007-4 R7.1.	CIP-011-1 2.2	Disposal – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.2.	CIP-011-1 2.1	Redeployment – See description and justification for CIP-007-4 R7.

CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 3.1, 3.2	Ports and services review – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.3.	CIP-010-1 3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.4.	CIP-010-1 3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 1.2	Restrict physical I/O ports – In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NEW	CIP-007-5 2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 4.3	Generate real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 5.6	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

NEW	CIP-007-5 R6	Limit malicious code on maintenance devices – This is a new requirement to address the FERC Order 706 paragraph 621 directive to protect against personnel introducing malicious code into the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protective (Protected??) Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code or creating an additional electronic access point.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4 where individual aspects of maintaining the plan are listed as separate requirements. The requirement to have an Incident Response Plan now applies to all Responsible Entities as a foundational element of a cyber security program for BES Cyber Systems.
CIP-008-4 R1.1.	CIP-008-5 1.1	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5.
CIP-008-4 R1.2.	CIP-008-5 1.2	Roles and responsibilities of incident response teams – No significant changes.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinating with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single Standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 3.3	Update incident response plan following review – Included additional specification on update of response plan Addresses FERC Order 706 Paragraph 686 directive to modify on lessons learned and aspects of the DHS Controls.
CIP-008-4 R1.5.	CIP-008-5 3.1	Review incident response plans annually – No significant changes.
CIP-008-4 R1.6.	CIP-008-5 2.1	Test incident response plans annually – No significant changes.
CIP-008-4 R2.	DELETED	Cyber Security Incident Documentation – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.

NEW	CIP-008-5 3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 3.1	Recovery Plan – Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.
CIP-009-4 R1.1.	CIP-009-5 1.1	Conditions for activation of recovery plan – Reworded to address FERC Order 706 paragraph 694 directive and simplified the requirement.
CIP-009-4 R1.2.	CIP-009-5 1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 3.2	Review results of recovery plan activities (tests, events) – Added the timeframe for update.
CIP-009-4 R4.	CIP-009-5 1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 2.2	Test information used for recovery – Combined Requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order 706 directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 1.4	Testing of backup media – Addresses FERC Order 706 paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 1.6	Process to preserve data for analysis – Added requirement to address FERC Order 706, paragraph 706 regarding the necessity to have procedures in place to retain cyber asset evidence as part of the recovery planning.

NEW	CIP-009-5 3.5	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.

Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.
NEW	CIP-010-1 2.1	Monitor for changes to the baseline configuration – Monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This change addresses FERC Order 706, paragraph 397 directive and is based on a review of DHS Catalog of Security Controls (or NIST 800-53).
NEW	CIP-010-1 3.2	Live Vulnerability Assessment – Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a live vulnerability assessment in a test environment.
NEW	CIP-010-1 3.3	Perform active VA on new BES Cyber Assets - Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

From: Wendy Kinnard
To: Wendy Kinnard
Subject: NERC Industry Webinar: Project 2008-06 Cyber Security Order 706 - December 13, 2011
Date: Monday, November 28, 2011 12:46:47 PM

Industry Webinar

Project 2008-06 Cyber Security Order 706
Version 5 CIP Standards Balloting Update

December 13, 2011 | 1:00–2:00 p.m. ET

Click here for: Registration
Click here for: Agenda
Teleconference: 800.698.5954 | **Access Code:** 8816510 | **Broadcast Audio Code:** 545534

Objective: This webinar will give attendees the opportunity to hear about the comment and balloting process for Version 5 of the posted drafts of Critical Infrastructure Protection (CIP) Standards on cyber security (CIP-002 through CIP-011). Specifically, this webinar will explain the ballot process and the use of the consolidated electronic comment form, address questions relating to the common ballot pool for the twelve initial ballots, and provide illustrative examples to assist industry stakeholders in submitting comments and ballots. The CSO706 Drafting Team organized a number of industry outreach meetings and webinars over the past several months to explain the new requirements in Version 5 of the Draft CIP standards on cyber security and to obtain feedback from industry participants, and the scheduling of this webinar coincides with the drafting team's posting of the Version 5 Draft CIP standards for industry formal comment and ballot.

Background: The Drafting Team for Project 2008-06 CSO706 has continued its work to address all of the FERC directives in Order 706 (http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf), since the filing of Version 4 of the CIP Cyber Security Standards in February 2011. The Version 5 CIP Cyber Security Standards were posted for industry comment and ballot in early November 2011, with a concurrent ballot at the end of the comment period. Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8:00 p.m. ET on Friday, January 6, 2011. Comments submitted during the formal comment period and the ballot for the standard both use

the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the consolidated electronic comment form.

For more information or assistance, please contact Steven Noess (via email) or at (404) 446-9691 or Wendy Kinnard (via email) or at (404) 446-9735.

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

Wendy (Sandberg) Kinnard
Standards Development Administrative Assistant
North American Electric Reliability Corporation
wendy.kinnard@nerc.net
(404) 446-9735 (O)
(404) 823-1366 (C)

NERC Reliability | Accountability

This email and any of its attachments may contain NERC proprietary information that is privileged, confidential, or subject to copyright belonging to NERC. This message and any attachments may contain confidential information protected by the attorney-client or other privilege. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout

---
You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1276991-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Version 5 Requirements & Status

Philip Huff – Arkansas Electric Cooperative Corporation
Doug Johnson – Commonwealth Edison Company
David Revill – Georgia Transmission Corporation

CSO706 SDT Webinar
August 24, 2011

to ensure the reliability of the bulk power system

Agenda

- Background
- Version 4 - Overview
- Version 5 – Requirements Summary
- Schedule and Implementation Plan

Project Background

Version 1

- Filed with FERC August 28, 2006
- Approved by FERC January 18, 2008
- Effective July 1, 2008 through January 1, 2010 (phased)

Version 2

- Low-hanging fruit
- Filed with FERC May 22, 2009
- Approved by FERC September 30, 2009
- Effective April 1, 2010

Version 3

- Compliance filing to Version 2
- Filed with FERC December 29, 2009
- Approved by FERC March 31, 2010
- Effective October 1, 2010

CIP-002-4 Overview

- **Version 4** of the CIP Standards
- Approved by Industry **December 30, 2010**
- Submitted to FERC **February 10, 2011**
  - 2,232 page filing
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

Looking Ahead to Version 5

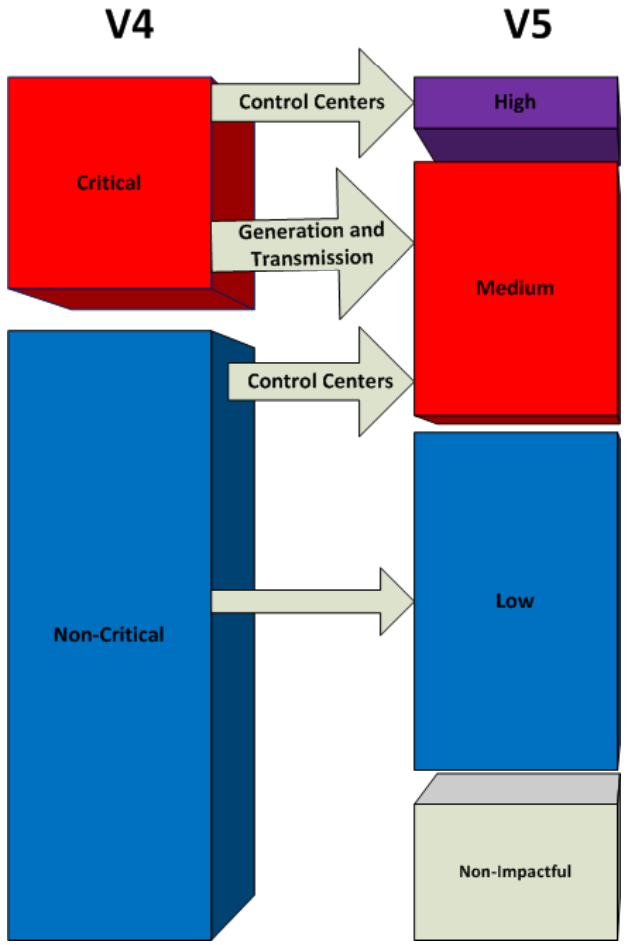
- The SDT continues work to address the remaining 50+ issues in Order 706
  - Version 5 builds on CIP-002-4 and previous drafts of CIP-010 & 011
  - Use similar content structure and terminology as previous CIP Standards (CIP-002 through CIP-009)

Development Goals

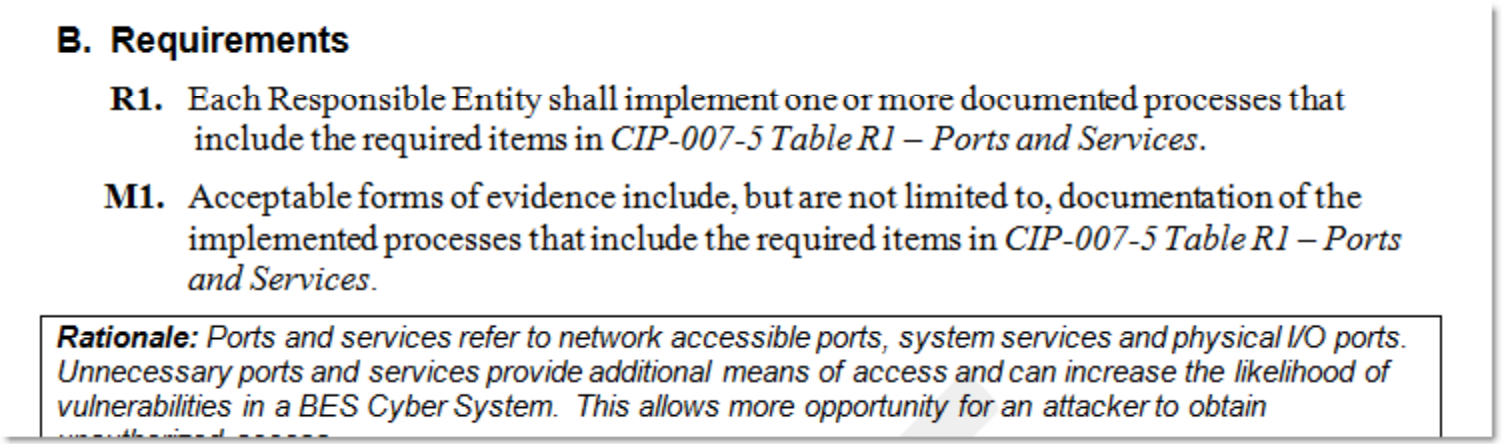
Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements	**Goal 5**: To minimize technical feasibility exceptions
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES	**Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance"
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements	

Levels of Impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Format (1/4) – Introductory Requirement



B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress

Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NERC*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafti
address unused physical ports.

Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which

Format (3/4) – Requirement Row

	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	**Requirement**	**Measurement**
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of compliance associated with the requirement row

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5 – CIP-011-5

to ensure the reliability of the bulk power system

CIP-002-5 Summary of Modifications

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update required lists for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

CIP-002-5 Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
  - Review of Transmission voltage threshold by SDT for V5
  - Use of MVA bright-line under consideration

CIP-003-5 Summary of Modifications (1/2)

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

CIP-003-5 Summary of Modifications (2/2)

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing

CIP-003-5 Addressing FERC Directives

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

CIP-004-5 Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

CIP-004-5 Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

CIP-004-5 Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

CIP-004-5 Addressing FERC Directives (Training)

FERC Order 706 Para. 433	""we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."
FERC Order 706 Para. 434	"The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
FERC Order 706 Para. 435	"Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."

- The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- The SDT added this as a topic for role specific training.
- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-004-5 Addressing FERC Directives (Immediate Revocation)

FERC Order 706 Para. 460

"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-005-5 Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

CIP-005-5 Addressing FERC Directives (2 Security Measures – Defense in Depth)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 496

"Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter."

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

CIP-006-5 Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24-month cycle with ongoing discussions of different cycles based on environment

CIP-006-5 Addressing FERC Directives

FERC Order 706 Para. 572

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."

- The SDT added this for High Impact BES Cyber Assets

FERC Order 706 Para. 581

"The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."

- The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

CIP-007-5 Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

CIP-007-5 Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

CIP-007-5 Addressing FERC Directives (Log Review)

FERC Order 706 Para. 525	"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"
FERC Order 706 Para. 628	"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

CIP-007-5 Addressing FERC Directives (Malware)

FERC Order 706 Para. 620

"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"

FERC Order 706 Para. 622

"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

CIP-007-5 Addressing FERC Directives (Ports & Services)

March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

CIP-008-5 Summary of Modifications

- Defined Reportable Cyber Security Incident
- Working to harmonize with EOP-004-2
- Includes additional specification on update and lessons learned associated with the response plan

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

A1

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.
  or
- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Slide 33

A1 Rework text format to be consistent with other slide formats (bullets and fonts).Applied to tother slides in CIP-008 and CIP-009 as well.

Author, 8/19/2011

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 673

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 676

"the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

CIP-009-5 Summary of Modifications

- Added requirement to implement the response plan
- Verification of backup media information prior to storage
- Preservation of data for analysis

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 706

"Preserve data for analysis"

CIP-009-5 1.6
Requires process to preserve data for analysis

CIP-010-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

CIP-010-5 Requirements Summary

- The SDT has made changes the Vulnerability Assessment requirements to:
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 609	"We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."
FERC Order 706 Para. 610	"we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
FERC Order 706 Para. 611	"the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

- The SDT proposes to require a "representative system" or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 541	"we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."
FERC Order 706. Para 542	"the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."
FERC Order 706 Para. 547	"we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"

- The SDT has added requirements for an "active vulnerability" assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 544	"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."
FERC Order 706 Para. 544	"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

CIP-011-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access

CIP-011-5 Requirements Summary

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected
  - Previously, this list was a requirement itself

CIP-011-5 Summary

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed
  - In version 5, the requirement is triggered when either:
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

CIP-011-5 Addressing FERC Directives

FERC Order 706 Para. 633	"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
FERC Order 706 Para 635	"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

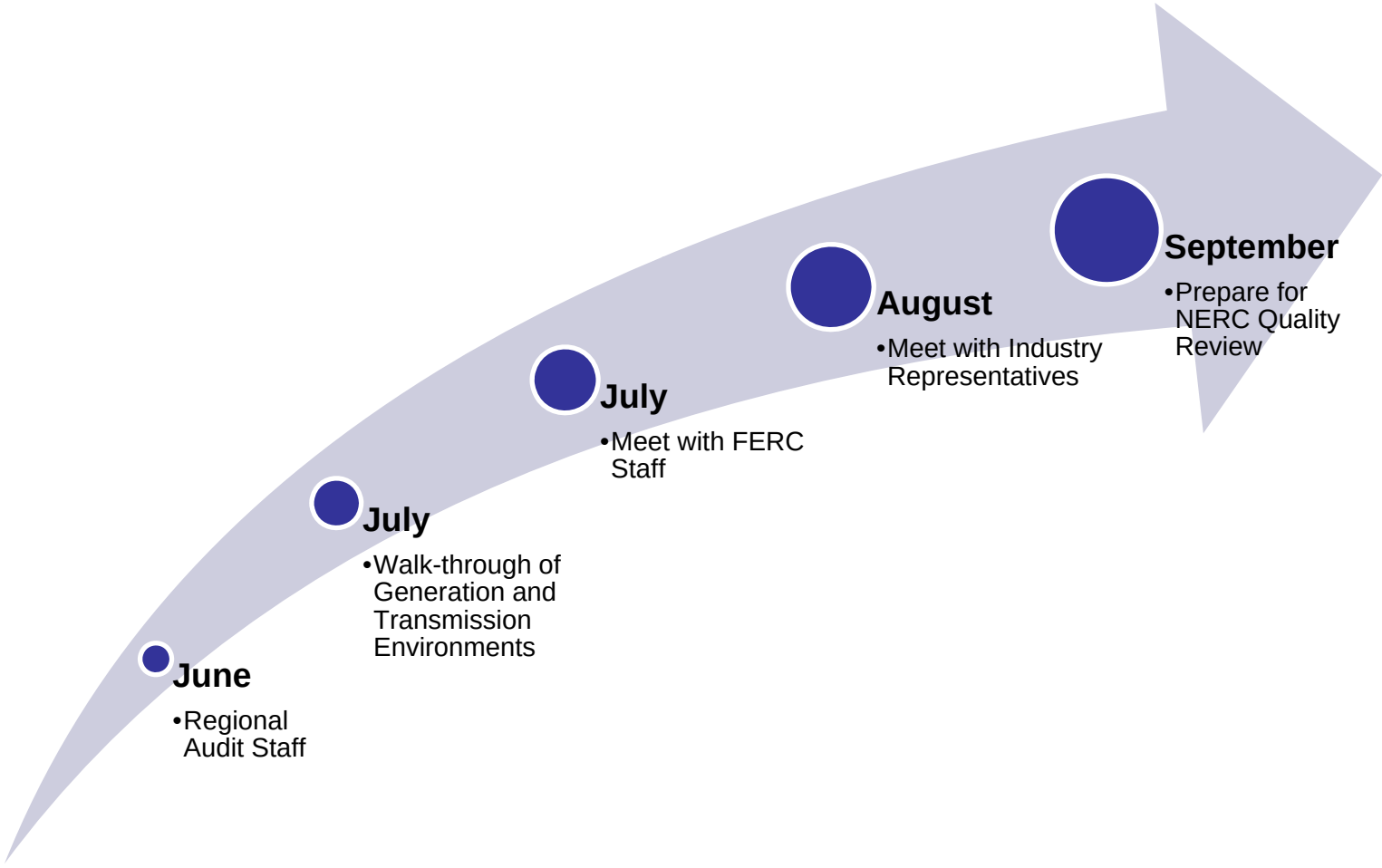
Implementation Plan

- Implementation plan is in the very early phases of development
- Current concepts include staggered Effective Dates for:
  - CIP-002-5
  - Organizational Requirements (CIP-003-5, CIP-008-5)
  - Technical Requirements (CIP-005-5, CIP-006-5, etc.)
- Technical Requirements would be further staggered by:
  - High Impact BES Cyber Systems
  - Medium Impact BES Cyber Systems
  - Low Impact Cyber Systems

Implementation Plan

- Currently evaluating a single implementation plan that would include compliance timelines for future newly identified BES Cyber Systems and those BES Cyber Systems that change categories
  - Eliminates the separate Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (IPFNICCANRE)

Schedule to Date – 2011



Key Dates Moving Forward

- **November 3rd, 2011 –**
  First Posting for Comment and Ballot
  - Webinars – November 15th and 29th, 2011
  - Ballot Opens – December 9th, 2011
  - Ballot Closing – December 19th, 2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

Points of Contact:
Philip Huff – philip.huff@aecc.com
Doug Johnson – douglas.johnson@comed.com
David Revill – david.revill@gatrans.com

Slides and Recording of Webinar will be Posted (on NERC Website)

to ensure the reliability of the bulk power system

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Ballot Pool Now Open: November 7 – December 15, 2011
Formal Comment Period Now Open: November 7, 2011 – January 6, 2012
Twelve Initial Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 60-day comment period through Friday, January 6, 2012.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single

standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the non-binding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The non-binding polls will take place in parallel with the next ballot of these standards.

Instructions for Joining Ballot Pool for Version 5 CIP Standards

A single ballot pool is being formed for the balloting of all ten standards, the implementation plan, and the definitions associated with the ten standards. The ballot pool that is formed will be cloned to create twelve separate ballot pools (one for each of the ten standards, one for the implementation plan, and one for the definitions). All members of the original ballot pool will automatically be eligible to vote in the twelve individual ballots.

The standards, implementation plan, and set of definitions are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

To join the ballot pool to be eligible to vote in the upcoming ballots, as well as future ballots and non-binding polls for the Version 5 CIP standards, go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their “ballot pool list server.” (Once the balloting begins, ballot pool members are prohibited

from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the standards being balloted for this project. The list server is: bp-2008-06_CIP-002-5_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments

Please note that comments submitted during the formal comment period and the ballot for the standard both use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

Next Steps

The drafting team will host a series of three webinars – two on the substance of the standards, and a third to address process questions. The webinars on the substance of the standards, which have already been announced, will be held on November 15, 2011, and November 29, 2011. A separate announcement for the webinar that will address process questions will be sent with registration information as soon as details have been finalized.

Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8 p.m. Eastern on Friday, January 6, 2011.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards Balloting Update

December 13, 2011 | 1:00–2:00 p.m. ET

Industry Webinar*

Dial-in: 800.698.5954 | Access Code: 8816510 | Broadcast Audio Code: 545534

1:00 p.m.	**Welcome and Opening Remarks**
1:05 p.m.	**Version 5 CIP Cyber Security Standards Ballot Process**
1:15 p.m.	**Version 5 Standards Consolidated Electronic Comment Form**
1:20 p.m.	**Balloting and Comment Illustrative Examples**
1:30 p.m.	**Questions and Answers**
2:00 p.m.	**Adjourn**

* Invited speakers include: Laura Hussey, NERC Standards Process Manager; Steven Noess, NERC Standards Development Advisor

Appendix 4B

Proposed Revisions 11-7-2011

Sanction Guidelines of the North American Electric Reliability Corporation

Effective: ~~January 1, 2011~~ _____, 2012

Table of Contents

1. Preamble and Overview 1

2. Document Scope and Exclusions 3

3. Basic Principles 4

3.1 Necessary Element of NERC Compliance Program 4
3.2 Settlement of Compliance Violations 4
3.3 Settlement Request 5
3.4 Settlement Effect on Continuation of Determination of Penalties, Sanctions, or Remedial Actions 5
3.5 Timing of Determination of Penalty, Sanction or Remedial Action 5
3.6 Determining Party 5
3.7 No Influence of Penalty, Sanction or Remedial Action upon Violation Confirmation Process 5
3.8 Reasonable Relationship to Violation 5
3.9 Use and Facets of Factors to Determine Penalties 6
3.10 Multiple Violations 6
3.11 Relation of the Penalty to the Seriousness of the Violation and Violator's Ability to Pay 7
3.12 Violation Time Horizon 8
3.13 Extenuating Circumstances 8
3.14 Concealment or Intentional Violation 8
3.15 Economic Choice to Violate 8
3.16 No Influence by Outcome of Economic Choice to Violate 9
3.17 Non-Monetary Sanctions or Remedial Actions 9
3.18 Non-Exclusiveness of Monetary Penalties or Non-Monetary Sanctions 9
3.19 Monetization of the Value of Sanctions 9
3.20 Maximum Limitations on Penalties 10
3.21 Frequency and Duration of Violations 9

4. Determination of Monetary Penalties 13

4.1 Initial Value Range of the Base Penalty Amount 13
4.1.1 Violation Risk Factor 13
4.1.2 Violation Severity Level 14
4.2 Setting of the Base Penalty Amount 14
4.2.1 Applicability of the Violation Risk Factor 14
4.2.2 First Violation 14
4.3 Application of Adjustment Factors 15
4.3.1 Repetitive Violations and Compliance History 15
4.3.2 Failure to Comply with Compliance Directives 16
4.3.3 Self-Disclosure and Voluntary Corrective Action 16
4.3.4 Degree and Quality of Cooperation in Violation Investigation and Remedial Action 17
4.3.5 Presence and Quality of Compliance Program 17
4.3.6 Violation Concealment 17
4.3.7 Intentional Violation 17
4.3.8 Extenuating Circumstances 18
4.4 Setting of the Final Penalty Amount 18
4.4.1 Violator's Financial Ability to Pay 18
4.4.2 Reconfirmation of Disgorgement of Unjust Profit or Gain 18

5. Determination of Non-Monetary Sanctions 20

6. Remedial Action 21

6.1 Definition and Anticipated Use 21
6.2 Compliance Requirements 21
6.3 No Obligation to Issue 21
6.4 Scope of Application 21

6.5 Availability 22
6.6 No Impact on Confirmation of Violation, or Penalties or Sanctions 22
6.7 Types of Remedial Actions 22

Appendix A: Base Penalty Amount Table 23

1. ~~Preamble and~~ Overview

The North American Electric Reliability Corporation ("NERC"), as the electric reliability organization ("ERO"), and regional entities to whom NERC has delegated authority (hereinafter referred to collectively as "regional entities" or individually as a "regional entity"[1]) shall determine and may levy monetary penalties and non-monetary sanctions and remedial action directives against owners, operators, and users of the bulk power system for violations of the requirements of NERC Reliability Standards ("reliability standards") approved by the Federal Energy Regulatory Commission ("FERC") and applicable authorities in Canada and/or Mexico. This document sets out the processes and principles to be followed, and factors that will be considered when determining penalties, sanctions, or remedial action directives for violations. Collectively these processes, principles and factors are NERC's penalties, sanctions, and remedial action directive guidelines.

NERC and the regional entities will ~~exclusively~~ follow the directives, principles and processes in these Sanction Guidelines when determining penalties, sanctions, or remedial action directives for a violation. ~~However,~~ The adjustment factors in these Sanction Guidelines~~are also~~ provide~~d to afford~~ NERC ~~or~~and the regional entities~~entity~~ the flexibility needed to ~~accommodate~~take into account the facts surrounding each violation. ~~In this manner, rigid prescription of specific penalty formulae can be avoided at the same time that appropriate limitations on the degree of discretion and flexibility available to address each violation on its merits is maintained.~~ The outcome will be ~~remedies~~penalties and sanctions that are commensurate ~~and fair compared~~ to the reliability impact of the violation and to ~~remedies~~those levied for similar violations, yet appropriately reflective of any unique facts and circumstances regarding the specific violation and violator.

~~The adjustment factors established in this document are generally consistent with those listed in the FERC Policy Statement on Enforcement issued on October 20, 2005. However, discussion of the factors presented in this document is not exhaustive as other facets of these factors, or other additional factors not discussed herein, may also be considered to determine a given penalty, sanction, or remedial action, as NERC or the regional entity deems appropriate under the circumstances.~~

Regional entities shall follow these Sanction ~~g~~Guidelines when ~~to~~ determin~~ing~~e penalties, sanctions, or remedial action directives. NERC shall oversee the regional entities' application of the Sanction ~~g~~Guidelines to ensure that regional entities achieve acceptable levels of consistency ~~are achieved~~. NERC's oversight will ~~also~~ ensure ~~comparable outcomes; i.e.~~ that there is acceptable similarity in the degree and type of sanction for violations constituting comparable levels of threat to reliability of the bulk power system. ~~In order to facilitate this oversight, regional entities' reporting to NERC of penalties and sanctions they have determined will be thorough and in sufficient detail that NERC can understand and reasonably replicate the outcomes reached;~~ NERC may develop reporting requirements or a standard reporting form for use by the regional entities for this purpose, as NERC deems necessary or appropriate.

As experience is gained by NERC and the regional entities through the use and application of these Sanction ~~g~~Guidelines, NERC will review the Sanction ~~g~~Guidelines and may modify them as NERC deems appropriate or necessary. Authority delegated by NERC to the regional entities with respect to penalties, sanctions, or remedial action directives does not include the authority to modify these Sanction ~~g~~Guidelines.

NERC and the regional entities will apply the provisions of this document in accordance with applicable statutory provisions and with the regulations, orders, and statements of policy of FERC and other ERO governmental authorities that are applicable to the determination and imposition of penalties and sanctions for violations of reliability standards in the respective jurisdictions.

[1] For purposes of this footnote, the term "regional entity" shall be read as either as single or plural, as necessary, to refer to the applicable regional entity or regional entities.

Any revision to this document ~~or to the principles and factors identified or addressed within it~~ must first be approved by the NERC board, then by FERC, appropriate authorities in Canada or appropriate authorities in Mexico prior to becoming effective and applicable within the United States or these authorities' respective jurisdictions.

2.Document Scope and Exclusions

This document identifies and discusses the processes and principles to be followed, and factors that will be considered to determine penalties, sanctions, or remedial actions for violations of the reliability standards.

This document notes but does not otherwise address the progression of actions and steps that NERC or the regional entity will follow to process a violation from its initial incoming status upon discovery as a possible violation, through to its possible final determination as a confirmed violation. This is set out in the NERC Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure.

This document notes but does not otherwise address how a possible violation or alleged violation is reviewed in order to confirm or dismiss it. NERC's process and requirements for this review are set out in the NERC Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure. Regional entities will undertake such reviews using the processes and requirements set out in the NERC Compliance Monitoring and Enforcement Program.

This document notes but does not otherwise address the processes and procedural steps by which a confirmed violation can be appealed, or by which a penalty, sanction, or remedial action determined and levied for a violation can be appealed. These procedures are set out in the NERC Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure, and applicable regional entity program documents.

The NERC Compliance Monitoring and Enforcement Program provides for the possibility of settlements within NERC or regional entity compliance enforcement programs. This document makes reference to settlements to but does not address them further.

3.2. Basic Principles

The following paragraphs identify and discuss the basic principles underpinning why and how NERC and the regional entities will determine penalties, sanctions, and remedial action directives for violations of the requirements of the reliability standards.

The principles are unique and complimentary; the order in which theythe principles are presented in this document does not set or indicate order of precedence.

3.1Necessary Element of NERC Compliance Program

Primary objectives of NERC as the ERO include the promotion and enforcement of compliance with the reliability standards by owners, operators, and users of the bulk power system; standards made mandatory by duly-authorized legislative bodies in the U.S and Canada, and designed to maintain and promote the reliability of the two countries' shared power grids. Consistent with these objectives, NERC and the regional entities will monitor and act to verify compliance with standards' requirements; however, beyond monitoring and acting only to verify compliance, NERC and the regional entities will also hold bulk power system owners, operators, and users — or their delegates — accountable for confirmed compliance violations. This accountability will include determination and the possible levying of penalties, sanctions, or remedial actions.

Penalties, sanctions, and remedial actions are valid and necessary mechanisms to NERC and the regional entities for the enforcement and promotion of compliance to the reliability standards, in part because they can:

a.promote compliance behavior;

b.provide deterrence to future incidents, actions or situations of noncompliance by the violator or others;

c.implement actions that will promptly correct behavior;

d.disgorge benefits that may or may have accrued to a violator as a consequence of violating;

e.visit upon a violator some portion of any damage their violation may or may have visited upon others.

Accordingly, the determination and potential levying of appropriate penalties, sanctions, or remedial actions by NERC or the regional entity upon those responsible for violations shall be a required step within the NERC and regional entity compliance enforcement programs.

3.2Settlement of Compliance Violations

NERC and the regional entities shall maintain the reliability of the bulk power system by enforcing compliance with NERC and regional entity reliability standards. NERC and regional entity compliance enforcements programs will lay out how NERC and the regional entities will do this. In particular and by necessity, elements of these programs regarding the confirmation of violations, the determination and levying of penalties, sanctions, or remedial actions, and appeals are rigid and legalistic in form and nature in order to respect the basic tenets of due process and natural justice inherent within United States and Canadian justice systems, respectively, upon which they are being based. However, absolute adherence to the compliance programs, to the exclusion of other options, may not be the most appropriate, efficient or desirable means by which to achieve the end goal in all circumstances, to all entities party to a violation.

2.1 Settlement of Compliance Violations

Pursuant toAs set out in the NERC Compliance Monitoring and Enforcement Program, Appendix 4C to the NERC Rules of Procedure, possible or alleged violations of the reliability standards may be resolved dealt with through settlements reached between NERC, a regional entity and the registered entity or entities to whom a possible, or alleged, or confirmed violation is attributed to by NERC or

the regional entity. Any provisions ~~made~~ within a settlement regarding penalties~~,~~ or sanctions~~, or remedial actions~~ can supersede any corresponding penalties or~~,~~ sanctions that would otherwise be determined pursuant to these guidelines.

~~3.1Settlement Request~~

~~Any entity found in or being investigated for a violation may request settlement negotiations at any time, including prior to issuance of a notice of alleged violation; however, NERC or the regional entity may decline to enter into or continue settlement negotiations after the possible violation or alleged violation becomes a confirmed violation.~~

~~3.2Settlement Effect on Continuation of Determination of Penalties, Sanctions, or Remedial Actions~~

~~Until a settlement is finalized or parties to that settlement agree otherwise, NERC or the regional entity may continue activities and actions towards the determination and levying of a penalty, sanction, or remedial action that would otherwise be applicable pursuant to these guidelines, or that will be applicable if the settlement is not finalized.~~

~~3.5Timing of Determination of Penalty, Sanction or Remedial Action~~

~~All possible violations and alleged violations will be reviewed by NERC or the regional entity with the outcome that either the violation will be confirmed or the violation will be dismissed.~~

2.2 Timing of Determination of Penalty, Sanction or Remedial Action Directive

The penalty~~,~~ or sanction~~, or other remedial action~~ for a violation will be determined during the enforcement process in accordance with Section 5.0 of Appendix 4C ~~when the violation becomes a confirmed violation or is resolved as part of a settlement agreement~~.

At any time during the enforcement process, including any ~~confirmation review,~~ hearings~~,~~ or appeals, NERC or the regional entity may determine that a remedial action directive to the registered entity is warranted and, in accordance with Section 7.0 of Appendix 4C,~~by the subject entity of the review, hearing, or appeals. NERC or the regional entity~~ may direct that the registered entity implement the~~such~~ remedial action~~s~~ directive ~~be undertaken by the subject entity at any time, including prior to confirmation of a violation, and without regulatory approval~~.

~~3.6Determining Party~~

~~The determination of penalty, sanction or other remedial action for a violation will generally be undertaken by the same entity determining the violation to be a confirmed violation, but subject to review by NERC if the determination is made by a regional entity.~~

~~3.7No Influence of Penalty, Sanction or Remedial Action upon Violation Confirmation Process~~

~~The penalty, sanction, or remedial action determined for a violation will not influence the outcome of the regional entity' or NERC's confirmation review of the violation. In particular, if the determination of penalty, sanction, or remedial action for a probable violation is being undertaken by the same entity undertaking the confirmation review, the entity will insure that there is sufficient separation, in such terms as time, process, personnel or the like, to preclude that the penalty, sanction, or remedial action determined influences the outcome of the confirmation review.~~

~~3.8~~2.3 Reasonable Relationship to Violation

Penalties and~~,~~ sanctions~~, and remedial actions~~ levied ~~or applied~~ for the violation of a reliability standard shall bear a reasonable relation to the seriousness of the violation while also reflecting consideration of the other factors specified in~~that~~ these Sanction gGuidelines ~~direct to take into account. In the United States, the legislation establishing mandatory enforceable reliability standards and the ERO requires that "Any penalty imposed … shall; (A) bear a reasonable relation to the~~

~~seriousness of the violation; and (B) take into consideration the efforts of the user, owner, or operator to remedy the violation in a timely manner~~[2].

~~3.9~~2.4 Use ~~and Facets~~ of Factors to Determine Penalties

Penalties levied for a ~~given~~reliability standard violation will be based on all facts and ~~other~~ information relevant to the violation~~incident or situation~~. To that end, these Sanction ~~g~~Guidelines include factors ~~which~~that NERC and the regional entities will consider while determining the penalty or sanction for a violation~~to be levied~~.

~~NERC considers, and these guidelines direct, that t~~The presence of some factors in connection with~~within~~ a violation aggravates the seriousness of that violation and should ~~cause an~~ increase ~~or expansion of~~ the penalty ~~to be levied~~. Conversely, the presence of certain~~some~~ other factors mitigates the~~that~~ seriousness of the violation and should ~~cause a decrease or reduction of~~reduce the penalty ~~to be levied~~. ~~Also, some factors may mitigate or aggravate, and should have commensurate impact. NERC considers, and these guidelines direct, that t~~The absence of an aggravating or mitigating factor will have no impact~~, as opposed to a mitigating or aggravating impact, respectively, to~~ on the~~a~~ penalty.

This document identifies many aggravating and mitigating ~~presents many of the relevant facets of the~~ factors that, if present in connection with a violation, should be considered in determining the penalty or sanction, and describes how these factors should be taken into account ~~included in these guidelines~~. ~~However, additional facets of these factors, or a~~Additional factors not identified in this document~~discussed herein,~~ may also be considered ~~into~~ determining~~e~~ a ~~given~~ penalty~~,~~ or sanction, ~~or remedial action,~~ as NERC or the regional entity deems appropriate under the circumstances. Where additional factors ~~or facets~~ are considered~~used~~ they will be identified, and their use will be justified, in the notice of penalty, and the~~. The~~ effect of using these factors ~~or facets~~ on the penalty~~,~~ or sanction~~, or remedial action~~ determined will ~~also~~ be fully and clearly disclosed.

~~3.10~~2.5 Multiple Violations

A violation is a failure ~~or inadequacy~~ to meet a requirement of a reliability standard by a bulk power system owner, operator or user ~~party~~ responsible to comply with that requirement.

The ~~failure or inadequacy of a violator to~~entity's noncompliance ~~comply~~ may involve more than one standard or several requirements of a single standard~~.; as~~ As such, multiple individual violations may exist~~be in play~~ when NERC or the regional entity determines penalties or~~,~~ sanctions~~, or remedial actions~~ for a~~n incident or situation of~~ noncompliance ~~are being determined~~.

~~Strictly speaking,~~ NERC or the regional entity may~~can~~ determine and levy a separate penalty or sanction~~, or direct remedial action,~~ upon a violator for each individual violation of a reliability standard requirement. However, where~~in instances of~~ multiple violations relate~~d~~ to a single act or common incidence of noncompliance, or where the penalties or sanctions for several unrelated violations by the entity are being determined at the same time, NERC or the regional entity or entities may~~will generally~~ determine and issue a single aggregate penalty~~,~~ or sanction~~, or remedial action directive~~ bearing reasonable relationship to the aggregate of the ~~related~~ violations. In such a case, ~~T~~the penalty~~,~~ or sanction~~, or remedial action will not be that determined individually for the least serious of the violations; it~~ will generally be at least as large or expansive as what would be called for individually for the most serious of the violations.

Some entities may ~~be~~ register~~ed as being responsible~~ for more than one reliability function in the NERC Compliance Registry (e.g., transmission owner, transmission operator, balancing authority, generation operator), and as a result, a single requirement in ~~some~~certain reliability standards may apply to the ~~responsible~~ entity for several of its registered functions. Where an entity performs several registered functions ~~are performed by the same entity~~, NERC or the regional entity will assess a

[2] ~~H.R.6, Energy Policy Act of 2005, Section 215, Paragraph c, subparagraph 6.~~

violation and associated penalty or sanction ~~will be assessed~~ against the entity, not against each function.

~~3.11~~2.6 Relation of the Penalty to the Seriousness of the Violation and Violator's Ability to Pay

As stated~~discussed~~ in Section ~~3.8,~~2.3 above, penalties levied for the violation of a reliability standard shall bear a reasonable relation to the seriousness of the violation. As part of the assessment of the seriousness of the violation, NERC or the regional entity shall ~~The seriousness of a given violation by a given violator shall be assessed by~~ review ~~of the applicability of~~ the Violation Risk Factors[3] associated with the violation and~~to~~ the characteristics of the violator's operation or power system. NERC or the regional entity may consider the size of the violator.~~Size is a characteristic of a violator's operation or system. The size of the violator can be considered in the assessment but shall not be the only characteristic considered. Where size is considered in such a review the facts relating to the violation in question will be reviewed~~ NERC or the regional entity will also consider the facts of the violation so ~~such~~ that the "actual" size of the violator is ~~properly discerned and~~ appropriately considered~~;~~. ~~t~~The following are provided as illustrative examples:

- If the violator belongs to a generation and transmission cooperative or joint-action agency, size will be attributed to the particular violator, rather than to that generation and transmission cooperative or joint-action agency.
- If the violator constitutes part of a corporate family the size of the violator will be attributed to that violator alone, in the absence of any facts indicating involvement of the whole corporation or corporate affiliates of the violator.
- If the violator is an entity established solely as a shell to register as subject to one or more Reliability Standards the size of the entity will be disregarded in favor of consideration of the size of the parent entity or any affiliates that NERC or the regional entity deems involved and constituting the "actual" size of the violator.

At the request of the violator, NERC or the applicable regional entity or entities may review the penalty in light of the violator's financial ability to pay the penalty. Financial ability shall include ~~both~~ the financial strength of the entity as well as its financial structure (e.g., for-profit versus non-profit). Where penalties are reduced or eliminated, NERC or the regional entity ~~shall~~may consider non-monetary sanctions ~~or remedial action~~ as alternatives or substitutes to ~~the~~a monetary penalty, pursuant to Sections ~~3~~2.12~~17~~, ~~3~~2.13~~18~~ and ~~3~~2.14~~19~~, below, of these Sanction Guidelines~~this document~~.

~~The above actions will: (i) promote that violators are penalized or sanctioned commensurate with the risk or effect that their specific violation of the reliability standards had or is having to the reliability of the bulk power system while also; (ii) mitigating overly burdensome penalties to less consequential or financially-limited entities concurrent with; (iii) promoting that no penalty is inconsequential to the violator to whom it is assessed. This will promote that penalties levied for violations of reliability standards bear a reasonable relation to the seriousness of the violation while also addressing violators' ability to pay the penalties they are assessed.~~ Consideration of the factors described in this subsection is intended to (i) promote that violators are penalized or sanctioned commensurate with the risk or effect that their specific violation of the reliability standards had or is having on the reliability of the bulk power system while also (ii) mitigating overly burdensome penalties to less consequential or financially-limited entities concurrent with (iii) promoting that no penalty is inconsequential to the violator to whom it is assessed. Consideration of these factors is intended to result in penalties levied for violations of reliability standards bearing a reasonable relation to the seriousness of the violation while also addressing violators' ability to pay the penalties they are assessed.

[3] See Section ~~4 Part~~ ~~4~~3.1.1 for a discussion of these factors.

~~3.12~~2.7 Violation Time Horizon

Reliability standards involving longer and broader time horizons, such as long-term planning activities, may have a lesser immediate impact and pose less immediate risk to the reliability of the bulk power system than standards ~~addressing~~involving shorter and narrower timeframes, such as entities' conduct in real time. Similarly, standards involving longer and broader time horizons typically will provide a longer time period over which to discover and remedy a violation when compared to standards involving~~addressing~~ more immediate activities such as next-day planning, same-day operations or real-time operations. Using a time horizon element in the determination of penalties for violations provides for recognition of the "more immediate" nature — and hence higher risk — of the threat of some violations as opposed to the lesser-risk "future threat if not corrected" nature of other violations.

NERC or the regional entity ~~Penalties levied for the violation of a reliability standard~~ shall consider the time horizon of the standard violated~~;~~. ~~v~~Violations of standards involving ~~more~~ immediate or real-time activities will generally incur larger penalties than violations of standards with longer or broader time horizons.

Time horizons inherent in reliability standard requirements are not reflected in the~~ir assigned~~ Violation Risk Factors or Violation Severity Levels for the requirement.[4]~~.~~ Accordingly, the time horizon element of a violation will be considered when determining the Base Penalty Amount[5] for the violation.

NERC or the regional entity will utilize judgment and will analyze the facts of the violation to determine ~~T~~the time horizon for the violation~~considered~~ and its impact on the selection of the Base Penalty Amount~~ for the violation will be decided upon by NERC or the regional entity based upon judgment and the facts of the violation. The rationale for the time horizon used and its impact on the setting of the Base Penalty Amount will be documented by NERC or the regional entity and provided within the Notice of Penalty issued for the violation~~. The rationale for the time horizon used and its impact on the setting of the Base Penalty Amount will be provided within the Notice of Penalty issued for the violation.

~~3.13~~2.8 Extenuating Circumstances

In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the regional entity may significantly reduce or eliminate penalties~~ may be significantly reduced or eliminated~~.

~~3.14~~2.9 Concealment or Intentional Violation

NERC or the regional entity ~~Penalties levied for the violation of a reliability standard~~ shall always consider as an aggravating factor~~take into consideration~~ any attempt by a violator to conceal the violation from NERC or the regional entity, or any intentional violation incurred for purposes other than a demonstrably good faith effort to avoid a significant and greater threat to the immediate reliability of the bulk power system.

~~3.15~~2.10 Economic Choice to Violate

~~Owners, operators, and users of the bulk power system may be presented with situations or circumstances where compliance with the reliability standards preclude or reduce an economic gain that could be realized by violating the standards.~~ Penalties shall be sufficient to assure that entities responsible for complying with reliability standards do not have incentives ~~find it attractive~~ to make economic choices that cause or unduly risk violations of~~to~~ reliability standards, or ~~risk or cause~~ incidents resulting from violations of the reliability standards. Economic choice includes economic gain for, or the avoidance of costs to, the violator. NERC or the regional entity shall treat economic

[4] See Section ~~4 Part 4~~3.1~~1~~ for a discussion of these factors.
[5] See Section ~~4 Part 4~~3.2

choice to violate as an aggravating factor when determining a penalty. ~~Penalties levied to violators who have made such a choice shall reflect this aspect of the violation.~~

~~3.16~~2.11 No Influence by Outcome of Economic Choice to Violate

~~Economic choices to violate are generally made for the violator's own potential gain, but making such a choice does not always result in all potential gains being realized or may result in damage or loss. However, irrespective of~~Whatever the financial outcome to the entity making an economic choice to violate a reliability standard, such decisions present a risk to~~others'~~ reliability and to others, commonly without ~~either~~ their knowledge or consent. Penalties levied to violators making an economic choice to violate shall reflect only that the violator made an economic choice to violate a reliability standard. ~~was made at all; t~~The lack of or reduced magnitude of any actual benefit received, or any damage suffered, by the violator as a consequence of making this choice will have no influence upon the determination of the penalty ~~to be levied~~.

~~3.17~~2.12 Non-Monetary Sanctions ~~or Remedial Actions~~

Enforcement actions taken by NERC or a regional entity are not limited to monetary penalties~~;~~. NERC or the regional entity may apply, at ~~the~~its discretion ~~of NERC or the regional entity~~, non-monetary sanctions ~~or remedial actions may also be applied and can~~ includinge limitations on activities, functions, operations, or placement of the violator's name on ~~other appropriate sanctions, including the establishment of~~ a reliability watch list ~~composed~~ of major violators.

~~3.18~~2.13 Non-Exclusiveness of Monetary Penalties or Non-Monetary Sanctions

NERC or the regional entity may impose a~~A~~ non-monetary sanction ~~may be imposed either~~ in lieu of or in addition to a monetary penalty ~~imposed~~ for the same ~~confirmed~~ violation, and vice versa. Imposition of a monetary penalty or non-monetary sanction for a violation does not preclude the imposition of the other as long as~~, in combination,~~ the aggregate penalty ~~continues to~~ bears a reasonable relation to the seriousness of the violation and other relevant factors.

~~3.19~~2.14 Monetization of the Value of Sanctions

A significant element of NERC's oversight of penalties, sanctions, and remedial action directives determined and levied or required by regional entities is to ensure~~ing~~ acceptable similarity in the degree and type of sanction for violations constituting comparable levels of threat to the reliability of the bulk power system by similarly situated entities. It is also a requirement and a commitment of NERC and the regional entities~~its designees~~ that penalties~~,~~ or sanctions~~, or remedial actions~~ levied ~~or applied~~ for the violation of a reliability standard bear reasonable relation to the seriousness of the violation. ~~Specifically with respect to penalties and sanctions, it is intuitive that i~~It is~~will be~~ easier, more objective, and more transparent to monitor and test for the acceptable similarity of penalties and sanctions if ~~(~~monetary~~)~~ penalties or monetized values of sanctions ~~determined for violations~~ are used as the primary basis of comparison~~, versus comparisons made on the basis of other (non-monetized) considerations~~. Similarly, there will be ~~strong intuitiveness and~~ transparency, particularly to those ~~interested but not strongly~~ familiar with the power industry, that NERC or the regional entity reasonably addressed the seriousness of a violation ~~has been reasonably addressed~~ if the consequences ~~for it to the violator~~ are ~~determined and can be~~ expressed clearly and quantifiably in monetary terms.

Penalties determined and levied by NERC or regional entities will by definition be valued in monetary terms: U.S or Canadian dollars. It ~~will be~~is the preference of NERC that ~~(~~non-monetary~~)~~ sanctions imposed either in lieu of or in addition to a penalty should include disclosure of the monetary value of~~that~~ the sanctions ~~represent to the violator~~. ~~It is intuitive that defensible monetary values for those sanctions will be most easily determined if~~ Generally, NERC or the regional entity will first determine the penalty for the violation ~~pursuant to these guidelines is first determined~~ and may, at their discretion, introduce~~then the~~ sanctions ~~to be levied are introduced and justified~~ as appropriate alternatives to the~~at~~ penalty or as additions to a lesser penalty. However, NERC or the

regional entity may determine the monetary value of sanctions ~~may be determined directly (e.g. without first determining a penalty amount) and monetized~~ using other methods.

~~NERC does not have a preference between penalties and sanctions for violations. The preference expressed here will support ensuring comparability of outcomes regarding application of these guidelines and the promotion of reasonable relationship between the seriousness of a violation and the sanctions, or penalties and sanctions, levied for it.~~

~~3.20Maximum Limitations on Penalties~~

~~Penalties are direct, monetary judgments levied against a violator by NERC or the regional entity for the violation of requirements of the reliability standards. In contrast, sanctions will impose limitations or restrictions of some kind that may result in economic or other impacts to the violator, and remedial actions are directives by NERC or a regional entity to the violator regarding the correction of conditions, practices or any other relevant action or activity underlying the noncompliance(s) involved.~~

2.15 Maximum Limitations on Penalties

~~In the United States, the Federal Power Act allows for the imposition of civil penalties of up to $1,000,000 per day per violation.~~ ~~NERC and the regional entities draw their authority to levy penalties from the Federal Power Act; accordingly this figure is and can be understood as the maximum monetary penalty that NERC or regional entities are authorized to levy. However, as this legislation also requires that "[a]ny penalty imposed … shall; (A) bear a reasonable relation to the seriousness of the violation; and (B) take into consideration the efforts of the user, owner, or operator to remedy the violation in a timely manner[6]"~~ ***~~entities required to comply with the reliability standards must also understand that~~*** ~~In~~ In the United States, the maximum penalty amount that NERC or a regional entity will assess for a violation of a reliability standard requirement is $1,000,000 per day per violation. NERC and the regional entities will ~~be obligated to~~ assess penalties amounts up to and including thise maximum amount for violations where warranted pursuant to these Sanction ~~g~~Guidelines.

In Canadian jurisdictions the maximum monetary penalty ~~potentially assessable~~ for a reliability standard violation is significantly less than $1,000,000 per day per violation. ~~the amount allowed in the United States under the Federal Power Act.~~ ~~Also~~Further, legislation presently governing certain~~some~~ Canadian jurisdictions does not accommodate the levying of such a penalty under certain~~some~~ circumstances, may not accommodate the levying of such a penalty for all violations, or does not accommodate the levying of any monetary penalties.

When NERC or a regional entity levies a penalty ~~may be levied~~, or propose~~s~~d ~~to~~ a penalty to regulatory authorities with jurisdiction to ~~be~~ levy~~ied~~ a penalty, NERC or the regional entity shall~~the~~ follow~~ing~~ these steps ~~will be followed~~:

a. NERC or the regional entity will initially disregard the penalty limitations of the applicable regulatory authorities ~~with jurisdiction~~, and will determine what the penalties or sanctions would be pursuant to these ~~s~~Sanction ~~g~~Guidelines ~~only~~.

b. NERC or the regional entity will review the maximum penalty allowed in the applicable~~by the regulatory authorities with~~ jurisdiction.

c. NERC or the regional entity will set the actual penalty ~~to be levied, or proposed to the regulatory authorities with jurisdiction to be levied,~~ as the lesser of (i) the penalty~~that~~ determined pursuant to these Sanction ~~g~~Guidelines and (ii) the maximum penalty or sanction allowed in~~by~~ the applicable jurisdiction~~regulatory authorities~~.

d. If ~~the lesser penalty is~~ the maximum penalty allowed in the applicable jurisdiction is lower than the penalty determined under the Sanction Guidelines, in addition to the legally permissible

[6] ~~H.R.6, Energy Policy Act of 2005, Section 215, Paragraph e, subparagraph 6.~~

penalty ~~by the regulatory authorities~~, the notice of penalty or similar document issued by NERC or the regional entity regarding the violation will also list the penalty that was determined pursuant to these Sanction ~~g~~Guidelines.

Adhering to the above steps will insure that ~~the result of~~ the determination of any penalty for any violation will produce output that can be directly compared (i.e. without influence of ~~local authorities'~~ any penalty limitations or restrictions applicable in certain jurisdictions) with the penalty determined for any other violation, thus assisting the efforts of NERC and others to ensure that these Sanction ~~g~~Guidelines are uniformly applied and that there is an acceptable level of consistency in their application ~~of these sanction guidelines~~ across North America. Regulatory authorities with jurisdiction may also find such information useful for their determination of the appropriateness of any penalty or sanction proposed to them to be levied against a violator of the reliability standards. ~~Similarly, policy and legislative bodies may find such information of value to the review or development of arrangements addressing such matters.~~

~~3.21~~2.16 Frequency and Duration of Violations

~~Section 316A of the Federal Power Act [16 U.S.C. § 825o-1(b)], as amended by the Energy Policy Act of 2005, provides that "any person who violates any provision of Part II of this title or any provision of any rule or order thereunder shall be subject to a civil penalty of not more than $1,000,000 for each day that such violation continues."~~

~~FERC Order No. 672 interprets this statement as setting a cap on the monetary penalties that the Commission, NERC and regional entities can impose under FPA section 215. FERC has referred to this statutory provision as imposing a maximum $1,000,000 "per day, per violation" penalty and has directed that the ERO must ensure that in the U.S. such a penalty amount ($1,000,000), in such a manner ("per day, per violation"), can be imposed for a violation of the Reliability Standards should the conduct at issue so warrant.~~

As stated in Section 2.15 above, the maximum penalty that will be imposed in the U.S. for violation of a reliability standard is $1,000,000 per day. However, ~~S~~some ~~R~~reliability ~~S~~standards may not support the assessment of penalties on a "per day, per violation" basis, but instead should have penalties calculated based on an alternative penalty frequency or duration. Where NERC or the regional entity deems that a monetary penalty is warranted, or where NERC or the regional entity ~~is~~ monetize~~s~~~~ing~~ (Section 2.14~~3.19~~) the value of a non-monetary sanction, ~~for the violation of such a standard NERC or the regional entity~~they shall determine the penalty or monetized amount consistent with the following:

Multiple Instances of Violation on One Day

The nature of some ~~R~~reliability ~~S~~standards includes the possibility that an entity could violate the same requirement two or more times on the same day. In this instance, NERC and~~or~~ the regional entity are~~is~~ not limited to penalizing the violator a maximum of $1,000,000 per day. ~~As NERC or the regional entity deems appropriate~~ NERC or the regional entity may deem that ~~there have been~~ multiple violations of the same requirement ~~that~~ occurred on the same day, each of which is subject to the maximum potential penalty of $1,000,000 per violation, per day. Also, NERC or the regional entity is not constrained to assessing the same penalty amount for each of the multiple violations, irrespective of their proximity in time.

Cumulative Over Time

Certain requirements of ~~the R~~reliability ~~S~~standards are measured not on the basis of discrete acts, but ~~of~~on cumulative acts over time. Reliability ~~S~~standards that fall into this category ~~are~~ generally ~~those~~ involve~~ing~~ measurements based on averages over a given period. ~~Where a violation of such a standard has occurred the element of averaging performance over a period of time introduces the~~

~~difficulty to NERC or the regional entity of reasonably identifying (i) what date the violation should be deemed to have occurred and (ii) its duration.~~

If a Reliability ~~S~~standard requirement measured by an average over time can only be violated once per applicable period, ~~then~~ there is risk that a disproportionately mild penalty might be levied in a situation where the violation was serious and the effects on the Bulk-Power System were severe. In the future, as individual reliability standards are revised, each ~~R~~reliability ~~S~~standard requirement that is based on an average over time will specify the minimum period in which a violation could occur and how to determine when a violation arises, which may be other than once per applicable period[7]. In the interim until relevant ~~R~~reliability ~~S~~standards are so modified, where assessing a penalty for violation of~~any ambiguity on this point will be construed conservatively, meaning that where an entity has not complied with~~ such a standard, NERC or the regional entity will generally consider that only one violation occurred per measurement period. However, ~~notwithstanding this general principle of one violation per measurement period,~~ if an average must be measured by a span of time greater than a month, each month of that span shall constitute at a minimum one violation.

Periodically Monitored Discrete Violation

Some ~~R~~reliability ~~S~~standards may involve discrete events which are only monitored periodically or which are reported by exception. If a requirement of such a standard states that a discrete event constitutes a violation, then (i) a violation arises when that event occurs and (ii) that violation continues until remedied; and~~furthermore,~~ (iii) the violation ~~is deemed to have~~ occurred at the point that the entity ~~-~~entered into noncompliance with the reliability standard, regardless of the monitoring period for the activity or its date of discovery or reporting. For example, if a task required by a ~~R~~reliability ~~S~~standard requirement was~~has~~ not ~~been~~ done by the required date, it is irrelevant that monitoring for compliance for the requirement occurs only on a yearly or other periodic basis; NERC or the regional entity will deem a violation to have occurred on the first day of noncompliance and each day thereafter until compliance is effectuated. Similarly, if a discrete event occurs and is not remedied on the date of its occurrence, then NERC or the regional entity will deem a violation to have occurred on the day of the first instance of the noncompliance and each day~~, or portion thereof~~ thereafter until the entity is in compliance ~~is effectuated~~.

~~Non-compliance with a standard of this type will subject the violator to the potential maximum monetary penalty of $1,000,000 per violation per day in violation.~~

NERC or the regional entity may, at its discretion, ~~is not constrained to~~ assess~~ing~~ the same penalty amount for each day that the entity was in violation of the r~~R~~eliability s~~S~~tandard requirement in question.

[7] ~~Para. 41; FERC Order on Clarification and Rehearing [Docket No. RR06-1-006]~~

4.3. Determination of Monetary Penalties

~~The following~~This section describes the specific steps that NERC or the regional entity will follow to determine the monetary penalty for a violation[8]. The determination of non-monetary sanctions is discussed in Section ~~5~~4 of this document~~; Section 6 discusses remedial action~~.

Step 1. NERC or the regional entity will set ~~T~~the Base Penalty Amount for the violation ~~will be set~~ as discussed in Sections ~~4~~3.1 and ~~4~~3.2, below.

Step 2. NERC or the regional entity will adjust the~~The~~ Base Penalty Amount set in Step 1 ~~will be reviewed~~ pursuant to Section ~~4~~3.3, below. This will result in the Adjusted Penalty Amount.

Step 3. NERC or the regional entity may review ~~T~~the Adjusted Penalty Amount determined in Step 2 ~~may be reviewed~~ in light of the violator's financial ability to pay the penalty. Also, where applicable, NERC or the regional entity will ~~re~~confirm that the penalty ~~set~~ will disgorge unjust profits or economic benefits associated with an economic choice to violate.[9] ~~.~~ At the conclusion of this review, NERC or the regional entity will set the Final Penalty Amount ~~will be set.~~

Step 4. NERC or the regional entity will take into account any limitations on the maximum permissible penalty in the applicable jurisdiction.

~~Unless NERC or the regional entity deems alternative frequency or duration is warranted penalties shall be assessed on a per violation per day basis.~~ At the discretion of NERC or the regional entity, a penalty may be assessed on a per violation per day basis or with alternative frequency or duration. Where NERC or the regional entity deems that alternative penalty frequency or duration is warranted, the Notice of Penalty associated with the violation will clearly identify this and provide the rationale for it. Where NERC or the regional entity deems that alternative penalty frequency or duration is warranted, penalties shall be determined in accordance with section ~~3.21~~2.16 of the~~se~~ Sanction Guidelines.

4.~~1~~3.1 Initial Value Range of the Base Penalty Amount

NERC or the regional entity will determine an initial value range for the Base Penalty Amount by considering ~~two factors regarding the violation:~~ the Violation Risk Factor ("VRF") of the requirement violated and the Violation Severity Level ("VSL") assessed for the violation. Using the Base Penalty Amount Table provided in Appendix A NERC or the regional entity will look up the initial value range for the Base Penalty Amount by finding the intersection of the violation's VRF and VSL on the table.[10] ~~.~~

4.~~1~~.~~1~~3.1.1 Violation Risk Factor

Each ~~requirement set out within NERC's~~ reliability standard~~s~~ requirement has been assigned a ~~Violation Risk Factor (~~VRF~~)~~ through the NERC reliability standards development process. The VRF~~factor~~s have been defined and approved through the standards development process and are assigned to requirements to provide clear, concise and comparative association between the violation of a requirement and the expected or potential impact of the violation to the reliability of the bulk power system. One of three defined levels of risk is assigned to each standards requirement: Lower VRF~~Risk Factor, or~~; Medium VRF~~Risk Factor,~~; or~~:~~ High VRF~~Risk Factor~~. ~~Definitions of the factors can be found in appropriate standards development process documentation.~~

[8] The text in this section discusses the determination of a single penalty for an individual violation; however, the process laid out is also applicable to determining the individual penalties, or a single aggregate penalty, for multiple violations that are associated with each other as discussed in Section ~~3 Part 3~~2.~~8~~1 of this document.

[9] ~~Reference: Section 3 Parts 3.15 and 3.16.~~

[10] As discussed in Section ~~3 Part 3~~2.~~5~~1 of this document, where there is more than one violation ~~in play~~, but the violations are sufficiently associated, NERC or the regional entity may set a single initial value range that is appropriate in light of the individual VRF/VSL combinations of the violations.

4.1.23.1.2 Violation Severity Level

Violation severity levels (VSLs) are defined measurementslevels of the degree to which a violator violated a requirement of a reliability standard was violated. Whereas VRFsviolation risk factors are determined pre-violation and indicate the relative potential impacts that violations of each standard could pose to the reliability of the bulk power system, VSLs arethe violation severity level is assessed post-violation and areis an indicator of the severity of thehow severely the violator actually violatedviolation of the standard(s) requirement(s) in question.

These Sanction gGuidelines utilize the VSLsviolation severity levels, which that have been established[11] by NERC for requirements of the reliability standards. Up to four levels can be defined for each requirement; the levels have been designated as: Lower, Moderate, High, and Severe.

4.23.2 Setting of the Base Penalty Amount

NERC or the regional entity will set the Base Penalty Amount set for the violation may be set at the highest figure of the initial value range determined pursuant to Section 4.13.1, above. However, NERC or the regional entity may set the Base Penalty Amount at or below the lowest figure of the initial value range in light of two specific circumstances regarding the violation and the violator, specifically:

a. The applicability of the VRFViolation Risk Factor of the violation to the specific circumstances[12] of the violator.

b. Whether this is an inconsequential first violation by the violator of the reliability standard(s) in question.

As noted in Section 3.122.7, NERC or the regional entity will consider the time horizon forinvolved with the violation when setting the Base Penalty Amount for the violation. As also noted in Section 3.12 this consideration will be documented for inclusion in the Notice of Penalty issued for the violation.

The penalty amount resulting from the this review will be the Base Penalty Amount that is used as the basis for further adjustment pursuant to the factors discussed in the next section (3.3) of this document.

4.2.13.2.1 Applicability of the Violation Risk Factor

Violation Risk FactorsVRFs are assigned to standards' requirements as indicators of the expected risk or harm to the bulk power system posed by the violation of a requirement by a typical or median entity that is required to comply. NERC or the regional entity may consider the specific circumstances of the violator to determine if the violation of the requirement in question actually produced the degree of risk or harm anticipated by the VRFViolation Risk Factor. If that expected risk or harm was not or would not have been produced, NERC or the regional entity may set the Base Penalty Amount to a value it (i) deems appropriate and (ii) is within the initial value range set above pursuant to Section 3.1.

4.2.23.2.2 First Violation

If the actual or foreseen impact of the violation is judged to be inconsequential by NERC or the regional entity and the violation is the first incidence of violation of the requirement in question by the violator, NERC or the regional entity may at its discretion: (i) set the Base Penalty Amount to a value it deems appropriate within the initial value range set above

[11] Assignment of these levels will be complete and filed with the Commission by March 1, 2008 in accordance with FERC Order on Compliance Filing dated June 7, 2007 [Docket No. RR06-1-007] .

[12] The circumstances of the violator will include but not be limited to, as appropriate: the violator's aggregate and net load;, and interconnections characteristics such as voltage class and transfer ratings;

pursuant to Section ~~4~~3.1, or (ii) excuse the penalty for the violation (i.e. set the Base Penalty Amount to $0~~$~~).

This relief will generally not be afforded to the violator if NERC or the regional entity determines that the violator has a poor internal compliance program, culture of compliance or compliance record; e.g. the circumstances discussed in Section ~~4~~3.3.1 have been an aggravating factor in one or more previous penalties assessed against~~to~~ the violator.

This relief will not be available for consideration in those instances where the violator ~~has~~ concealed or attempted to conceal the violation, failed or refused to comply with compliance directives from NERC or the regional entity, or intentionally violated for purposes other than a demonstrably good faith effort to avoid a significant and greater threat to the immediate reliability of the bulk power system.

~~4.3~~3.3 Application of Adjustment Factors

Adjustment factors provide an~~the~~ opportunity for~~to~~ NERC or the regional entity to adjust the base penalty to reflect the specific facts and circumstances material to each violation and violator.

These guidelines recognize and require that, as a minimum, NERC or the regional entity consider the following:

a. Repetitive violations and the violator's compliance history

b. Failure of the violator to comply with compliance directives

c. Disclosure of the violation by the violator through ~~S~~self-reporting~~disclosure~~, or as the result of a compliance self-analysis following a bulk power system event, and voluntary mitigating activities~~corrective action~~, by the violator

d. Degree and quality of cooperation by the violator in the violation investigation and in any remedial action directed for the violation, including the violator's cooperation in an event analysis concerning, and the performance of a compliance self-analysis by the violator following, a bulk power system event in which the violation occurred or to which it related.

e. The presence and quality of the violator's compliance program ~~quality~~

f. Settlement

~~f~~g. Any attempt by the violator to conceal the violation

h. Intentional violations

~~h~~i. Extenuating circumstances

~~Two documents issued by United States regulatory agencies will be instructive to NERC and the regional entities when they are determining penalties for violations of the reliability standards: the FERC's Policy Statement on Enforcement issued on October 20, 2005 under Docket No. PL06-00, and; U.S Securities and Exchange Commission (SEC) Release No. 44969 under the Securities and Exchange Act of 1934, issued on October 23 2001, also concurrently issued by the SEC as Release No. 1470 under Accounting and Auditing Enforcement.~~

NERC or the regional entity may also consider other ~~additional~~ factors it deems appropriate under the circumstances, as long as their use is clearly identified and adequately justified. The effect of using these factors must~~will also~~ be fully and clearly disclosed in the Notice of Penalty and supporting documents.

~~4.3.1~~3.3.1 Repetitive Violations and Compliance History

~~A bulleted point under Paragraph 20 of the FERC Policy Statement on Enforcement highlights repeat offenses by a violator.~~ If a violator has had repetitive infractions of the same

or a closely-related reliability standard requirement, particularly within a time frame defined within the standard(s) or deemed appropriate by NERC or the regional entity in the absence of a definition of~~the standard(s) defining the~~ a time frame in the relevant standard, NERC or the regional entity shall consider an~~some~~ increase to the penalty. In evaluating the violator's compliance history, NERC or the regional entity will take into account previous violations by affiliates of the violator, particularly violations of the same or similar reliability standard requirements, and will evaluate whether any such prior violations reflect recurring conduct by affiliates that are operated by the same corporate entity or whose compliance activities are conducted by the same corporate entity.

The ~~term "violation~~ reset ~~time~~ period~~"~~ or reset time frame of a standards requirement may be defined or implied within a given standard as~~to describe~~ the period of time generally required for a violator to continue operations without ~~incidence of further violation(s) of the~~violating a ~~R~~reliability ~~S~~standard~~s~~, particularly ~~of~~ the initial reliability standard violated or a similar standard ~~violated, in order to avoid~~Expiration of this reset period or reset time frame would serve to negate or minimize consideration of the violator's previous violation history for sanctioning purposes in the event of a subsequent violation(s). NERC or~~and~~ the ~~R~~regional entity~~Entities~~ shall exercise appropriate judgment and discretion in this regard as warranted by the facts and circumstances, particularly where no reset ~~time~~ period or reset time frame is specifically set within the standard violated. Repeat violations within violation reset ~~time~~ periods or reset time frames are aggravating factors in the determination of the penalty or sanction~~ing~~. ~~Accordingly, a~~A violation history of no violations will produce no mitigation of the penalty otherwise determined; a violation history of infrequent minor violations of lesser risk requirements assessed lower VSLs~~violation severity levels~~ may result in small or no increase; and a history of more frequent violations or previous violations of higher risk requirements assessed more severe VSLs~~violation severity levels~~ will generally incur commensurately larger increases.

~~4.3.2~~3.3.2 Failure to Comply with a Remedial Action~~Compliance~~ Directives or with Agreed Corrective or Mitigating Activity

If the violator has violated reliability standard requirements despite~~notwithstanding having~~ receiv~~inged~~ related remedial action ~~compliance~~ directives or despite having agreed to corrective or mitigating activities for prior violations, ~~such as for remedial action from NERC or the regional entity,~~ NERC or the regional entity shall consider increasing~~some increase to~~ the penalty.

~~4.3.3~~3.3.3 Disclosure of the Violation Through Self-Reporting and Voluntary Mitigating Activities by the Violator~~Corrective Action~~

NERC or the regional entity shall consider whether a violator ~~self-~~reported~~disclosed~~ the violation by a self-report, or as the result of a compliance self-analysis conducted by the violator following a bulk power system event, prior to detection or intervention by NERC or the regional entity, and any mitigating activities voluntarily~~action~~ undertaken by the violator to correct the ~~situation~~noncompliance. ~~NERC or the regional entity will be instructed in their consideration of these factors by the text of Paragraphs 24 and 25 of the FERC Policy Statement on Enforcement.~~ As they deem warranted, NERC or the regional entity may reduce the violator's penalty ~~consistent with the cited sections of the FERC policy~~. If a self-report or a self-certification submitted by the violator accurately identifies a violation of a Reliability Standard, an identification of the same violation in a subsequent compliance audit or spot check will not subject the violator to an escalated penalty as a result of the compliance audit process unless the severity of the violation is found to be greater than reported by the violator in the self-report or self-certification.

~~4.3.4~~3.3.4 Degree and Quality of Cooperation ~~in Violation Investigation and Remedial Action~~

NERC or the regional entity shall consider the degree and quality of the violator's cooperation with NERC or the regional entity ~~in the investigation of the violation and any remedial action arising from it~~. ~~NERC or the regional entity will be instructed in making their determination on this by the text of Paragraphs 26 and 27 of the FERC Policy Statement on Enforcement.~~ NERC or the regional entity may adjust the violator's penalty as they deem appropriate, which ~~warranted commensurate with the cited sections of the FERC policy statement. This~~ may result in an increase, a decrease or no change to the penalty. If the violation occurred in connection with a bulk power system event and the violator is cooperative in the event analysis process and performs an appropriate compliance self-analysis following the event, the violator's actions will be considered as mitigating factors in the determination of any penalties or sanctions for violations occurring in connection with the event.

~~4.3.5~~3.3.5 Presence and Quality of Violator's Internal Compliance Program

NERC or the regional entity shall consider the presence and quality of the violator's internal compliance program, if any, and other indicators of the violator's culture of compliance. ~~NERC or the regional entity will be instructed in making their determination on this factor by the text of Paragraphs 22 and 23 of the FERC Policy Statement on Enforcement. As they deem warranted,~~ NERC or the regional entity may reduce the violator's penalty as they deem appropriate. ~~consistent with the cited sections of the FERC policy. Consistent with the FERC policy~~ However, NERC or the regional entity may not increase a violator's penalty ~~specifically~~solely on the grounds that the violator has no internal compliance program or a poor quality program.

3.3.6 Settlement

NERC or the regional entity may consider a reduction in penalty if the violator resolves the violation through settlement, taking into account the speed with which settlement was reached.

~~4.3.6~~3.3.7 Violation Concealment and Non-Responsiveness

~~Two bulleted points under Paragraph 20 of the FERC Policy Statement on Enforcement highlight misrepresentation of material facts and resistance or impediment to inquiry of a violation. When determining a penalty NERC or the regional entity shall consider any concealment or attempt to conceal the violation, or information needed to investigate the violation, on the part of the violator.~~ NERC or the regional entity shall consider a significant increase to the penalty ~~I~~if NERC or the regional entity determines, based on its review of the facts, that the violator concealed or attempted to conceal the violation or information necessary to investigate the violation. The presumption in such circumstances is to double ~~, some significant increase to the penalty shall be considered; doubling of the penalty otherwise determined is suggested. Conduct of this nature on more than one occasion regarding one violation, or with respect to more than one violation, should incur an even larger increase to~~ the penalty otherwise determined. Additionally, NERC or the regional entity shall consider an increase to the penalty if NERC or the regional entity determines, based on its review of the facts, that the violator resisted or impeded the discovery and review of a violation.

~~4.3.7~~3.3.8 Intentional Violation

~~Another bulleted point under Paragraph 20 of the FERC Policy Statement on Enforcement highlights offenses as willful action by a violator.~~ When determining a penalty, NERC or the regional entity shall consider if the violator intentionally violated the reliability standard ~~without just cause; i.e.,~~ for purposes other than a demonstrably good faith effort to

avoid a significant and greater threat to the immediate reliability of the bulk power system. If the violator engaged in such conduct, a~~some~~ significant increase to the penalty shall be considered; the presumption in such cases is to doubl~~e~~~~ing of~~ the penalty otherwise determined ~~is suggested~~. If conduct of this nature has been detected on more than one occasion, NERC or the regional entity should assess an even larger increase to the penalty ~~otherwise determined~~.

NERC or the regional entity will consider violations attributable to an economic choice to violate as intentional violations. ~~Consistent with the FERC Policy Statement on Enforcement a~~Any penalty issued involving conduct of this manner shall a~~t~~s a minimum disgorge any profits or economic benefits the violator acquired as a consequence of the behavior, whenever and to the extent that they can be determined or reasonably estimated.

~~4.3.8~~3.3.9 Extenuating Circumstances

NERC or the regional entity will consider any~~if there are~~ extenuating circumstances regarding the violation that justify reduction or elimination of the penalty otherwise determined.

~~Consideration of adjusting a penalty for this factor would be inconsistent with NERC or the regional entity increasing a penalty after consideration of any other factor included in this section of these guidelines, such as intentional violation without justifiable cause or concealment or attempt to conceal.~~

~~4.4~~3.4 Setting of the Final Penalty Amount

The Adjusted Penalty Amount determined in Step 2 may be reviewed in light of the violator's financial ability to pay the penalty. ~~Also, i~~If the violation ~~was~~resulted from an economic choice, NERC or the regional entity will ~~re~~confirm that the penalty ~~set~~ will disgorge any unjust profits or economic benefits. At the conclusion of this review, if applicable, NERC or the regional entity will set the Final Penalty Amount ~~will be set~~.

~~4.4.1~~3.4.1 Violator's Financial Ability to Pay[13]

At the written request of the violator, NERC or the regional entity will review the penalty determined in Step 2 in light of relevant, verifiable information that the violator provides regarding its~~their~~ financial ability to pay. At the conclusion of this review NERC or the regional entity may:

1. Reduce the penalty ~~payable~~ to an amount that NERC or the regional entity~~, as applicable,~~ deems that the violator has the financial ability to pay, or;
2. Excuse the penalty amount payable, or;
3. Sustain the penalty amount determined in Step 2.

~~Where the penalty amount has been reduced or excused,~~ If NERC or the regional entity reduces or excuses the penalty, NERC or the regional entity shall consider the assessment of appropriate non-monetary sanction(s) as a substitute or an alternative for the penalty amount otherwise considered appropriate ~~that has been excused or by which the penalty has been reduced~~.

~~4.4.2~~3.4.2 ~~Rec~~Confirmation of Disgorgement of Unjust Profit or Gain

Notwithstanding the application of any other consideration or factor applicable to the determination of a just and reasonable penalty for the violation, if the violation in question involved an economic choice to violate a reliability standard, NERC or the regional entity

[13] NERC anticipates that this will be the primary vehicle for addressing the ability to pay of "not-for-profit" and other similar organizations.

shall ~~re~~confirm that the penalty ~~set~~ meets the requirements set forth in ~~Parts 3.15 and 3.16 of~~ Section~~s~~ ~~3~~2.10 and 2.11 of this document.

~~5.~~4. Determination of Non-Monetary Sanctions

The imposition of sanctions is not limited~~bounded~~ to monetary penalties. Non-~~M~~monetary sanctions ~~applied must~~may be applied with the objective of promoting reliability and compliance with the reliability standards. Non-monetary sanctions may include~~, but not be limited to, the following:~~ limiting activities, functions, or operations, or placing the violator on a reliability watch list of significant violators.

~~a.Limitations on activities, functions, or operations~~

~~a.Placing an entity on a reliability watch list composed of major violators~~

6.Remedial Action

6.1Definition and Anticipated Use

Remedial actions are directives that may be issued to a bulk power system owner, operator, or user to resolve an alleged violation of a reliability standard by addressing conditions, practices, or any other relevant action or activity that is immediately necessary to terminate or correct to protect the reliability of the bulk power system from an imminent threat. A remedial action directive will be issued when NERC or the regional entity identifies an alleged violation of a reliability standard that must be corrected immediately to protect the reliability of the bulk power system from the imminent threat that NERC or the regional entity has identified.

NERC or the regional entity will generally employ remedial action directives where they deem it necessary to clearly specify minimum corrective actions that the subject of the remedial action directive must take; additionally or alternatively a remedial action directive may clearly specify timelines within which the subject must take specified actions, complete specified tasks, or achieve specified outcomes. Also, to the extent NERC or the regional entity is authorized to do so, a remedial action directive may communicate penalties, sanctions, or further remedial actions that may be imposed should the specific remedial action directive not be complied with by those to whom it has been issued. As a rule of thumb, remedial action directives will be of use to NERC or the regional entity whenever any significant combination of specificity, clarity, or time is of the essence to address a threat to the reliability of the bulk power system brought on by lack of or inadequate compliance to the reliability standards.

6.2Compliance Requirements

In the United States, the Commission has concluded that owners, operators, or users of the bulk power system must comply with remedial action directives issued to them by NERC or a regional entity. Noncompliance with a remedial action directive may result in a substantially increased penalty or sanction.

Remedial action directives issued by NERC or the regional entity will include a deadline by which time the owner, operator, or user must complete requirements set out in the order, and by which time the entity must demonstrate compliance to the remedial action directive to NERC or the regional entity that issued it. Failure or refusal to meet the requirements or deadlines set out in a remedial action directive may itself result in further remedial action directives or significantly increased penalties or sanctions by NERC or the regional entity.

6.3No Obligation to Issue

NERC or the regional entity may, but is not obligated, to issue remedial action directives. Lack of being issued a remedial action directive does not relieve a bulk power system owner, operator, or user from any responsibilities they otherwise have to comply or maintain compliance with requirements of the reliability standards. Remedial action directives will be used by NERC or the regional entities only as they deem warranted, when they deem warranted.

6.4Scope of Application

The scope of remedial action directives issued by NERC or the regional entity will be limited to conditions, practices, or any other relevant actions or activities resulting in noncompliance, or that NERC or the regional entity considers at significant risk of becoming noncompliant, to requirements of the reliability standards, and that present an imminent threat to the reliability of the bulk power system. However, beyond merely directing compliance or improved compliance with standards' requirements, where NERC or the regional entity is authorized to do so, the directive may also stipulate how compliance or the improvement to compliance is to be achieved.

~~6.5Availability~~

~~In the United States, the Commission has interpreted the Federal Power Act to authorize the NERC or the regional entity can issue a remedial action directive prior to completion of the confirmation review of a probable violation, or prior to the determination of a penalty or sanction for that violation. The Commission also concluded it is not necessary for NERC or the regional entity to acquire the Commission's or other regulators' approval prior to issuing remedial action directives. Accordingly, NERC or the regional entity may issue remedial action directives to entities in the United States whenever they deem it necessary or otherwise warranted to do so. Also, NERC or the regional entity may issue remedial action directives to entities in the United States regarding a violation that is immediately necessary to terminate or correct to protect the reliability of the bulk power system from an imminent threat, irrespective of whether that violation is ultimately verified or dismissed by NERC or the regional entity's investigation of the violation.~~

~~6.6No Impact on Confirmation of Violation, or Penalties or Sanctions~~

~~Remedial action directives issued regarding a violation, in particular any costs incurred by the violator to comply with any such directive, will not be considered when reviewing whether the aggregate of any penalties and sanctions levied for that violation bear a reasonable relation to the seriousness of the violation. Also, any remedial action directives issued with respect to a violation will not influence the outcome of the confirmation review of that violation nor the determination of penalties or sanctions for that violation; ordering a violator to correct what needs correcting anyway is no grounds for dispelling a violation nor reducing or eliminating a penalty or sanction that would otherwise be determined appropriate for the violator for that violation.~~

~~6.7Types of Remedial Actions~~

~~NERC or the regional entities may issue remedial action directives to correct compliance with NERC or regional reliability standards and reduce or eliminate imminent threats to the reliability of the bulk power system. Examples of remedial actions include:~~

~~a.Specifying operating or planning criteria, limits, or limitations~~

~~b.Requiring specific system studies~~

~~c.Defining operating practices or guidelines~~

~~d.Requiring confirmation of data, practices, or procedures through inspection testing or other methods~~

~~e.Requiring specific training for personnel~~

~~f.Requiring development of specific operating plans~~

Appendix A: Base Penalty Amount Table

The following lists the Base Penalty amounts corresponding to combinations of ~~v~~Violation ~~r~~Risk ~~f~~Factor and ~~v~~Violation Ss~~s~~everity F~~f~~actor.

	Violation Severity Level							
Violation Risk Factor	**Lower**		**Moderate**		**High**		**Severe**	
	Range Limits		**Range Limits**		**Range Limits**		**Range Limits**	
	Low	**High**	**Low**	**High**	**Low**	**High**	**Low**	**High**
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

NOTE: This table describes the amount of penalty that could be applied for each day that a violation continues, subject to the considerations of Section 3.21 regarding frequency and duration of violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PROPOSED REVISIONS 11-7-2011

North American Electric Reliability Corporation

Compliance Monitoring and Enforcement Program

APPENDIX 4C TO THE RULES OF PROCEDURE

Effective: ~~October 7, 2011~~ , 2012

TABLE OF CONTENTS

1.0 **INTRODUCTION** **1**
1.1 Definitions **1**
2.0 **IDENTIFICATION OF ORGANIZATIONS RESPONSIBLE FOR COMPLYING WITH RELIABILITY STANDARDS** **5**
3.0 **COMPLIANCE MONITORING PROCESSES** **6**
3.1 Compliance Audits ..... **8~~7~~**
3.2 Self-Certification **14**
3.3 Spot Checking **15**
3.4 Compliance Investigations **17**
3.5 Self-Reporting **21**
3.6 Periodic Data Submittals ..... **22~~22~~~~21~~**
3.7 Exception Reporting ..... **23~~23~~~~22~~**
3.8 Complaints **23**
4.0 **ANNUAL IMPLEMENTATION PLANS** **25**
4.1 NERC Compliance Monitoring and Enforcement Program Implementation Plan **25**
4.2 Regional Entity Implementation Plan ..... **26~~26~~~~25~~**
5.0 ENFORCEMENT ACTIONS **26**
5.1 Preliminary Screen 22
5.2 Assessment of Possible Violations 23
5.3 Notification to Registered Entity of Alleged Violation **28**
5.4 Registered Entity Response ..... **30~~30~~~~29~~**
5.5 Hearing Process for Compliance Hearings ..... **31~~31~~~~30~~**
5.6 Settlement Process ..... **31~~31~~~~30~~**
5.7 NERC Appeal Process **32**
5.8 Approval of a Notice of Confirmed Violation 27
5.9 Notice of Penalty 27
5.10 Closure of Enforcement Action 28
6.0 MITIGATION OF VIOLATIONS OF RELIABILITY STANDARDS ..... **41~~34~~**
6.1 Requirement for Submission of Mitigation Plans ..... **41~~35~~~~34~~**
6.2 Contents of Mitigation Plans ..... **42~~35~~**
6.3 Timetable for Completion of Mitigation Plans 30
6.4 Submission of Mitigation Plans ..... **43~~37~~~~36~~**
6.5 Review and Acceptance or Rejection of Proposed Mitigation Plans ..... **44~~37~~**
6.6 Completion/Confirmation of Implementation of Mitigation Plans ..... **45~~39~~~~38~~**
6.7 Recordkeeping ..... **46~~39~~**
7.0 REMEDIAL ACTION DIRECTIVES ..... **46~~40~~~~39~~**
8.0 REPORTING AND DISCLOSURE ..... **48~~41~~**
9.0 DATA RETENTION AND CONFIDENTIALITY ..... **50~~43~~**
9.1 Records Management ..... 50~~43~~
9.2 Retention Requirements ..... **50~~43~~**
9.3 Confidentiality and Critical Energy Infrastructure Information ..... **50~~44~~~~43~~**

ATTACHMENT 1 – PROCESS FOR NON-SUBMITTAL OF REQUESTED DATA

ATTACHMENT 2 – COMPLIANCE ENFORCEMENT AUTHORITY HEARING PROCEDURE

COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM

1.0 INTRODUCTION

This Compliance Monitoring and Enforcement Program ("Compliance Program") is the program to be used by the North American Electric Reliability Corporation ("NERC") and the Regional Entities to monitor, assess, and enforce compliance with Reliability Standards within the United States. Compliance monitoring and enforcement programs also will be implemented in Canada consistent with Canadian laws and agreements.

1.1 Definitions

Capitalized terms used in this Compliance Program shall have the meanings set forth in Section 200 and Section 1501 of the NERC Rules of Procedure or as set forth below:

1.1.1 Alleged Violation: A Possible Violation for which the Compliance Enforcement Authority has determined, based on an assessment of the facts and circumstances surrounding the Possible Violation, that evidence exists to indicate a Registered Entity has violated a Reliability Standard.

1.1.2 Annual Audit Plan: A plan developed annually by the Compliance Enforcement Authority that includes the Reliability Standards and Registered Entities to be audited, and the schedule of Compliance Audits, and Compliance Audit Participant requirements for the calendar year.

1.1.3 Applicable Governmental Authority: The Federal Energy Regulatory Commission ("FERC") within the United States and the appropriate governmental authority with subject matter jurisdiction over reliability in Canada and Mexico.

1.1.4 Complaint: An allegation that a Registered Entity violated a Reliability Standard.

1.1.5 Compliance Audit: A systematic, objective review and examination of records and activities to determine whether a Registered Entity meets the requirements of applicable Reliability Standards.

1.1.6 Compliance Audit Participants: Registered Entities scheduled to be audited and the audit team members.

1.1.7 Compliance Enforcement Authority: NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.1.8 Compliance Investigation: A comprehensive investigation, which may include an on-site visit with interviews of the appropriate personnel, to determine if a violation of a Reliability Standard has occurred.

1.1.9 Confirmed Violation: An Alleged Violation for which (1) ~~an~~the Registered ~~e~~Entity has~~: (1)~~ accepted the Notice of Alleged Violation and Proposed Penalty or Sanction or other notification of the Alleged Violation~~finding of the violation by a Regional Entity or NERC and will not seek an appeal~~, or (2) there has been the issuance of a final order finding a violation, penalty or sanction~~completed the hearing and appeals process within NERC,~~ or (3) ~~allowed~~ the period~~time~~ for requesting a hearing or ~~submitting~~ an appeal has ~~to~~ expired and the Registered Entity has not contested the Alleged Violation or penalty in any filing with the Compliance Enforcement Authority, or (4) the Registered Entity has entered into a settlement agreement, regardless of whether or not the Registered Entity has admitted or contested~~to~~ the Alleged ~~v~~Violation ~~in a settlement agreement~~.

1.1.10 End Date: The last date of the period to be covered in a Compliance Audit.

1.1.11 Exception Report~~ing~~: Information provided to the Compliance Enforcement Authority by a Registered Entity indicating that a violation of a Reliability Standard has occurred (e.g., a system operating limit has been exceeded) or enabling the Compliance Enforcement Authority to ascertain the Registered Entity's compliance.

1.1.12 ISO/RTO: A FERC-approved independent system operator or regional transmission organization with exclusive and independent authority under section 205 of the Federal Power Act (16 U.S.C. 824d) to propose rates, terms and conditions of transmission service provided over the facilities it operates.

1.1.1~~2~~3 Mitigation Plan: An action plan~~, required when a Registered Entity violates a Reliability Standard as determined by any means including Compliance Enforcement Authority decision, settlement agreement, or otherwise, that is~~ developed by the Registered Entity to (1) correct a violation of a Reliability Standard and (2) prevent re-occurrence of the violation.

1.1.1~~3~~4 NERC Compliance Registry: A list, maintained by NERC pursuant to Section 500 of the NERC Rules of Procedure and Appendix 5B, the NERC *Statement of Compliance Registry Criteria*, of the owners, operators and users of the Bulk Power System, and the entities registered as their designees, that perform one or more functions in support of reliability of the Bulk Power System and are required to comply with one or more requirements of Reliability Standards.

1.1.1~~4~~5 NERC Compliance Monitoring and Enforcement Program Implementation Plan or NERC Implementation Plan: The annual NERC Compliance Monitoring and Enforcement Program

Implementation Plan that specifies the Reliability Standards that are subject to reporting by Registered Entities to the Compliance Enforcement Authority in order to verify compliance and identifies the appropriate monitoring procedures and reporting schedules for each such Reliability Standard.

1.1.1~~5~~6 Notice of Alleged Violation and Proposed Penalty or Sanction: A notice issued by the Compliance Enforcement Authority to a Registered Entity pursuant to Section 5.3.

1.1.1~~6~~7 Notice of Completion of Enforcement Action: A notice issued by the Compliance Enforcement Authority to a Registered Entity, pursuant to Section 5.10, stating than an enforcement action is closed.

1.1.1~~7~~8 Notice of Confirmed Violation: A notice issued by the Compliance Enforcement Authority to a Registered Entity confirming the violation of one or more Reliability Standards~~, as a result of (1) the Registered Entity accepting a Notice of Alleged Violation and the proposed penalty or sanction, or (2) the finding of a violation through a hearing and appeal, or (3) the expiration of the period for requesting a hearing or an appeal, or (4) the Registered Entity admitting the violation as part of an executed settlement agreement~~.

1.1.1~~8~~9 Notice of Penalty: A notice prepared by NERC and filed with FERC, following approval by NERC of a Notice or other notification of Confirmed Violation or a settlement agreement, stating the penalty or sanction imposed or agreed to for the Confirmed Violation or as part of the settlement.

1.1.~~19~~20 Notice of Possible Violation: A notice issued by the Compliance Enforcement Authority to a Registered Entity that (1) states a Possible Violation has been identified, (2) provides a brief description of the Possible Violation, including the Reliability Standard requirement(s) and the date(s) involved, and (3) instructs the Registered Entity to retain and preserve all data and records relating to the Possible Violation.

1.1.2~~0~~1 Periodic Data Submittals: Modeling, studies, analyses, documents, procedures, methodologies, operating data, process information or other information to demonstrate compliance with Reliability Standards and provided by Registered Entities to the Compliance Enforcement Authority on a time frame required by a Reliability Standard or an ad hoc basis.

1.1.2~~1~~2 Possible Violation: The identification, by the Compliance Enforcement Authority, ~~using one of the Compliance Monitoring and Enforcement Processes in Section 3.0,~~ of a possible failure by a

Registered Entity to comply with a Reliability Standard that is applicable to the Registered Entity.

1.1.2~~2~~3 Preliminary Screen: An initial evaluation of evidence indicating potential noncompliance with a Reliability Standard has occurred or is occurring, conducted by the Compliance Enforcement Authority for the purpose of determining whether a Possible Violation exists, and consisting of an evaluation of whether (1) the entity allegedly involved in the potential noncompliance is registered, ~~and~~ (2) the Reliability Standard requirement to which the evidence of potential noncompliance relates is applicable to a reliability function for which the entity is registered, and (3) if known, the potential noncompliance is not a duplicate of a Possible Violation or Alleged Violation which is currently being processed.

1.1.24 Public Notification List: A list posted on the NERC website, pursuant to Section 5.11 of this Appendix, of the names of Registered Entities that an ISO/RTO contends it has authority to allocate to, pursuant to a proceeding under section 205 of the Federal Power Act, some or all of a monetary penalty imposed on the ISO/RTO for a violation of a Reliability Standard.

1.1.2~~3~~5 Regional Implementation Plan: An annual plan, submitted ~~by~~on or about October ~~November~~ 1 of each year to NERC for approval that, in accordance with NERC Rule of Procedure Section 401.6 and the NERC Compliance Monitoring and Enforcement Program Implementation Plan, identifies (1) all Reliability Standards identified by NERC to be actively monitored during each year, (2) other Reliability Standards proposed for active monitoring by the Regional Entity, (3) the methods to be used by the Regional Entity for reporting, monitoring, evaluation, and assessment of performance criteria with each Reliability Standard, and (4) the Regional Entity's Annual Audit Plan.

1.1.2~~4~~6 Registered Entity: An owner, operator, or user of the Bulk Power System, or the entity registered as its designee for the purpose of compliance, that is included in the NERC Compliance Registry.

1.1.2~~5~~7 Remedial Action Directive: An action (other than a penalty or sanction) required by a Compliance Enforcement Authority that (1) is to bring a Registered Entity into compliance with a Reliability Standard or to avoid a Reliability Standard violation, and (2) is immediately necessary to protect the reliability of the Bulk Power System from an imminent or actual threat.

1.1.2~~6~~8 Required Date: The date given a Registered Entity in a notice from the Compliance Enforcement Authority by which some action by the Registered Entity is required.

1.1.2~~7~~9 Self-Certification: An attestation by a Registered Entity that it is compliant or non-compliant~~of compliance or non-compliance~~ with a Reliability Standard requirement that is the subject of the Self-Certification, or that it does not own facilities that are subject to the Reliability Standard requirement, or that the Reliability Standard requirement is not applicable to the Registered Entity ~~for which Self-Certification is required by the Compliance Enforcement Authority and that is included for monitoring in the Regional Implementation Plan~~.

1.1.2~~8~~30 Self-Report~~ing~~: A report by a Registered Entity stating ~~(1)~~ that the Registered Entity believes it has, or may have, violated a Reliability Standard~~, and (2) the actions that have been taken or will be taken to resolve the violation~~.

1.1.~~29~~31 Spot Check~~ing~~: A process in which the Compliance Enforcement Authority requests a Registered Entity to provide information (1) to support the Registered Entity's Self-Certification, Self-Report~~ing~~, or Periodic Data Submittal and to assess whether the Registered Entity complies with Reliability Standards, or (2) as a random check, or (3) in response to ~~events, as described in the Reliability Standards or based on~~ operating problems, ~~or~~ system events, or risk-based assessments.

2.0 IDENTIFICATION OF ORGANIZATIONS RESPONSIBLE FOR COMPLYING WITH RELIABILITY STANDARDS

NERC shall register the organizations responsible for complying with Reliability Standards, in accordance with Section 500 of the NERC Rules of Procedure and Appendix 5B, *Statement of Compliance Registry Criteria*. Organizations are responsible to register and to comply with Reliability Standards if they are owners, operators, and users of the Bulk Power System, perform a function listed in the functional types identified in Section II of Appendix 5B, and are material to the reliable operation of the Bulk Power System as defined by the criteria and notes in Appendix 5B. Regional Entities shall (i) develop and provide to NERC information to assist NERC to register organizations responsible for complying with Reliability Standards, and (ii) in the event of a registration appeal to NERC or an Applicable Governmental Authority, provide information requested by NERC concerning how the Registered Entity meets the registration criteria or is otherwise material to the reliability of the Bulk Power System.

NERC shall notify organizations of their inclusion on the NERC Compliance Registry and shall maintain the NERC Compliance Registry on its web site. NERC shall inform each Registered Entity at the time of registration of the Reliability Standards that are applicable to reliability functions for which the Registered Entity is registered. Each Registered Entity shall inform NERC or the applicable Regional Entity promptly of changes to the Registered Entity's registration information including planned or completed changes in ownership of Bulk Power System facilities, registration status, address and other contact information, and name of designated compliance contact. NERC will provide FERC and Applicable Governmental Authorities monthly updates to the NERC Compliance Registry.

NERC and each Regional Entity will designate a contact person(s) and require each Registered Entity to designate a contact person(s) responsible for sending and receiving all necessary information and communications concerning compliance matters. NERC and the applicable Regional Entity will designate where Registered Entities are to send information, data, Mitigation Plans, or any other compliance-related correspondence.

NERC shall maintain on its website a current listing of Reliability Standards that are applicable to all Registered Entities.

As provided for herein, during the course of compliance monitoring and enforcement activities relating to U.S. entities, NERC may obtain information that it will provide to FERC and, if the information pertains to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, to such other Applicable Governmental Authority. Any such provision of information to FERC or to another Applicable Governmental Authority shall be in accordance with Section 8.0, Reporting and Disclosure. ~~However, NERC will not provide non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosures and subject to such limitations as FERC may place on such disclosures. Similarly, during the course of compliance monitoring and enforcement activities relating to non-U.S. entities, NERC may obtain information that it will provide to the Applicable Governmental Authorities, including FERC, that have jurisdiction over the Registered Entity or the portion of the Bulk Power System to which the information pertains, but subject to any limitations placed on the disclosure of non-public, non-U.S. compliance information by the Applicable Governmental Authority with jurisdiction or by other law of the applicable jurisdiction. In any notice to, and request for permission to disclose compliance information from, FERC or another Applicable Governmental Authority pursuant to any provision of this Compliance Program, NERC will identify each Applicable Governmental Authority to which it proposes to disclose the information and the specific procedures that will be used for protecting from public disclosure any non-public compliance information that will be transferred to the other Applicable Governmental Authority or Authorities. The provisions of this paragraph do not apply to the provision by NERC to an Applicable Governmental Authority of information that is not directly related to a specific Registered Entity's compliance with a requirement of a Reliability Standard.~~

3.0 COMPLIANCE MONITORING ~~AND ENFORCEMENT~~ PROCESSES

The Compliance Enforcement Authority will monitor~~, assess, and enforce~~ Registered Entities' compliance with Reliability Standards using the compliance monitoring processes described in this Section ~~3.0 to collect information in order to make assessments of compliance. These processes are described in Sections 3.1 through 3.8 below~~. Scheduled compliance monitoring processes, such as Compliance Audits, will be conducted in accordance with applicable NERC Annual Implementation Plans and Regional Annual Implementation Plans, and individual entity audit plans. Compliance monitoring processes can also be initiated on an unscheduled basis as needed, in the judgment of NERC or the Compliance Enforcement Authority, based on Bulk Power System occurrences such as major events, disturbances, and trends. Factors that will be considered in determining whether a compliance monitoring process should be initiated on an unscheduled basis, and the type of compliance monitoring process to be initiated, include, but are not limited to, the significance of the occurrence to the reliability of the Bulk Power System, the

compliance record of the Registered Entity for which the compliance monitoring process would be initiated, and the quality of the Registered Entity's internal reliability compliance program.

If a compliance monitoring process described in this Section reveals a potential noncompliance with a Reliability Standard, the Compliance Enforcement Authority will conduct a Preliminary Screen of the potential noncompliance in accordance with Section 3.8. In addition, if the Compliance Enforcement Authority obtains evidence or information of a potential noncompliance with a Reliability Standard through any other means, including but not limited to an Exception Report or other report of noncompliance that a Registered Entity is required to submit in accordance with the terms of a Reliability Standard, the Compliance Enforcement Authority will conduct a Preliminary Screen of the information in accordance with Section 3.8. If the Preliminary Screen results in an affirmative determination with respect to the Preliminary Screen criteria, a Possible Violation exists and the Compliance Enforcement Authority will proceed in accordance with Section 5.0, Enforcement Actions.

~~Enforcement actions taken by the Compliance Enforcement Authority through the Compliance Program may include the imposition of remedial actions, sanctions, and penalties, where applicable, which shall be based on the schedule of penalties and sanctions approved for implementation by FERC and other Applicable Governmental Authorities. The imposition and acceptance of sanctions and penalties shall not be considered an acceptable alternative to any Registered Entity's continuing obligation to comply with the Reliability Standards.~~ Registered Entities found in violation of a Reliability Standard will be required to mitigate the violation regardless of any enforcement actions taken.

The ~~C~~compliance monitoring processes in this Section ~~Program~~ require~~s~~ timely information, reports and data from Registered Entities to effectively monitor compliance with Reliability Standards. The Compliance Enforcement Authority has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security procedures conforming to Section 1500 of the Rules of Procedure and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost of the information were placed into the public domain. If documents, data, information or other reports to determine compliance requested from a Registered Entity are not received by the Required Date, the Compliance Enforcement Authority may execute the steps described in **Attachment 1, Process for Non-submittal of Requested Data.**

Parties engaged in the process described in this section should consult with each other on the data and information that would be appropriate for effectively addressing this section's process requirements. If a ~~party~~Registered Entity believes that a request for documents, data or information is unreasonable, the ~~party~~Registered Entity may request a written determination from the NERC General Counsel~~compliance program officer~~.

Any report or other submission of information by a Registered Entity required by the Compliance Program shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity. Electronic signatures are permitted in accordance with

processes established by NERC and the Regional Entity. NERC or the Compliance Enforcement Authority may require the signer to provide a statement of the basis of his or her authority to sign on behalf of the Registered Entity.

3.1 Compliance Audits

All Registered Entities are subject to audit for compliance with all Reliability Standards applicable to the functions for which the Registered Entity is registered. Compliance Audits are conducted on the Registered Entity's site to the extent required by NERC Rule of Procedure 403.11.2. Compliance Audit processes for Compliance Audits conducted in the United States shall be based on professional auditing standards recognized in the U.S., which may include, for example~~including~~ Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards and standards sanctioned by the Institute of Internal Auditors. Compliance Audit processes for Compliance Audits conducted outside the U.S. may be based on Canadian or other international standards. All Compliance Audits shall be conducted in accordance with audit guides established for the Reliability Standards included in the Compliance Audit, consistent with accepted auditing guidelines as approved by NERC. The audit guides will be posted on NERC's website.

3.1.1 Compliance Audit Process Steps

The process steps for a Compliance Audit are as follows:[1]

- The Compliance Enforcement Authority posts~~distributes~~ the Annual Audit Plan (developed in coordination with NERC) ~~to the Compliance Audit Participants and NERC~~. The Compliance Enforcement Authority provides additional information to the Compliance Audit Participants, including audit materials, coordinating agendas and changes to the audit schedule as required. ~~Prior to the Compliance Audit, the Compliance Enforcement Authority informs the Registered Entity of the Reliability Standards to be evaluated.~~ NERC or the Regional Entity provides the audit schedules to FERC and to any other Applicable Governmental Authority based upon the agreements in place with the other Applicable Governmental Authority.

- At least ~~two (2) months~~ninety (90) days prior to commencement of a regularly scheduled Compliance Audit, the Compliance Enforcement Authority notifies the Registered Entity of the Compliance Audit and the Reliability Standards to be evaluated, identifies the audit team members and their recent employment history, and requests data, including a completed NERC pre-audit questionnaire. If the audit team members change from the time of the original notification, the Compliance Enforcement Authority will promptly notify the Registered Entity of the change and will allow time for the Registered Entity to object to the new audit team member(s) (see Section 3.1.5.4).

- The Registered Entity provides to the Compliance Enforcement Authority the required information in the format and by the Required Date specified in the request.

[1] ~~This process normally completes within sixty (60) days of the completion of the on-site Compliance Audit work at the Registered Entity's site.~~

- The audit team reviews the submitted information for conformance with the requirements of the Reliability Standards~~ prior to performing the Compliance Audit. The audit team follows NERC audit guidelines in the implementation of the Compliance Audit~~.

- The~~is~~ audit team~~shall include~~ conduct~~sing~~ an exit briefing with the Registered Entity, provide~~sing~~ for a review of the audit report with the Registered Entity before it is finalized, and completes~~issuing~~ an audit report in accordance with Section 3.1.6~~, including an assessment of compliance with the Reliability Standards, to the Compliance Enforcement Authority~~.

- If the audit team identifies evidence of a potential noncompliance with a Reliability Standard requirement by the Registered Entity, the Compliance Enforcement Authority conducts a Preliminary Screen of the potential noncompliance in accordance with Section 3.8.

- ~~The Compliance Enforcement Authority reviews the report developed by the audit team and completes a Preliminary Screen for any Possible Violations of Reliability Standards, based on the potential noncompliances with Reliability Standards (if any) identified in the report.~~

- ~~If the Compliance Enforcement Authority concludes that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation.~~

- ~~The Compliance Enforcement Authority provides the final audit report to the Registered Entity and to NERC.~~

3.1.2 Compliance Enforcement Authority Annual Audit Plan and Schedule

The Compliance Enforcement Authority shall develop an Annual Audit Plan. The Annual Audit Plan of Regional Entities will be included in the Regional Implementation Plans submitted to NERC for review and approval (see Section 4.2). NERC or the Regional Entity provides the Annual Audit Plans to FERC and to any other Applicable Governmental Authority consistent with the agreements in place with the Applicable Governmental Authority.

Prior to ~~January~~October 1 of the year preceding the year covered by the Annual Audit Plan, the Compliance Enforcement Authority shall notify Registered Entities subject to Compliance Audits during the upcoming year~~,~~ of the audit schedule~~s, methods, and data requirements for the audit~~. The Compliance Enforcement Authority will give due consideration to any schedule changes requested by Registered Entities for reasonable cause~~to avoid unnecessary burdens~~.

Revisions and additions to a Regional Entity Annual Audit Plan shall be communicated to and approved by NERC, and shall be communicated to the Registered Entity~~ shall be notified~~ in a timely manner (normally sixty (60) days in advance) of changes or revisions to scheduled audit dates.

3.1.3 Frequency of Compliance Audits

The Compliance Enforcement Authority will perform comprehensive Compliance Audits as required by the NERC Rules of Procedure and based on criteria established by NERC. In addition to scheduled Compliance Audits, the Compliance Enforcement Authority ~~Additionally, (i) may initiate~~ an unscheduled Compliance Audit of any Registered Entity ~~(i) may be initiated~~ at any time ~~by the Compliance Enforcement Authority~~ if the Compliance Enforcement Authority reasonably determine~~d~~s it to be necessary to ensure the Registered Entity's compliance with Reliability Standards, and (ii) shall ~~be~~ initiate~~d by the~~ an unscheduled Compliance Audit ~~Enforcement Authority or by NERC~~ if directed by FERC. The Compliance Enforcement Authority shall notify NERC and FERC ~~P~~prior to or on the same date it notifies the Registered Entity that an unscheduled Compliance Audit is being initiated~~, the Compliance Enforcement Authority shall notify NERC and FERC that an unscheduled Compliance Audit is being initiated~~. If NERC initiates the unscheduled Compliance Audit, it shall notify the appropriate Regional Entity or Entities. The ~~Registered Entity~~Compliance Enforcement Authority shall provide~~receive~~ at least ten (10) business days advance notice to the Registered Entity that an unscheduled Compliance Audit is being initiated, which notice shall include identification of the members of the Compliance Audit team. ~~The Registered Entity shall make any objections to the composition of the Compliance Audit team, which shall be based on failure to meet the criteria specified in Section 3.1.5.2, at least five (5) business days prior to the start of on-site audit work for the unscheduled Compliance Audit.~~

3.1.4 Scope of Compliance Audits

3.1.4.1 Reliability Standards

A Compliance Audit shall include those Reliability Standards applicable to the Registered Entity that are identified in the NERC Implementation Plan for the current year, and may include other Reliability Standards applicable to the Registered Entity whether or not they~~that~~ are identified in the Regional Entity's Regional Implementation Plan for the current year. ~~The Compliance Audit may include any other Reliability Standards that are applicable to the Registered Entity.~~

3.1.4.2 Period Covered

The Registered Entity's data and information ~~should~~must show compliance with the Reliability Standards that are the subject of the Compliance Audit for the entire period covered by the Compliance Audit. The Compliance Enforcement Authority will indicate the beginning and End Date of the audit period in its notice of the Compliance Audit. The audit period begin~~sning with~~ the day after the End Date of the prior Compliance ~~a~~Audit by the Compliance Enforcement Authority ~~ended~~ (or the later of June 18, 2007 or the date the Registered Entity~~'s date of registration~~ became subject to compliance with the Reliability Standards if the Registered Entity has not previously been subject to a Compliance Audit)~~, and ending with the End Date for the Compliance Audit. However, if another Compliance Monitoring and Enforcement process has been conducted with respect to the Registered Entity subsequent to the date that would otherwise be the start of the period, the period covered by the Compliance Audit may, in the Regional Entity's discretion, begin with the completion of that Compliance Monitoring and Enforcement process for those Reliability Standards requirements that were the subject of the Compliance Monitoring and Enforcement process~~. The Compliance Enforcement Authority may modify the beginning date of the audit period for any given Reliability Standard requirement based on an intervening compliance monitoring process. The End Date may be a predetermined specific date

or may be stated generally as the last day ~~will be stated in the Compliance Enforcement Authority's notification~~ of the Compliance Audit ~~issued to the Registered Entity pursuant to Section 3.1.1~~.

The Registered Entity will be expected to demonstrate compliance for the entire period described above. ~~However, i~~If a Reliability Standard specifies a document retention period that does not cover the entire period described above, the Registered Entity will not be found in noncompliance solely on the basis of the lack of specific information that has rightfully not been retained based on the retention period specified in the Reliability Standard. However, in such cases, the Compliance Enforcement Authority will require the Registered Entity to demonstrate compliance through other means.

3.1.4.3 Review of Mitigation~~on~~ Activities ~~Plans~~

The Compliance Audit ~~will~~may include a review of any mitigating activities~~Mitigation Plans~~ which the Registered Entity has not yet completed, for the purpose of determining whether the Registered Entity is making adequate progress towards completion of the mitigating activities~~Mitigation Plan~~.

3.1.5 Conduct of Compliance Audits

3.1.5.1 Composition of Compliance Audit Teams

The audit team shall be comprised of ~~staff from~~members whom the Compliance Enforcement Authority has determined have the requisite knowledge, training and skills to conduct the Compliance Audit. ~~and such other persons as are included in the audit team pursuant to Section 3.1.5.3, and~~ The Compliance Audit team may include (i) contractors and industry subject matter experts ~~as determined by the Compliance Enforcement Authority to be appropriate to comprise a sufficient audit team~~, (ii) NERC staff members (which may include contractors to NERC), (iii) compliance staff members of other Regional Entities, and (iv) representatives of FERC and other Applicable Governmental Authorities so long as the Registered Entity is subject to the Applicable Governmental Authority's reliability jurisdiction. The audit team leader shall be a staff member from the Compliance Enforcement Authority and is responsible for the conduct of the Compliance Audit and preparation of the audit report.

3.1.5.2 Requirements for Compliance Audit Team Members

Each audit team member must:

- Be free of conflicts of interests in accordance with Compliance Enforcement Authority policies. ~~For example, e~~Employees or contractors of the Registered Entity being audited shall not be allowed to participate as auditors in the Compliance Audit of the Registered Entity.

- Comply with the NERC Antitrust Compliance Guidelines and shall have either signed appropriate confidentiality agreements or acknowledgments that the confidentiality agreement signed by the Compliance Enforcement Authority is applicable.

- Successfully complete all NERC or NERC-approved Regional Entity auditor training applicable to the Compliance Audit.

- Prior to the Compliance Audit, the Compliance Enforcement Authority shall provide confirmation to the Registered Entity that all audit team members have~~Provide copies of~~ executed confidentiality agreements or acknowledgements~~ to be provided to the Registered Entity prior to the audit~~.

3.1.5.3 Compliance Audit Observers ~~or~~and Other Attendees~~Participants~~

In any Regional Entity Compliance Audit of a Registered Entity, in addition to the audit team members, the following may participate as observers: (i) NERC Staff (which may include contractors to NERC)~~ may participate either as observers or as audit team members~~; (ii) other members of the Regional Entity's Compliance ~~s~~Staff~~, in addition to the audit team, may participate as observers~~; (iii) with the permission of the Regional Entity, compliance staff members of other Regional Entities~~ may participate either as observers or as audit team members~~; and (iv) representatives of FERC and of other Applicable Governmental Authorities ~~may participate either as observers or as audit team members~~ so long as the Registered Entity is subject to the Applicable Governmental Authority's reliability jurisdiction.

In addition, at the request of the Registered Entity being audited, the Regional Entity may allow attendance at the Compliance Audit by: (1) representatives of corporate affiliates of the Registered Entity being audited that are Registered Entities or that provide compliance services, support or oversight to the Registered Entity being audited, and (2) representatives of Registered Entities whose compliance activities are conducted by the Registered Entity being audited or by the same corporate entity that conducts the compliance activities of the Registered Entity being audited (e.g., representatives of other members of a Joint Registration Organization or of participants in a Coordinated Functional Registration pursuant to Section 500 of the Rules of Procedure). Each such additional attendee must execute a confidentiality agreement approved by the Regional Entity.

Compliance audit observers and attendees are not audit team members and do not participate in conducting the Compliance Audit or in making audit findings and determinations.

The Compliance Audit team leader or other staff of the Regional Entity conducting the Compliance Audit will communicate in advance with any observers or other attendees to ensure there are no undue disruptions to the audit, such as space limitations, no conflicts of interest, and no other considerations that in the judgment of the Compliance Audit team leader may be detrimental to the conduct and quality of the audit. If the Compliance Audit team leader identifies any such issues, he/she shall work with the proposed observers or attendees to facilitate observation in a less disruptive manner; or, alternatively, the Regional Entity Compliance staff will work with the proposed observers or attendees to schedule their participation in, observation of, or attendance at a different Compliance Audit in which such issues are not presented.

3.1.5.4 Registered Entity Objections to Compliance Audit Team

A Registered Entity subject to a Compliance Audit may object to any member of the audit team on grounds of a conflict of interest or the existence of other circumstances that could interfere with the team member's impartial performance of his or her duties. Any such objections must be provided in writing to the Compliance Enforcement Authority no later than fifteen (15) days prior to the start of on-site audit work. This fifteen (15) day requirement shall not apply ~~(i)~~ where an audit team member has been appointed less than twenty (20) days prior to the start of on-site audit work, in which case the Registered Entity must provide any objections to the Compliance Enforcement Authority within five (5) business days after receiving notice of the appointment of the Compliance Audit team member.~~; and (ii)~~

~~i~~In the case of an unscheduled Compliance Audit pursuant to Section 3.1.3, ~~in which case~~ the Registered Entity must provide any objections to the Compliance Enforcement Authority at least five (5) business days prior to the start of on-site audit work for the unscheduled Compliance Audit.

The Compliance Enforcement Authority will make a final determination on whether the member will participate in the Compliance Audit of the Registered Entity. Nothing in Section 3.1 shall be read to limit the participation of NERC staff in the Compliance Audit or to limit the participation of FERC staff in a Compliance Audit of a Registered Entity, or involving a portion of the Bulk Power System, over which FERC has jurisdiction.

3.1.6 Compliance Audit Reports

The audit team shall develop a draft audit report that shall include a description of the objective, scope, and methodology of the Compliance Audit; identify any evidence~~-~~ of potential~~possible~~ noncompliance with Reliability Standards by the Registered Entity found by the audit team; identify any ~~Mitigation Plans or~~ Remedial Action Directives, Mitigation Plans or other mitigating activities which have been completed or pending in the year of the Compliance Audit; and identify if~~the nature of~~ any C~~c~~onfidential I~~i~~nformation has been redacted. The report may also state areas of concern and recommendations identified by the audit team. ~~A separate document may be prepared that contains recommendations of the audit team. Any recommendations contained in that document will be considered non-binding.~~ The draft report will be provided to the Registered Entity for comment.

The audit team ~~will~~ considers corrections based on comments of the Registered Entity, ~~and provide the~~ finalizes the audit report, ~~to the Compliance Enforcement Authority who will review the report and assess compliance with the Reliability Standards~~ and provides the Registered Entity with a copy of the final report on or before the date the final report is provided to NERC. The Compliance Enforcement Authority~~Regional Entities will~~ provides the final report to NERC, which ~~will~~ in turn provides the report to FERC ~~-~~if the report pertains to a Registered Entity or to a portion of the Bulk Power System over which FERC has jurisdiction and/or to another Applicable Governmental Authority if the report pertains to a Registered Entity or to a portion of the Bulk Power System over which the other Applicable Governmental Authority has jurisdiction. The provision of the final report to FERC or to another Applicable Governmental Authority shall be in accordance with Section 8.0, Reporting and Disclosure.~~ Provided, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining

~~permission from FERC for such disclosure and subject to such limitations as FERC may place on such disclosure; and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission for such disclosure from the Applicable Governmental Authority with jurisdiction over the Registered Entity or the portion of the Bulk Power System to which such non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction. The Registered Entity shall receive the final audit report at least five (5) business days prior to the release of the report to the public.~~ Work papers and other documentation associated with the audit shall be maintained by the Compliance Enforcement Authority in accordance with NERC or Regional Entity requirements.

NERC will not publicly post the final audit report for at least five (5) business days following receipt. If~~In the event~~ the audit report identifies any Possible Violations of one or more Reliability Standards, the final audit report, or pertinent part thereof identifying the Possible Violations, shall not be released to the public by NERC~~ or the Compliance Enforcement Authority~~ until (i) the Possible Violation is dismissed prior to becoming a Confirmed Violation, or (ii) NERC submits a Notice of Penalty to FERC or other Applicable Governmental Authority~~,~~ or (iii) the Registered Entity executes~~admits to a violation or enters into~~ a settlement agreement with the Compliance Enforcement Authority pursuant to Section 5.6.

Information deemed by a Compliance Enforcement Authority or the Registered Entity as ~~e~~Critical ~~e~~Energy ~~i~~Infrastructure ~~i~~Information or ~~e~~Confidential ~~i~~Information~~ (as defined in Section 1501 of the NERC Rules of Procedure)~~ shall be redacted from any public reports.

3.2 Self-Certifications

The Compliance Enforcement Authority may require Registered Entities to self-certify their compliance with Reliability Standards.

~~If a Self-Certification accurately identifies a violation of a Reliability Standard, an identification of the same violation in a subsequent Compliance Audit or Spot Check will not subject the Registered Entity to an escalated penalty as a result of the Compliance Audit process unless the severity of the violation is found to be greater than reported by the Registered Entity in the Self-Certification.~~

3.2.1 Self-Certification Process Steps

The process steps for the Self-Certification process are as follows:[2]

- The Compliance Enforcement Authority posts and updates the reporting schedule containing the applicable reporting periods and informs Registered Entities. The Compliance Enforcement Authority and NERC will ensure~~s~~ that the appropriate Reliability Standards, compliance procedures, and required submittal forms for the Reliability Standards being evaluated are maintained and available~~ electronically~~.

[2] ~~If no Possible Violations are found, this process normally completes within sixty (60) days of the Compliance Enforcement Authority's receipt of data.~~

- The Compliance Enforcement Authority requests the Registered Entity to make a Self-Certification within the advance notice period specified by the Reliability Standard. If the Reliability Standard does not specify the advance notice period, this request will be issued in a timely manner (normally thirty (30) days advance notice).

- The Registered Entity provides the required information to the Compliance Enforcement Authority in the form and manner, and by the Required Date, specified by the Compliance Enforcement Authority. The Self-Certification response may state that (i) the Registered Entity is in compliance with the Reliability Standard requirement, (ii) the Registered Entity is not in compliance with the Reliability Standard requirement, (iii) the Registered Entity does not own facilities that are subject to the Reliability Standard requirement, or (iv) the Reliability Standard requirement is not applicable to the Registered Entity.

- At a minimum, ~~T~~the Compliance Enforcement Authority reviews Self-Certifications of noncompliance and Self-Certifications in which the Registered Entity has responded that it does not own facilities that are subject to the Reliability Standard requirement or that the Reliability Standard Requirement is not applicable to the Registered Entity,~~information to determine compliance with the Reliability Standards~~ and the Compliance Enforcement Authority may request additional data and/or information if necessary.

- ~~The Compliance Enforcement Authority completes the assessment of the Registered Entity for compliance with the Reliability Standard (and with the Registered Entity's Mitigation Plan, if applicable). If the Compliance Enforcement Authority concludes, after completing a Preliminary Screen(s), that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation.~~If the Compliance Enforcement Authority's review of the Self-Certification indicates a potential noncompliance with a Reliability Standard by the Registered Entity, the Compliance Enforcement Authority conducts a Preliminary Screen of the potential noncompliance in accordance with Section 3.8.

Receipt of a Self-Certification by the Compliance Enforcement Authority shall not be construed as a finding by the Compliance Enforcement Authority that the Registered Entity is compliant with, not compliant with, or not subject to, the Reliability Standard requirement.

3.3 Spot Check~~sing~~

Spot Check~~sing~~ will be conducted by the Compliance Enforcement Authority. Spot Check~~sing~~ may be initiated at the discretion of ~~by~~ the Compliance Enforcement Authority or as directed by NERC, ~~at any time to verify or confirm Self-Certifications, Self-Reporting, and Periodic Data Submittals. Spot Checking may also be random or may be initiated in response~~for reasons including but not limited ~~to events, as described in the Reliability Standards, or~~ to operating problems, ~~or~~ system events, or risk-based assessments based on the Registered Entity's Bulk Power System facilities and operations and their significance to the reliability of the Bulk Power System and the Registered Entity's compliance history and internal compliance program or other indicators of its culture of compliance, or on a random schedule. ~~The Compliance Enforcement Authority then reviews the information submitted to verify the Registered Entity's compliance~~

~~with the Reliability Standard. Compliance auditors may be assigned to the Spot Checking process by the Compliance Enforcement Authority as necessary.~~

3.3.1 Spot Check~~ing~~ Process Steps

The process steps for Spot Check~~sing~~ are as follows~~:~~[3]

- The Compliance Enforcement Authority shall issue a notification letter to ~~notifies~~ the Registered Entity that a Spot Check~~ing~~ will be performed~~,~~ ~~and~~ the reason for the Spot Check~~ing~~, and the scope of the Spot Check including the Reliability Standard requirements that will be covered, in accordance with~~in~~ the advance notice period specified by the Reliability Standard. If the Reliability Standard requirement does not specify an advance notice period, any information submittal request made by the Compliance Enforcement Authority will allow at least twenty (20) days for the Registered Entity to submit the information or make it available for review.

- The Compliance Enforcement Authority, as part of the notification package,~~during the advance notice period, notifies~~ shall provide the Registered Entity with~~of~~ the names and employment histories of the persons who will be conducting the Spot Check~~ing~~. The Compliance Enforcement Authority shall provide confirmation to the Registered Entity that the members of the Spot Check team have executed confidentiality agreements or acknowledgements. The Registered Entity may object to inclusion of any individual on the Spot Check~~ing~~ team on the grounds specified in ~~accordance with~~ Section 3.1.5.4. Any such objections must be submitted to the Compliance Enforcement Authority by the later of (i) five (5) business days before the information ~~being~~ requested by the Compliance Enforcement Authority is submitted and (ii) five (5) business days after the Registered Entity is notified of the persons on the Spot Check~~ing~~ team. Nothing in Section 3.1~~this step~~ shall be read to limit the participation of NERC ~~or FERC~~ staff ~~on the~~in a Spot Check~~ing team~~ or to limit the participation of FERC staff in a Spot Check of a Registered Entity, or involving a portion of the Bulk Power System, over which FERC has jurisdiction.

- The Spot Check~~ing~~ may require submission of data, documentation, and information and ~~or possibly~~ an on-site review.

- The Registered Entity provides the required information to the Compliance Enforcement Authority in the format and by the date specified in the request.

- The ~~Compliance Enforcement Authority~~Spot Check team conducts a review~~s~~ of the information submitted to determine compliance with the Reliability Standard~~s~~ requirements and may request additional data and/or information if necessary ~~for a complete assessment of compliance~~.

- If the Spot Check team's review of the information submitted indicates a potential noncompliance with a Reliability Standard requirement by the Registered Entity, the

[3] ~~If no Possible Violations are found, this process normally completes within ninety (90) days of the Compliance Enforcement Authority's receipt of data.~~

Compliance Enforcement Authority conducts a Preliminary Screen pursuant to Section 3.8.

- The Spot Check team ~~Compliance Enforcement Authority~~ prepares a draft Spot Check report~~reviews its draft assessment of the Registered Entity's compliance with the Registered Entity~~ and provides the Registered Entity ten (10) business days ~~an opportunity for the Registered Entity~~ to comment on the draft ~~assessment~~report.

- The ~~Compliance Enforcement Authority~~Spot Check team considers any corrections based on the Registered Entity's comments, finalizes ~~completes and documents the assessment of the Registered Entity for compliance with the Reliability Standard and provides a~~the Spot Check report and provides it to the Registered Entity and to NERC ~~indicating the results of the Spot Checking~~.

- If the Compliance Enforcement Authority is a Regional Entity, the Regional Entity provides the final report to NERC. NERC provides the report to FERC if the report pertains to a Registered Entity or to a portion of the Bulk Power System over which FERC has jurisdiction and/or to another Applicable Governmental Authority if the report pertains to a Registered Entity or to a portion of the Bulk Power System over which the other Applicable Governmental Authority has jurisdiction. The provision of the report to FERC or to another Applicable Governmental Authority shall be in accordance with Section 8.0, Reporting and Disclosure.~~Provided, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosure and subject to such limitations as FERC may place on such disclosure; and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission for such disclosure from the Applicable Governmental Authority with jurisdiction over the Registered Entity or the portion of the Bulk Power System to which such non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.~~

- The report will not be publicly posted, or otherwise made publicly available, by the Regional Entity or by NERC.

~~If the Compliance Enforcement Authority concludes, after completing a Preliminary Screen(s), that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation.~~

3.4 Compliance Investigations

A Compliance Investigation may be initiated at any time by the Compliance Enforcement Authority or NERC in response to a system disturbance, Complaint, or any potential noncompliance with~~possible violation of~~ a Reliability Standard identified by any other means.

Compliance Investigations will generally be led by the Regional Entity's staff. NERC reserves the right to assume the leadership of a Compliance Investigation.[4] The Regional Entity shall not be entitled to appeal NERC's decision to lead a Compliance Investigation.

Compliance Investigations are confidential, unless FERC directs that a Compliance Investigation should be public or that certain information obtained in the Compliance Investigation should be publicly disclosed. Confirmed Violations resulting from a Compliance Investigation will be made public.

FERC or another Applicable Governmental Authority may initiate an investigation at any time in response to a system disturbance, Complaint, or potential noncompliance with~~possible violation of~~ a Reliability Standard identified by any other means, or for any other purpose authorized by law. Investigations initiated by FERC or another Applicable Governmental Authority shall be governed by and conducted pursuant to the statutory authority and rules of the Applicable Governmental Authority and not the procedures set forth herein. If an Applicable Governmental Authority other than FERC initiates an investigation of a U.S.-related matter, NERC shall provide notice to FERC of the investigation prior to disclosure of any non-public U.S.-related compliance information regarding the matter to be investigated to the other Applicable Governmental Authority. NERC's notice to FERC shall identify the other Applicable Governmental Authority, shall describe the nature of the proposed disclosures to the other Applicable Governmental Authority, and shall state the procedures NERC will utilize in connection with the Compliance Investigation to ensure compliance with the requirements of 18 C.F.R. §39.7(b)(4) concerning nondisclosure of violations and Alleged Violations.

If FERC initiates an investigation of a non-U.S.-related matter, NERC shall provide notice of the investigation to the Applicable Governmental Authority having jurisdiction over the Registered Entity or the portion of the Bulk Power System that is the subject of the investigation prior to disclosure to FERC of any non-public non-U.S.-related compliance information regarding the matter to be investigated. NERC's notice to the other Applicable Governmental Authority shall describe the nature of the proposed disclosures to FERC and shall state the procedures NERC will utilize in connection with the investigation to ensure compliance with regulations of the other Applicable Governmental Authority or other law of the applicable jurisdiction concerning disclosure of non-public compliance information.

3.4.1 Compliance Investigation Process Steps

The process steps for a Compliance Investigation are as follows:[5]

[4]Examples of situations in which NERC may decide to lead a Compliance Investigation include: (i) to assure consistency in investigative processes, (ii) to coordinate Compliance Investigations into matters that may cross Regional Entity boundaries, (iii) where the potential noncompliance is related to the Regional Entity or one of its affiliates, divisions, committees or subordinate structures, or (iv) where the Regional Entity determines it cannot conduct the Compliance Investigation.

[5]~~If no Possible Violation(s) are found, this process normally completes within sixty (60) days following the decision to initiate a Compliance Investigation.~~

- The Compliance Enforcement Authority ~~is notified or~~ becomes aware of circumstances indicating a Reliability Standard may have been or is being violated and determines whether a Compliance Investigation is warranted. Within three (3)~~two (2)~~ business days of the decision to initiate a Compliance Investigation, the Compliance Enforcement Authority: (i) notifies the Registered Entity of the initiation and initial scope of the Compliance Investigation, (ii) instructs the Registered Entity~~the requirements~~ to preserve all records and information relevant to the Compliance Investigation~~ and, where appropriate, the reasons for the Compliance Investigation~~, and (iii) provides a copy of the notice to~~notifies~~ NERC~~ of the initiation of and the reasons for the Compliance Investigation~~. The~~While the Compliance Enforcement Authority may, at its discretion, notify the Registered Entity of the reasons for its~~ Compliance Investigation may be expanded beyond the initial scope based on information obtained by the Compliance Enforcement Authority after initiation of~~,~~ the Compliance Investigation~~, as it unfolds, need not be limited to this scope~~.

- NERC assigns a NERC staff member to the Compliance Investigation as an observer or team member and to serve as a single point of contact for communications with NERC. Within three (3)~~two (2)~~ business days after NERC receives~~is~~ ~~notified~~notice of the decision to initiate a Compliance Investigation, NERC will notify FERC and each other Applicable Governmental Authority having jurisdiction over a Registered Entity or a portion of the Bulk Power System to which the Compliance Investigation relates. Any such notice to FERC or to another Applicable Governmental Authority will be provided in accordance with Section 8.0, Reporting and Disclosure.~~ Provided, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to an Applicable Governmental Authority other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.~~

- The Compliance Enforcement Authority requests data or documentation and provides a list of individuals on the Compliance Investigation team and their recent employment history. ~~The Registered Entity may object to any individual on the Compliance Investigation team in accordance with Section 3.1.5.4; however, the Registered Entity may not object to participation by NERC, by FERC staff or by staff of another Applicable Governmental Authority on the Compliance Investigation team. If the Reliability Standard does not specify the advance notice period, a request is normally issued with no less than twenty (20) days advance notice.~~

~~-~~Within ten (10) business days of receiving the notification of a Compliance Investigation, a Registered Entity subject to a Compliance Investigation may object to any member of the Compliance Investigation team on grounds of a conflict of interest or the existence of other circumstances that could interfere with the team member's impartial performance of his or her duties; however, the Registered Entity may not object to participation by NERC, by

FERC staff or by staff of another Applicable Governmental Authority having reliability jurisdiction over the Registered Entity in the Compliance Investigation. Such objections must be provided in writing to the Compliance Enforcement Authority within such ten (10) business day period. The Compliance Enforcement Authority will make a final determination as to whether the individual will participate in the Compliance Investigation of the Registered Entity.

- The Registered Entity provides the required information to the Compliance Enforcement Authority in the format and by the Required Date ~~as~~ specified in the request. If information is not received in the time and format requested, the Compliance Enforcement Authority may initiate the steps in **Process for Non-Submittal of Requested Data** in **Attachment 1**.

- If necessary, the Compliance Investigation may include ~~an~~ on-site visits with interviews of the appropriate personnel and review of data.

- ~~In conducting the Compliance Investigation, t~~The Compliance Enforcement Authority may require the Registered Entity to (i) provide a verification under oath by an officer, employee, attorney or other authorized representative of the Registered Entity attesting to the accuracy, completeness and truth of the Registered Entity's responses to the Compliance Enforcement Authority's requests for information; and (ii) produce one or more officers, employees or other authorized representatives of the Registered Entity who are familiar with the matter(s) that are the subject of the Compliance Investigation, to be interviewed or to provide testimony under oath concerning such matters. The Compliance Enforcement Authority shall determine in each case (i) whether representatives of the Registered Entity shall be allowed to be present when an interview is taking place or testimony is being taken, and (ii) whether, and by what method, the interview or testimony shall be recorded; provided, that counsel for the person being interviewed or giving testimony may be present when the interview is being conducted or testimony is being taken (regardless of whether such counsel also represents the Registered Entity).

- The Compliance Enforcement Authority reviews information to determine compliance with the Reliability Standards. The Compliance Enforcement Authority may request additional data and/or information, if necessary ~~for a complete assessment or to demonstrate compliance~~.

- The Compliance Enforcement Authority completes the assessment of compliance with the Reliability Standard, ~~and/or approval of the applicable~~ which may include review of a Mitigation Plan or mitigating activities, ~~writes~~ and provides a~~distributes the~~ report of the Compliance Investigation to NERC, and ~~notifies~~ the Registered Entity.

- If the Compliance Enforcement Authority ~~concludes~~, at any time during the Compliance Investigation, identifies a potential noncompliance with a Reliability Standard requirement by a Registered Entity, the Compliance Enforcement Authority shall conduct a Preliminary Screen of the potential noncompliance in accordance with Section 3.8 ~~and~~

~~after completing a Preliminary Screen(s), that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation~~.

- If the Compliance Enforcement Authority determines that no violation occurred, it shall send the Registered Entity and NERC a notice that the Compliance Investigation has been completed. NERC will in turn notify FERC and, if the Compliance Investigation pertained to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, will also notify such other Applicable Governmental Authority. Any such notice to FERC or to another Applicable Governmental Authority shall be provided in accordance with Section 8.0, Reporting and Disclosure.~~Provided, however, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.~~

3.5 Self-Report~~sing~~

Self-Report~~sing is~~ are encouraged at the time a Registered Entity becomes aware (i) that it has ~~of a~~ violat~~edion of~~ a Reliability Standard, or (ii) ~~a change in~~ the violation severity level of a previously reported violation has changed. Self-Report~~sing~~ of a violation of a Reliability Standard ~~is~~are encouraged regardless of whether the Reliability Standard requires reporting on a pre-defined schedule in the Compliance Program ~~and~~or whether the violation is determined outside the pre-defined reporting schedule. If possible, and without delaying the Self-Report, a Self-Report may include the actions that have been taken or will be taken to resolve the violation.

3.5.1 Self-Report~~ing~~ Process Steps

The process steps for Self-Report~~sing~~ are as follows:[6]

- The Compliance Enforcement Authority posts the Self-Report~~ing~~ submittal forms and ensures they are maintained and available ~~on its Web site~~.

- The Registered Entity provides the Self-Report~~ing~~ information to the Compliance Enforcement Authority.

- The Compliance Enforcement Authority reviews the information to evaluate~~determine~~ compliance with the Reliability Standards and may request that the Registered Entity ~~to~~ provide clarification or additional data and/or information.

[6] ~~This process normally completes within sixty (60) days following the Compliance Enforcement Authority's receipt of data.~~

~~□The Compliance Enforcement Authority completes the assessment of the Registered Entity for compliance with the Reliability Standards and any Mitigation Plan, if applicable, and notifies the Registered Entity.~~

- ~~If t~~The Compliance Enforcement Authority ~~concludes, after~~ conduct~~sing~~ a Preliminary Screen~~(s),~~ of the Self-Report information in accordance with Section 3.8~~that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation.~~

3.6 Periodic Data Submittals

The Compliance Enforcement Authority requires Periodic Data Submittals in accordance with the schedule stated in the applicable Reliability Standard, or as established by the Compliance Enforcement Authority, or on an as-needed basis. ~~Requests for data submittals will be issued by t~~The Compliance Enforcement Authority shall issue requests for Periodic Data Submittals to Registered Entities within at least the minimum advance notice period specified by the applicable Reliability Standard. If the Reliability Standard does not specify an advance notice period, the Compliance Enforcement Authority will normally issue this request ~~will normally be issued~~ with no less than twenty (20) days advance notice.

3.6.1 Periodic Data Submittals Process Steps

The process steps for Periodic Data Submittal are as follows:[7]

- The Compliance Enforcement Authority posts the current data reporting schedule on its web site and informs~~keeps~~ Registered Entities ~~informed~~ of changes and/or updates. The Compliance Enforcement Authority ensures that the ~~appropriate Reliability Standard compliance procedures and the~~ required submittal forms for the Reliability Standards being evaluated are maintained and available ~~via its web site~~.
- The Compliance Enforcement Authority makes a request for a Periodic Data Submittal.
- The Registered Entity provides the required information to the Compliance Enforcement Authority in the format and by the Required Date~~as~~ specified in the request.
- The Compliance Enforcement Authority reviews the data submittal to determine compliance with the Reliability Standards and may request additional data and/or information if necessary ~~for a complete assessment or to demonstrate compliance~~.
- If the Compliance Enforcement Authority's review of the data submittal indicates a potential noncompliance with a Reliability Standard requirement by the Registered Entity, the Compliance Enforcement Authority performs a Preliminary Screen of the potential noncompliance in accordance with Section 3.8.

[7] ~~If no Possible Violation(s) are found, this process generally completes within ten (10) business days of the Compliance Enforcement Authority's receipt of data.~~

- ~~If the Compliance Enforcement Authority's assessment of the Registered Entity's compliance indicates there may be a Possible Violation, the Compliance Enforcement Authority provides an opportunity for the Registered Entity to comment on the assessment before it is finalized.~~

- ~~If the Compliance Enforcement Authority concludes, after conducting a Preliminary Screen(s), that there is a Possible Violation of a Reliability Standard, it shall send the Registered Entity a Notice of Possible Violation.~~

Receipt of a Periodic Data Submittal by the Compliance Enforcement Authority shall not be construed as a finding by the Compliance Enforcement Authority that the Registered Entity is compliant with, not compliant with, or not subject to, the Reliability Standard requirement.

~~3.7Exception Reporting~~

~~Some Reliability Standards require reporting of exceptions to compliance with the Reliability Standard as a form of compliance monitoring. The Compliance Enforcement Authority shall require Registered Entities to provide reports identifying any exceptions to the extent required by any Reliability Standard.~~

~~The Compliance Enforcement Authority shall also require Registered Entities to confirm the number of exceptions that have occurred in a given time period identified by NERC, even if the number of exceptions is zero.~~

~~3.8~~3.7 Complaints

Either NERC or Regional Entities may receive Complaints alleging violations of a Reliability Standard. ~~A Regional Entity~~ The Compliance Enforcement Authority will conduct a review of each Complaint it receives to determine if the Complaint provides sufficient basis for initiating another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process, except that NERC will review any Complaint ~~(1) that is related to a Regional Entity or its affiliates, divisions, committees or subordinate structures, (2)~~ where the Compliance Enforcement Authority~~Regional Entity~~ determines it cannot conduct the review, or ~~(3)~~ if the complainant wishes to remain anonymous or specifically requests NERC to conduct the review of the Complaint.

If the Complaint is submitted to NERC, NERC will forward the information to the Regional Entity, as appropriate.

All anonymous Complaints will be reviewed and any resulting ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement processes conducted by NERC will be conducted in accordance with Section ~~3.8.2~~3.7.2 to prevent disclosure of the identity of the complainant.

The Compliance Enforcement Authority conducting the review will determine if the Complaint may be closed as a result of the initial review and assessment ~~of the Complaint to determine~~or if it provides sufficient basis for initiating another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process. The ~~Regional Entity~~Compliance Enforcement Authority will report the results of its review of the Complaint to NERC. If, as a result of the initial review of the Complaint, the Compliance Enforcement Authority determines that initiating another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is warranted, the Compliance

Enforcement Authority shall conduct that ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process ~~will be conducted~~ in accordance with the applicable provisions of Section 3.0.

~~3.8.1~~3.7.1 Complaint Process Steps

The detailed process steps for the Complaint process are as follows:[8]

- The complainant notifies NERC or a Regional Entity using the NERC compliance hotline, submitting a NERC Complaint reporting form, or by other means. NERC and the Regional Entity shall post ~~A~~a link to the Complaint reporting form ~~will be posted~~ on their respective ~~the NERC and Regional Entity~~ Web sites. The Complaint should include sufficient information to enable NERC or the Regional Entity to make an assessment regarding~~of~~ whether the initiation of another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is warranted. NERC or the Regional Entity may not act on a Complaint if the Complaint is incomplete and does not include sufficient information.

- If the Compliance Enforcement Authority determines that initiation of another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is warranted, it initiates the ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process in accordance with the applicable provisions of Section 3.0 or Section 5.0; otherwise it takes no further action. The Compliance Enforcement Authority notifies the complainant, the Registered Entity, and NERC of the initiation of the ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process. If the Compliance Enforcement Authority determines that initiation of another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is not warranted, it will notify the complainant, NERC, and the Registered Entity that no further action will be taken.

- The Compliance Enforcement Authority fully documents the Complaint and the Complaint review, and whether another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is warranted~~initiated or not~~.

~~3.8.2~~3.7.2 Anonymous Complainant Notification Procedure

A~~n anonymous~~ complainant who believes, or has information indicating, there has been a violation of a Reliability Standard, and wishes to remain anonymous, can report the information and request that the complainant's identity not be disclosed.[9] All Complaints lodged by a person or entity requesting that the complainant's identity not be disclosed shall be investigated by NERC following the procedural steps described in Section ~~3.8.1~~3.7.1. Anonymous Complaints received by a Regional Entity will either be directed to NERC or the Regional Entity will collect and forward the information to NERC, at the Regional Entity's discretion. Neither NERC nor the Regional Entity shall disclose the identity of any person or entity reporting information indicating violations of Reliability Standards to NERC or to a Regional Entity that

---

[8] ~~If no Possible Violations are found, this process normally completes within sixty (60) days following receipt of the Complaint.~~

[9] NERC has established a Compliance Hotline that may be used for the submission of Complaints by persons or entities that ~~to~~ do not want his/her/its identity disclosed (see www.nerc.com for additional information).

requests that his/her/its identity not be revealed. The identity of the complainant will only be known by NERC and in the case where a Regional Entity collects the information, by NERC and the Regional Entity. If the Compliance Enforcement Authority determines that initiation of another ~~C~~compliance ~~M~~monitoring ~~and~~ or ~~E~~enforcement process is not warranted, it will notify the complainant, NERC, and the Registered Entity that no further action will be taken.

3.8 Preliminary Screen

If the Compliance Enforcement Authority obtains information, through one of the compliance monitoring processes described in this Section 3.0 or by any other means, that indicates a potential noncompliance with a Reliability Standard requirement, the Compliance Enforcement Authority shall conduct a Preliminary Screen of the potential noncompliance. The Preliminary Screen shall be conducted within five (5) business days after the Compliance Enforcement Authority identifies the potential noncompliance, except that (i) if the Compliance Enforcement Authority identifies the potential noncompliance during a Compliance Audit, the Preliminary Screen shall be conducted immediately following the exit briefing of the Registered Entity, and (ii) if the Compliance Enforcement Authority identifies the potential noncompliance during a Compliance Investigation, the Preliminary Screen shall be conducted immediately after the Registered Entity is first notified of the potential noncompliance identified by the Compliance Investigation.

A Preliminary Screen shall be limited to determining whether:

(1) the entity allegedly involved in the potential noncompliance is a Registered Entity;

(2) the Reliability Standard requirement to which the evidence of potential noncompliance relates is applicable to the entity, has been approved by the Applicable Governmental Authority, and is in effect at the time of the potential noncompliance; and

(3) if known, the potential noncompliance is not a duplicate of a Possible Violation or Alleged Violation that is currently being processed.

If the Preliminary Screen results in an affirmative determination with respect to the above criteria, a Possible Violation exists and the Compliance Enforcement Authority shall proceed in accordance with Section 5.0.

The Compliance Enforcement authority shall maintain records of all Preliminary Screens.

4.0 ANNUAL IMPLEMENTATION PLANS

4.1 NERC Compliance Monitoring and Enforcement Program Implementation Plan

NERC will maintain and update the NERC Implementation Plan, to be carried out by Compliance Enforcement Authorities in the performance of their responsibilities and duties in implementing the NERC Compliance Monitoring and Enforcement Program. The NERC

Implementation Plan will be provided to the Regional Entities on or about Septemberby October 1 of each year and will specify the Reliability Standards requiring reporting by Registered Entities to the Compliance Enforcement Authority to provide verification of compliance through one of the monitoring methods described in this Compliance Programplan document. The NERC Implementation Plan will be posted on the NERC web site. NERC may update and revise the NERC Implementation Plan during the course of the year as necessary. Regional Entities have discretion to make modifications to the NERC Implementation Plan with respect to individual Registered Entities, based on a determination concerning the Registered Entity's past and current compliance performance. As these changes to the NERC Implementation Plan occur, Registered Entities that have previously been notified concerning the schedule and scope of Compliance Audits and other compliance monitoring processes may be required to make adjustments in response to these changes.

4.2 Regional Entity Implementation Plan

By on or about OctoberNovember 1 of each year, each Regional EntityEntities will submit a Regional Implementation Plan for the following calendar year to NERC for review and approval. The Regional Implementation Plan and the Regional Entity's other relevant Compliance Program documents shall be posted on the Regional Entity's Web site. The Regional Entity may update and revise the Regional Entity Implementation Plan during the course of the year as necessary, with NERC approval, or as required by NERC. Regional Entities have discretion to make modifications to the Regional Entity Implementation Plan with respect to individual Registered Entities, based on a determination concerning the Registered Entity's past and current compliance performance. As these changes to the Regional Entity Implementation Plan occur, Registered Entities that have previously been notified concerning the schedule and scope of Compliance Audits and other compliance monitoring processes may be required to make adjustments in response to these changes.

5.0 ENFORCEMENT ACTIONS

The Compliance Enforcement Authority shall determine (i) whether there have been violations of Reliability Standards by Registered Entities within the Compliance Enforcement Authority's area of responsibility, and (ii) if so, the appropriate remedial actionsmitigating activities, and penalties and sanctions, as prescribed in the NERC *Sanction Guidelines* (Appendix 4B to the NERC Rules of Procedure). NERC will work to achieve consistency in the application of the *Sanction Guidelines* by Regional Entities by direct oversight and review of penalties and sanctions, and each Regional Entity shall provide to NERC such information as is requested by NERC concerning any penalty, sanction, or remedial actionsmitigating activities imposed by the Regional Entity.

The imposition and acceptance of penalties and sanctions shall not be considered an acceptable alternative to any Registered Entity's continuing obligation to comply with the Reliability Standards.

The Compliance Enforcement Authority has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security

procedures conforming to Section 1500 of the Rules of Procedure and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost of the information were placed into the public domain. Parties engaged in the process described in this section should consult with each other on the data and information that would be appropriate for effectively addressing this section's process requirements. If a Registered Entity believes that a request for documents, data or information is unreasonable, the Registered Entity may request a written determination from the NERC General Counsel. If documents, data or information requested from a Registered Entity in connection with an enforcement process are not received by the Required Date, the Compliance Enforcement Authority may execute the steps described in **Attachment 1, Process for Non-submittal of Requested Data.**

The following enforcement process is undertaken by the Compliance Enforcement Authority following identification~~, through one of the Compliance Monitoring and Enforcement processes set forth in Section 3.0,~~ of a Possible Violation ~~evidence~~ of ~~noncompliance with~~ a Reliability Standard requirement by a Registered Entity. However, under the circumstances presented by some Possible Violations, Alleged Violations or Confirmed Violations, absolute adherence to the following enforcement process, to the exclusion of other approaches, may not be the most appropriate, efficient or desirable means by which to achieve the overall objectives of the Compliance Program for NERC, the Compliance Enforcement Authority and the Registered Entity. In such circumstances, other approaches may be considered and employed.

~~**5.1Preliminary Screen**~~

~~If the Compliance Enforcement Authority identifies or obtains evidence of potential noncompliance with a Reliability Standard, the Compliance Enforcement Authority shall perform a Preliminary Screen to determine whether there is a Possible Violation. A Preliminary Screen shall be limited to determining whether:~~

~~(i)the entity allegedly involved in the potential noncompliance is a Registered Entity; and~~

~~(ii) the Reliability Standard requirement to which the evidence of potential noncompliance relates is applicable to a reliability function for which the entity is registered.~~

~~The Compliance Enforcement Authority shall complete the Preliminary Screen within five (5) business days after identifying or obtaining evidence of potential noncompliance with a Reliability Standard.~~

~~The Compliance Enforcement Authority shall maintain records of all Preliminary Screens.~~

5.1 Notice of Possible Violation

If a Preliminary Screen conducted in accordance with Section 3.8 results in an affirmative determination with respect to the Preliminary Screen~~above~~ criteria, a Possible Violation exists.

The Compliance Enforcement Authority shall issue a Notice of Possible Violation to the Registered Entity. The Notice of Possible Violation shall:

(i) state that a Possible Violation by the Registered Entity has been identified;

(ii) provide a brief description of the Possible Violation, including the Reliability Standard requirement(s) and, if known, the date(s) involved; and

(iii) instruct the Registered Entity to retain and preserve all data and records relating to the Possible Violation.

Upon issuing a Notice of Possible Violation, the Compliance Enforcement Authority reports the Possible Violation to~~enters the Possible Violation into the~~ NERC~~ compliance reporting and tracking system~~. NERC reports the Possible Violation to the NERC Board of Trustees Compliance Committee and submits a Notice of Possible Violation, on a confidential basis, to FERC and to other Applicable Governmental Authorities, as applicable. Any such notice to FERC or to other Applicable Governmental Authorities shall be provided in accordance with Section 8.0, Reporting and Disclosure.

~~5.2~~5.2 Assessment of Possible Violation

After issuing a Notice of Possible Violation, the Compliance Enforcement Authority shall conduct an assessment of the facts and circumstances surrounding the Possible Violation to determine whether evidence exists to indicate the Registered Entity has violated the Reliability Standard requirement(s) identified in the Notice of Possible Violation, or whether the Possible Violation should be dismissed. The Compliance Enforcement Authority may consider any additional information to demonstrate that the Possible Violation should be dismissed or modified.

~~5.3~~5.3 Notification to Registered Entity of Alleged Violation

If the Compliance Enforcement Authority determines, based on an assessment of the facts and circumstances surrounding a Possible Violation, that evidence exists to indicate a Registered Entity has violated a Reliability Standard, ~~and the Compliance Enforcement Authority and the Registered Entity have not entered into settlement negotiations pursuant to Section 5.6,~~ the Compliance Enforcement Authority shall notify the Registered Entity of the determination of the Alleged Violation, ~~and shall notify NERC of the Alleged Violation,~~ through issuance of ~~issue~~ a Notice of Alleged Violation and Proposed Penalty or Sanction or similar notification, and shall report the Alleged Violation to NERC ~~(signed by an officer or designee of the Compliance Enforcement Authority) to the Registered Entity (CEO or equivalent and compliance contact) and shall enter the Alleged Violation into the NERC compliance reporting and tracking system~~. The notification of Alleged Violation shall be transmitted by the Compliance Enforcement Authority to the Registered Entity by electronic mail and shall be effective as of the date of the electronic mail message from the Compliance Enforcement Authority transmitting the notification. The notification~~Notice~~ of Alleged Violation shall include~~state~~, at a minimum:

(i) the Reliability Standard and requirement(s) thereof the Registered Entity has allegedly violated,

(ii) the date and time the Alleged Violation occurred (or is occurring),

(iii) the facts the Compliance Enforcement Authority believes demonstrate or constitute the Alleged Violation,

(iv) the proposed penalty or sanction, if any, determined by the Compliance Enforcement Authority to be applicable to the Alleged Violation in accordance with the NERC *Sanction Guidelines*, including an explanation of the basis on which the particular penalty or sanction was determined to be applicable,

(v) notice that the Registered Entity shall, within thirty (30) days, elect one of the following options or the Compliance Enforcement Authority will deem the Registered Entity to have accepted the determination of violation and proposed penalty or sanction:

1. agree with the Alleged Violation and proposed penalty or sanction, and agree to submit and implement a Mitigation Plan or other mitigating activities to correct the violation and its underlying causes, and may provide a response in accordance with Section 5.4, or

2. agree with the Alleged Violation and agree to submit and implement a Mitigation Plan or other mitigating activities to eliminate the violation and its underlying causes, but contest the proposed penalty or sanction, and may provide a response in accordance with Section 5.4, or

3. contest both the Alleged Violation and proposed penalty or sanction,

(vi) notice that the Registered Entity may elect to submit a Mitigation Plan while contesting the Alleged Violation and/or the proposed penalty or sanction, and that submission of a Mitigation Plan will not waive the Registered Entity's right to contest the Alleged Violation and/or the proposed penalty or sanction;

(vii) notice that if the Registered Entity elects to contest the Alleged Violation and/or the proposed penalty or sanction, the Registered Entity may elect to have a hearing conducted pursuant to either (i) the short-form procedure in Section 1.3.4~~1.3.2~~, or (ii) the ~~full~~general hearing procedure, in **Attachment 2, Hearing Procedures**, and

(viii) required procedures to submit the Registered Entity's Mitigation Plan.

NERC shall ~~forward a copy of the Notice of Alleged Violation to~~notify FERC of the Alleged Violation and, if the Alleged Violation pertains to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, ~~to~~shall notify such other Applicable Governmental Authority of the Alleged Violation, within two (2) business days of receipt from the Compliance Enforcement Authority~~, provided, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and~~

~~NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction~~. Any such notice to FERC or to another Applicable Governmental Authority shall be provided in accordance with Section 8.0, Reporting and Disclosure.

~~Upon acceptance by the Registered Entity of the Alleged Violation and proposed penalty or sanction, the Notice of Confirmed Violation or other enforcement action will then be processed and issued to the Registered Entity.~~

~~5.4~~5.4 Registered Entity Response

If the Registered Entity agrees with, does not contest, or does not respond to the ~~Notice~~notification of Alleged Violation within thirty (30) days following the date of the notification of Alleged Violation by electronic mail, it shall be deemed to have accepted the Compliance Enforcement Authority's determination of violation and penalty or sanction, ~~in which case~~and the Compliance Enforcement Authority shall issue a Notice of Confirmed Violation or similar notification to the Registered Entity and shall ~~enter the Confirmed Violation into the~~ report the Confirmed Violation to NERC ~~compliance reporting and tracking system~~. At the time of notifying the Registered Entity~~issuing the Notice~~ of the Confirmed Violation ~~to the Registered Entity~~, the Compliance Enforcement Authority~~Regional Entity~~ shall also provide notice to the Registered Entity that it may provide a written explanatory statement to accompany the filing with FERC and public posting ~~Notice~~ of the Confirmed Violation. The Registered Entity's statement must include the name, title, and signature of an officer, employee, attorney or other authorized representative of the Registered Entity.

If the Registered Entity contests the Alleged Violation or the proposed penalty or sanction, the Registered Entity shall submit to the Compliance Enforcement Authority, within thirty (30) days following the date of the notification of the Alleged Violation, a response explaining its position, signed by an officer, employee, attorney or other authorized representative together with any supporting information and documents. The Compliance Enforcement Authority shall schedule a conference with the Registered Entity within ten (10) business days after receipt of the response. If the Compliance Enforcement Authority and the Registered Entity are unable to resolve all issues within forty (40) days after the Registered Entity's response, the Registered Entity may request a hearing. The Compliance Enforcement Authority and the Registered Entity may agree in writing to extend the forty (40) day period. If no hearing request is made prior to the end of the forty (40) day period, the violation will be become a Confirmed Violation~~, in which case the Compliance Enforcement Authority shall issue a Notice of Confirmed Violation to the Registered Entity and to NERC.~~.

If a hearing is requested the Compliance Enforcement Authority shall initiate the hearing process in accordance with **Attachment 2, Hearing Procedures**~~by convening a hearing body and~~

~~issuing a written notice of hearing to the Registered Entity and the hearing body and identifying the Compliance Enforcement Authority's designated hearing representative~~.[10]

~~5.5~~5.5 Hearing Process for Compliance Hearings

The Compliance Enforcement Authority hearing process is set forth in **Attachment 2**.

~~5.6~~5.6 Settlement Process

The Registered Entity can request settlement negotiations at any time, including prior to the issuance of notification of an ~~Notice of~~ Alleged Violation; however, the Compliance Enforcement Authority may decline to engage in or to continue settlement negotiations after a Possible Violation or Alleged Violation becomes a Confirmed Violation in accordance with Section 5.4. The Registered Entity or the Compliance Enforcement Authority may terminate settlement negotiations at any time. The time for the Registered Entity to respond to the notification of Alleged Violation pursuant to Section 5.4 is suspended during settlement negotiations. NERC shall be notified of all settlement negotiations and may participate in any settlement negotiations. All settlement negotiations will be confidential until such time as the settlement is approved by NERC. For all settlement discussions, the Compliance Enforcement Authority shall require the Registered Entity to designate an individual(s) authorized to negotiate on its behalf.

The Compliance Enforcement Authority may consider all relevant facts in settlement negotiations. A settlement agreement must ensure that the reliability of the Bulk Power System will not be compromised by the settlement and that a violation of a Reliability Standard will not occur as a result of the settlement. All settlement agreements must provide, if the settlement is approved, for waiver of the Registered Entity's right to further hearings and appeal.

The Compliance Enforcement Authority and the Registered Entity will execute a settlement agreement~~issue a letter~~ setting forth the final settlement terms including all penalties, sanctions and mitigation requirements provided for in the final settlement.

The ~~Regional Entity~~Compliance Enforcement Authority shall report the terms of all settlements of compliance matters to NERC. NERC will review the settlement for the purpose of evaluating its consistency with other settlements entered into for similar violations or under other, similar circumstances. The Registered Entity may submit an explanatory statement, conforming to the requirements of Section 5.4, to be included in the settlement agreement and which shall be subject to consent of the Compliance Enforcement Authority as part of the settlement agreement. The settlement agreement may state that the Registered Entity (i) admits the Alleged Violation, or (ii) does not contest the Alleged Violation, or (iii) neither admits nor denies the Alleged Violation, but may not state that the Registered Entity denies the Alleged Violation. Based on this review, NERC will either approve the settlement or reject the settlement and notify the Compliance Enforcement Authority~~Regional Entity and the Registered Entity~~ of any changes to

[10] ~~If the dispute involves a proposed Mitigation Plan, which has not been accepted by the Compliance Enforcement Authority, the Registered Entity may file a request for hearing with the Compliance Enforcement Authority.~~

the settlement that would result in approval, and within five (5) business days the Compliance Enforcement Authority will in turn notify the Registered Entity. If NERC rejects the settlement, the ~~Regional Entity~~Compliance Enforcement Authority will attempt to negotiate a revised settlement agreement with the Registered Entity including any changes to the settlement specified by NERC.

NERC will report the approved settlement of the violation to FERC and, if the settlement relates to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, to such other Applicable Governmental Authority. Any such report to FERC or to another Applicable Governmental Authority shall be provided in accordance with Section 8.0, Reporting and Disclosure.~~, provided, that NERC will not disclose non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.~~ NERC will also publicly post the violation settled (regardless of whether the settlement includes or does not include an admission of a violation) and the resulting penalty or sanction provided for in the settlement. This posting shall include a copy of the settlement or a description of the terms of the settlement, and a copy of any Mitigation Plan that is agreed to as part of the settlement, with any Critical Energy Infrastructure Information and Confidential Information redacted. The Compliance Enforcement Authority will issue a letter setting forth the final settlement terms including all penalties, sanctions and mitigation requirements provided for in the final settlement. Postings of Notices of Confirmed Violations are addressed in Section 8.0.

~~5.7~~5.7 NERC Appeal Process

~~The~~A Registered Entity or the Compliance Enforcement Authority may appeal the decision of a Regional Entity hearing body~~'s decision~~ to NERC, as provided for in NERC Rules of Procedure, Section 409.[11]

On appeal, NERC shall either affirm the ~~Regional Entity~~ decision or remand to the ~~Regional Entity~~Compliance Enforcement Authority with reasons for its remand, which may include a direction to the ~~Regional Entity~~Compliance Enforcement Authority to revise the decision. If NERC affirms the ~~Regional Entity~~ decision, the ~~Regional Entity~~Compliance Enforcement Authority shall issue a Notice of Confirmed Violation to the Registered Entity. If NERC directs the Compliance Enforcement Authority~~Regional Entity~~ to revise ~~its~~the decision, ~~the~~a Registered Entity that was the subject of the decision or the Compliance Enforcement Authority~~Staff of the Regional Entity whose interests are adversely affected by the directed revision~~ may reopen the proceeding on any issue whose resolution is affected by NERC's directive, irrespective of whether the issue was previously litigated, settled or unopposed.

~~[11]This process generally completes within ninety (90) days of NERC's receipt of request for appeal.~~

~~5.8~~5.8 ~~Approval of a Notice~~Notification of Confirmed Violation

A Notice or other notification of Confirmed Violation issued to a Registered Entity pursuant to Sections 5.4 or 5.7 shall include a detailed record of the enforcement action, including the facts and circumstances analyzed and the information on which the Compliance Enforcement Authority relied in proposing a penalty or sanction.

After NERC receives~~receiving~~ a ~~Notice~~notification of Confirmed Violation ~~through the NERC compliance reporting and tracking system~~from the Compliance Enforcement Authority, NERC shall review the ~~Notice~~notification of Confirmed Violation and utilize the information therein to prepare a Notice of Penalty. NERC shall advise the Compliance Enforcement Authority~~Regional Entity~~ of any additional detail or further development of the factual findings that NERC deems necessary before the Notice of Penalty can be issued.

NERC may direct the Compliance Enforcement Authority~~Regional Entity~~ to revise a penalty determination, in which case the Registered Entity subject to the penalty, or the Compliance Enforcement Authority, as applicable~~Staff of the Regional Entity~~, may reopen the proceedings on any issue on which the penalty was based, irrespective of whether the issue was previously litigated, settled or unopposed.

5.9 Notice of Penalty

If (i) the Registered Entity accepts~~does not dispute~~ the Notice of Alleged Violation and Proposed Penalty or Sanction or other notification of enforcement action from the Compliance Enforcement Authority ~~and the proposed penalty or sanction~~, or (ii) a decision has been entered affirming an ~~finding a~~Alleged ~~v~~Violation and all appeals have been concluded, or (iii) a settlement agreement has been reached addressing the Possible Violation or Alleged Violation~~(s)~~, NERC shall submit~~prepare~~ a ~~draft~~ Notice of Penalty to the Applicable Governmental Authority and provide a copy to the ~~Regional Entity~~Compliance Enforcement Authority. The Regional Entity shall inform the Registered Entity that a Notice of Penalty is pending public filing, at least five (5) business days prior to the public filing and posting. NERC will file the Notice of Penalty with FERC and any other Applicable Governmental Authority~~, as provided in the next paragraph,~~ no sooner than five (5) business days after NERC approves the ~~Notice of~~ Confirmed Violation or settlement agreement.

NERC shall file the Notice of Penalty with FERC and, if the Possible Violation or Alleged Violation pertains to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, to such other Applicable Governmental Authority. Any such filing with FERC or with another Applicable Governmental Authority shall be made in accordance with Section 8.0, Reporting and Disclosure.~~; provided, that NERC will not disclose any non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to Applicable Governmental Authorities other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority~~

~~or by other law of the applicable jurisdiction.~~ NERC will include with the Notice of Penalty any statement provided by the Registered Entity as set forth in Sections 5.4 or ~~5.7~~5.6.

The penalty or sanction will be effective upon expiration of the thirty (30) day period following filing with FERC of the Notice of Penalty (or such longer period as ordered by FERC) or, if FERC decides to review the penalty or sanction, upon final determination by FERC.

5.10 ~~Closure~~Completion of Enforcement Action

Following FERC approval of, or expiration of the period for action by FERC on, a Notice of Penalty filed by NERC, the Compliance Enforcement Authority shall issue a payment due notice and invoice to the Registered Entity. The payment due notice and invoice shall state the payment due date which shall be thirty (30) days from the date of the payment due notice and invoice. Upon payment of all monetary penalties by the Registered Entity, the Compliance Enforcement Authority shall issue a notice confirming payment to the Registered Entity, and provide a copy of the notice confirming payment to NERC. Following the completion by the Registered Entity of all requirements set forth in the Notice of Penalty and any settlement agreement, the Compliance Enforcement Authority shall issue the Registered Entity a Notice of Completion of Enforcement Action.

If the Compliance Enforcement Authority dismisses or disposes of a Possible Violation or Alleged Violation that does not become a Confirmed Violation, the Compliance Enforcement Authority shall issue a Notice of Completion of Enforcement Action to the Registered Entity.

A copy of the Notice of Completion of Enforcement Action shall also be provided to NERC by the Compliance Enforcement Authority.

The Notice of Completion of Enforcement Action shall include a release of any data retention directives that were previously issued to the Registered Entity in connection with the matter. Upon issuance of a Notice of Completion of Enforcement Action, tracking of the violation is completed, and the enforcement action shall be closed.

5.11 Special Procedures for an Enforcement Action Against an ISO/RTO Where the Monetary Penalty May be Allocated by the ISO/RTO to Other Registered Entities

A Registered Entity that is an ISO/RTO may have authority to allocate, pursuant to a proceeding under section 205 of the Federal Power Act, some or all of a monetary penalty imposed on the ISO/RTO for violation of a Reliability Standard, to another Registered Entity(ies) that the Compliance Enforcement Authority, NERC or FERC determines was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation of the Reliability Standard. In such circumstances, the ISO/RTO may request the Compliance Enforcement Authority to make a determination, during the enforcement process for a Notice of Possible Violation issued to the ISO/RTO, that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. This Section sets forth the procedures to be followed when an ISO/RTO that has received a Notice of Possible Violation requests a determination by the Compliance Enforcement Authority that another Registered Entity(ies) was

responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation.

The procedures in this section apply only where an ISO/RTO requests a determination that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in a Notice of Possible Violation issued to the ISO/RTO, and shall not apply where the ISO/RTO anticipates or is entitled to allocate or assign a monetary penalty among all, or an identified segment of, its members, customers or users, pursuant to general cost recovery provisions in the ISO/RTO's tariffs, agreements or governance documents and regardless of actual fault or responsibility of the entities to whom the monetary penalty is issued for the violation for which the penalty is imposed.

5.11.1 Public Notification List

NERC shall maintain on its website a Public Notification List for each ISO/RTO. The Public Notification Lists shall be based solely on information provided to NERC by each ISO/RTO, and NERC shall have no responsibility to correct errors and omissions on a Public Notification List or in information provided by the ISO/RTO to NERC for inclusion in the Public Notification List. Inclusion of a Registered Entity on the Public Notification List shall not constitute or be construed as a determination by NERC that the ISO/RTO has the authority to allocate to the Registered Entity all or a part of any monetary penalty that may be imposed on the ISO/RTO for violation of a Reliability Standard. The Public Notification List for an ISO/RTO shall be developed and maintained in accordance with the following steps:

(1) The ISO/RTO shall provide to NERC a list of the Registered Entities to which the ISO/RTO contends it has authority to allocate all or a part of any monetary penalty that is imposed on the ISO/RTO for violation of a Reliability Standard, and the NERC registration identification number for each Registered Entity on the list.

(2) The ISO/RTO shall provide revisions to the information for the Public Notification List to NERC from time to time as changes occur, and shall notify NERC of any errors, omissions, corrections or additions needed to the Public Notification List.

(3) NERC shall post and maintain the Public Notification List based on the information provided to NERC by the ISO/RTO. The posted Public Notification List shall consist of the names and NERC registration identification numbers of the Registered Entities and the date each Registered Entity was placed on the Public Notification List.

(4) Each ISO/RTO shall also provide on its website a link to the ISO/RTO's Public Notification List on the NERC website.

5.11.2 ISO/RTO's Request for Determination and Notice to Other Registered Entity or Registered Entities

In order to request the Compliance Enforcement Authority to make a determination in an enforcement action that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to a violation (if confirmed) of a Reliability Standard for which the ISO/RTO has received a Notice of Possible Violation, the ISO/RTO shall, no later than five (5) business days after receiving the Notice of Possible Violation (i) submit a written request to the Compliance Enforcement Authority and (ii) issue a notice to the specified other Regional Entity(ies), each conforming to the requirements of the following two paragraphs of this Section.

The ISO/RTO's written request to the Compliance Enforcement Authority shall contain:

(1) the Compliance Enforcement Authority's identification number for the Notice of Possible Violation;

(2) a statement that the ISO/RTO is requesting that the Compliance Enforcement Authority make a determination that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions and omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation;

(3) the name(s) of, and contact information for, the specified other Registered Entity(ies), including name(s) and address(es) of the Registered Entity(ies) and name(s), telephone number(s) and e-mail address(es) of the contact person(s) for the other Registered Entity(ies);

(4) a statement of the basis for the ISO/RTO's authority to allocate some or all of the monetary penalty to the specified other Registered Entity(ies), including copies of any supporting tariffs, agreements, orders, or governance documents;

(5) a brief statement of the factual basis on which the ISO/RTO contends in good faith that the specified other Registered Entity(ies) was responsible for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. As the enforcement action proceeds, the ISO/RTO shall not be limited by the statement in its written request of the factual basis on which it contends the specified other Registered Entity(ies) was responsible for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation, but rather may supplement, expand or modify this explanation as additional information becomes available during the course of the enforcement action; and

(6) If the specified other Registered Entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, a statement demonstrating that there are extraordinary circumstances warranting that the Compliance Enforcement Authority make the requested determination with respect to the specified other Registered Entity despite the specified other Registered Entity's absence from the Public Notification List.

The ISO/RTO's notice to the specified other Registered Entity(ies) shall contain the following information:

(1) The name of the Registered Entity, and the name, telephone number and e-mail address of the Registered Entity's contact person (person to whom the notice is being sent);

(2) A statement that the ISO/RTO has received a Notice of Possible Violation from the Compliance Enforcement Authority, the Compliance Enforcement Authority's identification number for the Notice of Possible Violation, and contact information for the Compliance Enforcement Authority;

(3) A statement that the ISO/RTO has requested the Compliance Enforcement Authority to make a determination that the Registered Entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, and that the ISO/RTO intends to seek to allocate to the Registered Entity all or a portion of any monetary penalty that is imposed on the ISO/RTO for the violation (if confirmed), if the Compliance Enforcement Authority determines the Registered Entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation.

(4) A statement that the Registered Entity should contact the Compliance Enforcement Authority as soon as possible for further information and to request to participate in the enforcement action relating to the Notice of Possible Violation.

The ISO/RTO shall cause its notice to the specified other Registered Entity(ies) to be delivered to the other Registered Entity(ies) by next-business-day delivery using a delivery service that provides verification of delivery. The ISO/RTO shall provide the Compliance Enforcement Authority with (i) a copy of the notice sent to each specified other Registered Entity, and (ii) a copy of the delivery service's verification of delivery of the notice to each specified other Registered Entity.

5.11.3 Responses of the Compliance Enforcement Authority and the Specified Other Registered Entity or Registered Entities to ISO/RTO's Request for Determination and Notice

Upon (i) verifying that the specified other Registered Entity(ies) was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, or, if the specified other Registered Entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determining that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the specified other Registered Entity(ies), (ii) verifying, based on the written request from the ISO/RTO, that the ISO/RTO has authority to allocate to the specified other Registered Entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed)

identified in the Notice of Possible Violation, and (iii) receiving the copy of the notice and of the verification of delivery to the specified other Registered Entity(ies) showing timely delivery of the notice to the specified other Registered Entity(ies) in accordance with Section 5.11.2, the Compliance Enforcement Authority shall provide the other Registered Entity(ies) with a copy of a non-disclosure agreement (which shall include the Registered Entity's agreement to comply with the confidentiality requirements of the Compliance Program and of Section 1500 of the NERC Rules of Procedure) that must be executed to obtain a copy of the Notice of Possible Violation and a copy of the ISO/RTO's written request to the Compliance Enforcement Authority for a determination that the specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. In addition to transmitting the non-disclosure agreement, the Compliance Enforcement Authority shall advise the specified other Registered Entity(ies) that: (i) the specified other Registered Entity(ies) may elect not to participate in the enforcement action, and may submit a written statement to the Compliance Enforcement Authority stating why the specified other Registered Entity is not participating and providing any facts or information the Registered Entity wishes to provide concerning the occurrence(s) that are the subject of the Notice of Possible Violation, and (ii) whether or not the specified other Registered Entity elects to participate in the enforcement action, the Compliance Enforcement Authority may make a determination that the specified other Registered Entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation.

If the Compliance Enforcement Authority has (i) verified that the specified other Registered Entity(ies) was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation or, if the specified other Registered Entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determined that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the specified other Registered Entity(ies), and (ii) verified that the ISO/RTO has authority to allocate to the specified other Registered Entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, then a specified other Registered Entity that has received a timely notice from the ISO/RTO as described in Section 5.11.2 shall be permitted to participate in the enforcement action concerning the Notice of Possible Violation if the Registered Entity submits a written request to participate to the Compliance Enforcement Authority and executes a non-disclosure agreement in the form provided by the Compliance Enforcement Authority as described above. The specified other Registered Entity must submit its written request to participate prior to, as applicable (i) the date of execution of a settlement agreement between the Compliance Enforcement Authority and the ISO/RTO, or (ii) the date that the Compliance Enforcement Authority issues a Notice of Confirmed Violation to the ISO/RTO. The Compliance Enforcement Authority is not required to suspend or delay the enforcement process pending receipt of a request to participate from the specified other Registered Entity(ies), nor to revisit or redo any aspect of the enforcement process that has already occurred prior to receipt of the specified other Registered Entity(ies)'s written request to participate; however, upon receipt of a written request to participate and executed nondisclosure agreement from the specified other Registered Entity(ies), the Compliance Enforcement Authority shall suspend activity in the enforcement action until it has acted on the request to participate.

Upon receiving the specified other Registered Entity's written request to participate in the enforcement action and the Registered Entity's executed nondisclosure agreement, the Compliance Enforcement Authority shall issue a notice to the ISO/RTO and to the specified other Registered Entity stating that the specified other Registered Entity is allowed to participate in the enforcement action. The Compliance Enforcement Authority's notice that the specified other Registered Entity is allowed to participate in the enforcement action shall include a copy of the Notice of Possible Violation originally issued to the ISO/RTO and, if a Notice of Alleged Violation and Proposed Penalty or Sanction or similar notification has been issued to the ISO/RTO, a copy of the latter Notice or notification.

If the Compliance Enforcement Authority determines (i) that the specified other Registered Entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation and that there are not extraordinary circumstances that warrant making the requested determination with respect to the specified other Registered Entity, or (ii) that the ISO/RTO does not have authority to allocate to the specified other Registered Entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, or (ii) that the ISO/RTO did not provide a timely notice to the specified other Registered Entity in accordance with Section 5.11.1, the Compliance Enforcement Authority shall issue a notice to the ISO/RTO and to the specified other Registered Entity stating that the Compliance Enforcement Authority will not make the determination requested by the ISO/RTO and that the specified other Registered Entity will not be allowed to participate in the enforcement action relating to the Notice of Possible Violation.

5.11.4 Compliance Enforcement Authority's Notices to NERC

(a) Within five (5) business days after receiving an ISO/RTO's written request for a determination that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to a violation identified in the Notice of Possible Violation issued to the ISO/RTO, the Compliance Enforcement Authority shall provide to NERC (i) a copy of the ISO/RTO's written request for a determination that a specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, and (ii) the ISO/RTO's notice to the specified other Registered Entity(ies).

(b) On the same day that the Compliance Enforcement Authority issues a notice pursuant to Section 5.11.3 stating, as applicable, that (i) it will or will not make the determination requested by the ISO/RTO or (ii) the specified other Registered Entity(ies) are or are not allowed to participate in the enforcement action, the Compliance Enforcement Authority shall provide a copy of the notice to NERC and shall send a copy of the notice to any other entities that have been allowed to participate in the enforcement action.

5.11.5 Participation by the Specified Other Registered Entity or Registered Entities in the Enforcement Action Against the ISO/RTO

Upon receiving notice from the Compliance Enforcement Authority that it is allowed to participate in the enforcement action, the specified other Registered Entity may participate in the

same manner as the ISO/RTO and shall be subject to all applicable requirements and deadlines specified in the NERC Compliance Program.

5.11.6 Compliance Enforcement Authority's Determination

If the Compliance Enforcement Authority has (i) verified that the specified other Registered Entity was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, or, if the specified other Registered Entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determined that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the specified other Registered Entity(ies), (ii) verified that the ISO/RTO has authority to allocate to the specified other Registered Entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, and (iii) verified that the specified other Registered Entity(ies) received a timely notice(s) from the ISO/RTO as described in Section 5.11.2, then, if the enforcement action is not resolved by a settlement agreement stating whether or not the specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, the Compliance Enforcement Authority shall make, and include in its proposed Notice of Penalty, its determination of whether or not the specified other Registered Entity(ies) were responsible, in whole or in part, for actions or omissions that caused or contributed to the violation. The Compliance Enforcement Authority's determination shall only address whether or not the specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation, and shall not address whether all or a part of any monetary penalty imposed on the ISO/RTO for the violation should be allocated or assigned to the specified other Registered Entity(ies).

If the specified other Registered Entity(ies) has requested permission, and been allowed, to participate in the enforcement action, any settlement agreement specifying that the specified other Registered Entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation must be agreed to by the specified other Registered Entity(ies).

5.11.7 Procedure Where ISO/RTO Members Are Allowed to Directly Assign Monetary Penalties for Violations of Reliability Standards to the ISO/RTO

If an ISO/RTO's tariffs, agreement or other relevant governance documents establish procedures, that have been approved by FERC, that allow members of the ISO/RTO to directly assign to the ISO/RTO monetary penalties imposed on the ISO/RTO member(s) for violations of Reliability Standards, then the ISO/RTO members may follow the same requirements of Sections 5.11.2, 511.3 and 511.5 as are applicable to an ISO/RTO under those sections, and the ISO/RTO shall be afforded the same rights to participate in the enforcement action as a specified other Registered Entity under Sections 5.11.2, 5.11.3, 5.11.5 and 5.11.6, subject to the same requirements and conditions specified in those sections. In such circumstances, the ISO/RTO shall be deemed to be a "specified other Registered Entity" for purposes of this Section.

5.11.8 Obligation to Pay Monetary Penalty

(a) The ISO/RTO shall be obligated and responsible to pay any monetary penalty imposed by the Compliance Enforcement Authority on the ISO/RTO for violation of a Reliability Standard, in accordance with Section 5.10 of this Appendix, (i) regardless of whether the Compliance Enforcement Authority has made a determination that a specified other Registered Entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation, (ii) without regard to the timing of any separate proceeding(s) in which the ISO/RTO seeks to allocate some or all of the monetary penalty to a specified other Registered Entity(ies), and (iii) without regard to whether or when the ISO/RTO receives payment from the specified other Registered Entity(ies).

(b) In an enforcement action subject to Section 5.11.7, the ISO/RTO member(s) shall be obligated and responsible to pay any monetary penalty imposed by the Compliance Enforcement Authority on the ISO/RTO member(s) for violation of a Reliability Standard, regardless of whether or when the ISO/RTO members receive payment or reimbursement from the ISO/RTO.

6.0 MITIGATION OF VIOLATIONS OF RELIABILITY STANDARDS

The Compliance Enforcement Authority has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security procedures conforming to Section 1500 of the Rules of Procedure and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost of the information were placed into the public domain. Parties engaged in the process described in this section should consult with each other on the data and information that would be appropriate for effectively addressing this section's process requirements. If a Registered Entity believes that a request for documents, data or information is unreasonable, the Registered Entity may request a written determination from the NERC ~~director of enforcement~~General Counsel. If documents, data, information or other reports requested from a Registered Entity in connection with development of a Mitigation Plan or other mitigating activities are not received by the Required Date, the Compliance Enforcement Authority may execute the steps described in **Attachment 1, Process for Non-submittal of Requested Data.**

6.1 Requirement for Submission of Mitigation Plans

A Registered Entity found to be in violation of a Reliability Standard shall file with the Compliance Enforcement Authority (i) a proposed Mitigation Plan to correct the violation, or (ii) a description of how the violation has been mitigated, and any requests for extensions of Mitigation Plans or a report of completed mitigation. A Registered Entity may also submit a proposed Mitigation Plan at any other time, including with a Self-Report, or, without admitting it has committed a violation, in response to a Notice of Possible Violation or ~~Notice~~notification of Alleged Violation.

6.2 Contents of Mitigation Plans

A Mitigation Plan shall include the following information:

- The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section 2.0.

- The Possible, Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.

- The cause of the Possible, Alleged or Confirmed Violation(s).

- The Registered Entity's action plan to correct the Possible, Alleged or Confirmed Violation(s).

- The Registered Entity's action plan to correct the cause of the Possible, Alleged or Confirmed Violation.

- The Registered Entity's action plan to prevent recurrence of the Possible, Alleged or Confirmed Violation(s).

- The anticipated impact of the Mitigation Plan on the Bulk Power System reliability and an action plan to mitigate any increased risk to the reliability of the Bulk Power System while the Mitigation Plan is being implemented.

- A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Possible, Alleged or Confirmed Violation(s) corrected.

- Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined for not completing work associated with accepted milestones.

- Any other information deemed necessary or appropriate

The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity~~, which if applicable, shall be the person that signed the Self-Certification or Self-Reporting submittals~~.

6.3 Timetable for Completion of Mitigation Plans

The Mitigation Plan shall be completed in accordance with its terms.~~time to have a reasonable potential to correct all of the violation(s) prior to the next applicable compliance reporting/assessment period after occurrence of the violation for which the Mitigation Plan is~~

~~submitted. In all cases the Mitigation Plan should be completed without delay, and should encompass actions necessary to prevent a recurring violation of the Reliability Standard requirements underlying the Possible, Alleged or Confirmed Violation(s). The Compliance Enforcement Authority will expect full compliance with the Reliability Standard to which the Mitigation Plan is applicable at the next report or assessment of the Registered Entity.~~ At the Compliance Enforcement Authority's discretion, the completion deadline may be extended for good cause including, but not limited to: (i) operational issues such as the inability to schedule an outage to complete mitigating activities~~short assessment periods (i.e., event driven or monthly assessments)~~, and (ii) construction requirements in the Mitigation Plan that require longer to complete than originally anticipated~~extend beyond the next assessment period or other extenuating circumstances~~. If the Mitigation Plan extends beyond the next applicable reporting/assessment period, sanctions for any violation of the applicable Reliability Standard(s) occurring during the implementation period will be held in abeyance and will be waived if the Mitigation Plan is satisfactorily completed.

Any violations assessed during the period of time the accepted Mitigation Plan is being implemented will be recorded by the Compliance Enforcement Authority with associated sanctions or penalties. Regional Entities will report any findings of violations recorded during this time period to NERC with the notation that the Registered Entity is working under an accepted Mitigation Plan with an extended completion date with penalties and sanctions held in abeyance until completion of the Mitigation Plan. Upon completion of the accepted Mitigation Plan in accordance with Section 6.6, the Compliance Enforcement Authority will notify the Registered Entity that any findings of violations of the applicable Reliability Standard during the period that the accepted Mitigation Plan was being implemented have been waived and no penalties or sanctions will apply. Regional Entities will also notify NERC of any such waivers of violations of Reliability Standards.

A request for an extension of any milestone or the completion date of the accepted Mitigation Plan by a Registered Entity must be received by the Compliance Enforcement Authority at least five (5) business days before the original milestone or completion date. The Compliance Enforcement Authority may accept a request for an extension or modification of a Mitigation Plan if the Compliance Enforcement Authority determines the request is justified, and shall notify NERC of the extension or modification within five (5) business days.

If a Mitigation Plan submitted by a Registered Entity is rejected by the Regional Entity acting as Compliance Enforcement Authority or the hearing body in accordance with Section 6.5, the Registered Entity shall be subject to any findings of violation of the applicable Reliability Standards during the period the Mitigation Plan was under consideration and to imposition of any penalties or sanctions imposed for such violations.

6.4 Submission of Mitigation Plans

A Mitigation Plan may be submitted at any time but shall have been submitted by the Registered Entity within thirty (30) days after being served the notification~~Notice~~ of Alleged Violation, if the Registered Entity does not contest the Alleged Violation and penalty or sanction, or shall be reflected in a settlement agreement or Notice of Penalty. If the Registered Entity disputes the ~~Notice of~~ Alleged Violation or the penalty or sanction, the Registered Entity shall submit its Mitigation Plan within ten (10) business days following issuance of the written decision of the

hearing body, unless the Registered Entity elects to appeal the hearing body's determination to NERC. The Registered Entity may choose to submit a Mitigation Plan while it contests an Alleged Violation or penalty or sanction or in response to a Notice of Possible Violation; such submission shall not be deemed an admission of a violation or the appropriateness of a penalty or sanction. If the Registered Entity has not yet submitted a Mitigation Plan, or the Registered Entity submits a Mitigation Plan but it is rejected by the Regional Entity acting as Compliance Enforcement Authority or the hearing body in accordance with Section 6.5, any subsequent violations of the Reliability Standard identified by the Compliance Enforcement Authority before the hearing body renders its decision will not be held in abeyance and will be considered as repeat violations of the Reliability Standard.

6.5 Review and Acceptance or Rejection of Proposed Mitigation Plans

Unless the time period is extended by the Compliance Enforcement Authority, it will complete its review of the Mitigation Plan, and will issue a written statement accepting or rejecting the Mitigation Plan, within thirty (30) days of receipt; otherwise the Mitigation Plan will be deemed accepted. In order to extend the initial or an extended period for review of the Mitigation Plan, the Compliance Enforcement Authority shall, within the initial or extended review period, notify the Registered Entity (and NERC if NERC is not the Compliance Enforcement Authority) that the review period is being extended and identify the date by which the Compliance Enforcement Authority will complete its review of the Mitigation Plan. The Compliance Enforcement Authority's extension notice shall also state that if the Compliance Enforcement Authority has not issued a notice by the end of the extended review period either stating that the Compliance Enforcement Authority accepts or rejects the proposed Mitigation Plan or further extending the Compliance Enforcement Authority's period for review of the Mitigation Plan, the Mitigation Plan will be deemed accepted.

If the Compliance Enforcement Authority rejects a Mitigation Plan, the Compliance Enforcement Authority will provide the Registered Entity with a written statement describing the reasons for the rejection, and will require the Registered Entity to submit a revised Mitigation Plan by the Required Date. The Compliance Enforcement Authority will notify the Registered Entity within ten (10) business days after receipt of a revised Mitigation Plan whether the Compliance Enforcement Authority will accept or reject the revised Mitigation Plan and provide a written statement describing the reasons for rejection and the Required Date for the second revised Mitigation Plan. If the second review results in rejection of the Mitigation Plan, the Registered Entity may request a hearing in accordance with the Hearing Procedures, by submitting to the Compliance Enforcement Authority a written request for hearing including an explanation of why the Mitigation Plan should be accepted. After the hearing is completed, the Compliance Enforcement Authority will issue a written statement accepting a Mitigation Plan it deems as appropriate.

Within five (5) business days after a Regional Entity accepts a Mitigation Plan, the Regional Entity (i) will notify NERC and the Registered Entity of the acceptance of the Mitigation Plan and (ii) will provide the accepted Mitigation Plan to NERC. NERC will review the accepted Mitigation Plan and, within thirty (30) days following its receipt of the Mitigation Plan from the Regional Entity, will notify the Regional Entity and the Registered Entity, on a contemporaneous basis, as to whether the Mitigation Plan is approved or disapproved by NERC. If NERC disapproves a Mitigation Plan that was accepted by the Regional Entity, NERC shall state its

reasons for the rejection, and may state the changes to the Mitigation Plan that would result in approval by NERC. The Registered Entity shall not be subject to findings of violations of the specific requirements of Reliability Standards that are the subject of the Mitigation Plan or to imposition of penalties or sanctions for such violations with respect to the period of time the Mitigation Plan was under consideration by NERC and for a reasonable period following NERC's disapproval of the Mitigation Plan, so long as the Registered Entity promptly submits a modified Mitigation Plan that addresses the concerns identified by NERC.

If a Registered Entity submits a Mitigation Plan prior to issuance of a ~~Notice~~notification of Confirmed Violation or entry into a settlement, such as with a Self-Report or in response to a Notice of Possible Violation, the Regional Entity may provisionally accept the proposed Mitigation Plan. If the Regional Entity subsequently determines, upon completing its assessment of the Possible Violation, that the facts and circumstances are different than those on which the accepted Mitigation Plan was based, the Regional Entity may, by notice to the Registered Entity and to NERC, require the Registered Entity to submit a revised Mitigation Plan that fully addresses the facts and circumstances of the violation. The Regional Entity's notice shall state the additional or different facts and circumstances that need to be addressed in the revised Mitigation Plan. The Registered Entity shall submit a revised Mitigation Plan in response to the notice within thirty (30) days following the date of the notice, unless the Regional Entity specifies or allows a longer time period. The Registered Entity's revised Mitigation Plan shall be subject to review and acceptance or rejection by the Regional Entity and by NERC in accordance with this Section 6.5. If the Regional Entity issues a ~~Notice~~notification of Confirmed Violation or enters into a settlement with the Registered Entity and does not identify a need to request modifications to the provisionally-accepted Mitigation Plan based on additional or different facts and circumstances, the Regional Entity shall issue a notice to the Registered Entity, with a copy to NERC, stating that the "provisional" nature of the acceptance is terminated and the acceptance is final. The Regional Entity shall issue such notice within five (5) business days of issuance of the Notice of Confirmed Violation or entry into the settlement.

NERC will submit to FERC, as non-public information, an approved Mitigation Plan relating to violations of Reliability Standards within seven (7) business days after NERC approves the Mitigation Plan. NERC shall publicly post the approved Mitigation Plan as part of the public posting of the related Notice of Penalty in accordance with Section 8.0 or settlement in accordance with Section 5.6.

6.6 Completion/Confirmation of Implementation of Mitigation Plans

The Registered Entity shall provide updates at least quarterly to the Compliance Enforcement Authority on the progress of the Mitigation Plan. The Compliance Enforcement Authority will track the Mitigation Plan to completion and may conduct on-site visits and review status during audits to monitor Mitigation Plan implementation.

Upon completion of the Mitigation Plan, the Registered Entity shall provide to the Compliance Enforcement Authority certification, signed by an officer, employee, attorney or other authorized representative of the Registered Entity, that all required actions described in the Mitigation Plan have been completed and shall include data or information sufficient for the Compliance Enforcement Authority to verify completion. The Compliance Enforcement Authority shall request such data or information and conduct follow-up assessments, on-site or other Spot

Checksing, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed ~~and the Registered Entity is in compliance with the subject Reliability Standard requirement(s)~~.

In the event all required actions in the Mitigation Plan are not completed within the applicable deadline including any extensions of the original deadline granted under Section 6.3, any violation(s) of a Reliability Standard subject to the Mitigation Plan that occurred during the originally scheduled time period for completion will be enforced immediately and a new Mitigation Plan must be submitted for acceptance by the Compliance Enforcement Authority. In addition, the Compliance Enforcement Authority may conduct a Compliance Audit of, or issue a Remedial Action Directive to, the Registered Entity.

Upon request by NERC, the Regional Entity~~ies~~ will provide to NERC the quarterly status reports and such other information as NERC requests~~,~~. ~~and~~ The Regional Entity will notify NERC when each Mitigation Plan is verified to have been completed.

6.7 Recordkeeping

The Compliance Enforcement Authority will maintain a record containing the following information for each Mitigation Plan:

- Name of Registered Entity.
- The date of the violation.
- Monitoring method by which the violation was detected, i.e., Self-Certification, Self-Report~~ing~~, Compliance Audit, Compliance Investigation, Complaint, etc.
- Date(s) of Notice of Possible Violation and ~~Notice~~notification of Alleged Violation (if applicable).
- Expected and actual completion date of the Mitigation Plan and major milestones.
- Expected and actual completion date for each required action.
- Accepted changes to milestones, completion dates, or scope of Mitigation Plan.
- Registered Entity's completion notice and data submitted as evidence of completion.

7.0 REMEDIAL ACTION DIRECTIVES

The Compliance Enforcement Authority may issue a Remedial Action Directive when such action is immediately necessary to protect the reliability of the Bulk Power System from an imminent or actual threat. A Remedial Action Directive may include, but is not limited to, any of the following: specifying operating or planning criteria, limits, or limitations; requiring specific system studies; defining operating practices or guidelines; requiring confirmation of data, practices, or procedures through inspection testing or other methods; requiring specific

training for personnel; requiring development of specific operating plans; directing a Registered Entity to develop and comply with a plan to remediate a violation; imposing increased auditing or additional training requirements; and requiring a Registered Entity to cease an activity that may constitute a violation of a Reliability Standard.

A Remedial Action Directive may be issued to a Registered Entity at any time, including during any procedures relating to a Possible Violation or an Alleged Violation of a Reliability Standard. The Compliance Enforcement Authority will specify ~~if~~whether a Remedial Action Directive obviates the need for a Mitigation Plan.

Prior to issuing a Remedial Action Directive, the ~~Regional Entity~~Compliance Enforcement Authority shall consult the Reliability Coordinator for the Registered Entity~~, if applicable, to ensure that the Remedial Action Directive is not in conflict with directives issued by the Reliability Coordinator~~.

Any Remedial Action Directive must be provided in a notice to the Registered Entity and shall include: (i) a list of the Possible Violation(s) or Alleged Violation(s) of Reliability Standards that are the basis for issuance of the Remedial Action Directive; (ii) a discussion of the factual basis for the Remedial Action Directive; (iii) the requirements the Compliance Enforcement Authority is imposing to remove the imminent or current threat to the reliability of the Bulk Power System; (iv) a deadline for compliance and a schedule for specific periodic updates to the Compliance Enforcement Authority; (~~i~~v) a statement that the Registered Entity is in a state of noncompliance with the Reliability Standards listed in (i) until the requirements listed in the Remedial Action Directive are completed and certified completed by an officer of the Registered Entity; and (vi) notice to the Registered Entity that failure to comply with the directive by the Required Date may result in further Remedial Action Directives or significantly increased sanctions.

The Compliance Enforcement Authority will cause the notice of the Remedial Action Directive to be delivered to the Registered Entity by (i) electronic mail~~means~~ to the Registered Entity's CEO or equivalent and copied to the Registered Entity's designated contact person for reliability matters and (ii) by a recognized express courier service that provides tracking and verification of delivery to the recipient. The notice will be deemed received on the earlier of the actual date of receipt of the electronic submission or receipt of the express courier~~date of~~ delivery as specified by the express courier service's verification of delivery ~~shall be the date of actual receipt of the Remedial Action Directive~~. The Compliance Enforcement Authority will monitor implementation of Remedial Action Directives as necessary to verify compliance.

The ~~Regional Entity~~Compliance Enforcement Authority will notify NERC within two (2) business days after issuing a Remedial Action Directive and will copy NERC on all correspondence sent to the Registered Entity.

Once the Compliance Enforcement Authority has given the Registered Entity notice of the Remedial Action Directive, the Registered Entity may contest the Remedial Action Directive by giving written notice to the Compliance Enforcement Authority within two (2) business days following the date of actual receipt of notice of the Remedial Action Directive. Due to the urgency of resolving any objections to a Remedial Action Directive, the hearing shall be conducted under the expedited hearing process set forth in Section 1.9 of **Attachment 2, Hearing Procedures**. Notice to contest the Remedial Action Directive and participation in the

hearing process set forth in Section 1.9 of **Attachment 2, Hearing Procedures** shall constitute the Registered Entity's right to appeal the Remedial Action Directive. The Registered Entity may elect not to implement the Remedial Action Directive until the hearing process is completed, or may proceed with implementing the Remedial Action Directive even if it is contesting the Remedial Action Directive.

8.0 REPORTING AND DISCLOSURE

8.1 Information to be Reported

Regional Entities shall promptly~~prepare and~~ submit to NERC electronic ~~all required~~ reports~~,~~ containing current information concerning the information listed below. NERC will work with Regional Entities to specify form, content, timing, and method of submitting reports and notices.

(1) The status of the review and assessment of ~~Registered Entity compliance with Reliability Standards, (2)~~ all Possible Violations, Alleged Violations and Confirmed Violations of Reliability Standards by Registered Entities~~, (3) the status of Possible Violations and Alleged Violations~~,

(2) The potential impact of any Alleged Violation or Confirmed Violation on the reliability of the Bulk Power System,

(4~~3~~) ~~s~~Sanctions and penalties,

(~~5~~4) Remedial Action Directives imposed, ~~and~~

(~~6~~5) Mitigation Plan~~(s) accepted including dates for all required actions and for completion.~~, and

(6) The name of a Regional Entity staff person knowledgeable about the information to serve as a point of contact.

8.2 Reporting to Applicable Governmental Authorities and Public Disclosure

~~Regional Entities shall report all Possible Violations, Alleged Violations and Confirmed Violations to NERC by promptly entering the Possible Violation, Alleged Violation or Confirmed Violation into the NERC compliance reporting and tracking system.~~ Within two (2) business days of receiving a report from a Regional Entity of a Possible Violation, Alleged Violation or Confirmed Violation, NERC shall notify FERC of the Possible Violation, Alleged Violation or Confirmed Violation.~~and,~~

~~w~~Where the report pertains to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, NERC shall ~~also~~ notify such other Applicable Governmental Authority, within two (2) business days of receiving a report of a Possible Violation, Alleged Violation or Confirmed Violation from the Regional Entity; provided, that NERC will not disclose any non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to an Applicable Governmental Authority other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations

placed by FERC on such disclosure~~;~~. ~~and~~ Likewise, NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.

In any notice to, and request for permission to disclose compliance information from, FERC or another Applicable Governmental Authority pursuant to any provision of this Compliance Program, NERC will identify each Applicable Governmental Authority to which it proposes to disclose the information and the specific procedures that will be used for protecting from public disclosure any non-public compliance information that will be transferred to the other Applicable Governmental Authority or Authorities. The provisions of this paragraph do not apply to the provision by NERC to an Applicable Governmental Authority of information that is not directly related to a specific Registered Entity's compliance with a requirement of a Reliability Standard. ~~Such reports shall include information regarding the nature of the Possible Violation, Alleged Violation or Confirmed Violation, the name of the Registered Entity involved, the status of any ongoing review and assessment of the Possible Violation, Alleged Violation, or Confirmed Violation, the name of a Regional Entity staff person knowledgeable about the information to serve as a point of contact, as required by 18 C.F.R. §39.7(b), and, in the case of an Alleged Violation or Confirmed Violation, its potential impact on the reliability of the Bulk Power System.~~

~~Regional Entities shall report to NERC, through the NERC compliance reporting and tracking system, the status of Possible Violations and Alleged Violations, regardless of significance, that have not yet resulted in a Notice of Confirmed Violation or have not completed the hearing process, or for which mitigation activities (including activities being carried out pursuant to a settlement agreement) have not been completed. Regional Entities will ensure the information is current when these reports are provided.~~

~~Regional Entities shall report a Confirmed Violation to NERC at the same time the Notice of Confirmed Violation is issued to the Registered Entity.~~ NERC will publicly post on its Web site each Notice of Penalty, with any Critical Energy Infrastructure Information or other Confidential Information redacted, ~~with the identify of the violator,~~ together with any statement submitted by the Registered Entity, when NERC files the Notice of Penalty with FERC pursuant to Section 5.9.

NERC will provide reports quarterly to FERC and, where a report contains information pertaining to a Registered Entity or to a portion of the Bulk Power System over which another Applicable Governmental Authority has jurisdiction, to such other Applicable Governmental Authority, on the status of all Possible, Alleged and Confirmed Violations for which mitigation activities have not been completed. All such reports to FERC and to other Applicable Governmental Authorities shall be provided in accordance with this Section.~~; provided, that NERC will not disclose any non-public U.S. compliance information that is subject to 18 C.F.R. §39.7(b)(4) to an Applicable Governmental Authority other than FERC without first obtaining permission from FERC for such disclosure and subject to any limitations placed by FERC on such disclosure, and NERC will not disclose non-public non-U.S. compliance information to an Applicable Governmental Authority (including FERC) without first obtaining permission from~~

~~the Applicable Governmental Authority that has jurisdiction over the Registered Entity or portion of the Bulk Power System to which the non-public information pertains and subject to any limitations placed on such disclosure by such Applicable Governmental Authority or by other law of the applicable jurisdiction.~~

9.0 DATA RETENTION AND CONFIDENTIALITY

9.1 Records Management

The Compliance Enforcement Authority records management policy shall provide for a routine and orderly process for the retention and disposal of electronic and paper records related to the Compliance Program, ensure verification of compliance with appropriate business, regulatory, and legal requirements and at a minimum conform to the data retention requirements of the Reliability Standards. The policy shall allow for the maintenance of records as required to implement the Compliance Program.

9.2 Retention Requirements

The Compliance Enforcement Authority records management policy will require that information and data generated or received pursuant to Compliance Program activities, including Compliance Audits, Self-Certifications, Spot Checks~~sing~~, Compliance Investigations, Self-Reports~~sing~~, Periodic Data Submittals, Exception Reporting, and Complaints, as well as a hearing process, will be retained for the longer of (i) five (5) years or (ii) any retention period specified in a Reliability Standard or by FERC or another Applicable Governmental Authority. The obligation to retain information and data commences upon the initiation of the Compliance Program activity that produces the data or information. If the information or data is material to the resolution of a controversy, the retention period for such data shall not commence until after the controversy is resolved.

Upon request from NERC, Regional Entities will provide to NERC copies of such information and data. NERC will retain the information and data in order to maintain a record of activity under the Compliance Program. In providing the information and data to NERC, the Regional Entity shall preserve any mark of confidentiality.

9.3 Confidentiality and Critical Energy Infrastructure Information

9.3.1 Definitions

Information or data generated or received pursuant to Compliance Program activities, including a hearing process, shall be treated in a confidential manner pursuant to the provisions of Section 1500 of the NERC Rules of Procedure. The terms "~~c~~Confidential ~~i~~Information," "~~c~~Confidential ~~b~~Business and ~~m~~Market ~~i~~Information," "~~c~~Critical ~~e~~Energy ~~i~~Infrastructure ~~i~~Information," and "~~c~~Critical ~~i~~Infrastructure" shall have the meanings stated in Section 1501 of the NERC Rules of Procedure.

9.3.2 Protection of Confidential Information

The Compliance Enforcement Authority personnel (including any contractors, consultants and industry subject matter experts) and committee members, and participants in Compliance Program activities shall be informed of, and agree to comply with, Section 1500 of the NERC Rules of Procedure concerning ~~c~~Confidential ~~i~~Information.

9.3.3 Critical Energy Infrastructure Information

The Compliance Enforcement Authority will keep confidential all ~~c~~Critical ~~e~~Energy ~~i~~Infrastructure ~~i~~Information in accordance with Section 1500 of the NERC Rules of Procedure~~s~~. Information deemed to be C~~c~~ritical ~~e~~Energy ~~i~~Infrastructure ~~i~~Information shall be redacted, in accordance with Section 1500 of the NERC Rules of Procedure, and shall not be released publicly.

ATTACHMENT 1

PROCESS FOR NON-SUBMITTAL OF REQUESTED DATA

~~If data, information, or other reports (including Mitigation Plans) requested from a Registered Entity are not received by the Required Date, the Compliance Enforcement Authority may sequentially execute the following steps for each Reliability Standard for which the Compliance Enforcement Authority has requested data, information, or other reports. The Compliance Enforcement Authority however will afford the Registered Entity reasonable opportunity to resolve a difficulty submitting data due to time or format issues.~~

~~Step 1:~~	~~The Compliance Enforcement Authority will issue a follow-up notification to the Registered Entity's designated contact.~~
~~Step 2:~~	~~The Compliance Enforcement Authority will issues a follow-up notification to the Registered Entity's vice president or equivalent responsible for compliance (with a copy to NERC and the Registered Entity's designated contact).~~
~~Step 3:~~	~~The Compliance Enforcement Authority will issue a follow-up notification to the Registered Entity's chief executive officer or equivalent (with a copy to NERC, the Registered Entity's vice president or equivalent responsible for compliance and the Registered Entity's designated contact).~~ ~~A full Compliance Audit may be scheduled at this step.~~
~~Step 4:~~	~~Thirty (30) days after the Required Date, a Reliability Standard violation may be applied at the Severe Violation Severity Level.~~ ~~Step 4 does not apply to Compliance Audits and Mitigation Plan tracking requests.~~

FERC's regulations at 18 C.F.R §39.2(c) provide that each user, owner or operator of the Bulk Power System within the United States (other than Alaska and Hawaii) shall provide FERC, the ERO and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by FERC and set out in the rules of the ERO and each Regional Entity. In order to enforce this requirement, NERC or a Regional Entity may take the steps described in this section where a Registered Entity in the United States fails to provide, in a timely manner and in the form requested, information requested by NERC or a Regional Entity in connection with a compliance monitoring or enforcement process.

If NERC or a Regional Entity has requested data, information or reports from a Registered Entity in connection with a compliance monitoring or enforcement process, and the data, information or report is not received by the Required Date, NERC or the Regional Entity shall sequentially execute the following steps; provided, however, that upon seasonable request from the Registered Entity stating in reasonable detail the basis for the Registered Entity's need for additional time, NERC or the Regional Entity may afford the Registered Entity reasonable additional time to submit the data, information or report due to the scope or difficulty of the request or requirement for data, information or reports, the amount of the data, information or reports requested or required, or the form in which the data, information, or other reports has been requested or is required to be provided.

1. Step 1: NERC or the Registered Entity will issue a notification to the Registered Entity's designated contact for reliability matters, identifying the data, information or report that were requested or required and the Required Date and stating that the Required Date has passed and the Registered Entity should, within five (5) business days, either provide the data, information or report, or contact NERC or the Regional Entity with a proposed date by which the Registered Entity will provide the data, information or report. If NERC or the Regional Entity agrees with the Registered Entity on a revised date by which the Registered Entity will provide the data, information or report, the agreed revised date shall become the revised Required Date.

2. Step 2: If the Registered Entity does not provide a response to the notification in, and in accordance with, Step 1 within five (5) business days, or by a revised date as agreed to in Step 1, NERC or the Regional Entity will issue a notification to the Registered Entity's designated contact for reliability matters, with a copy to the Registered Entity's chief executive officer or equivalent, stating that if the data, information or report is not received within ten (10) business days, NERC or the Regional Entity may (i) implement a compliance monitoring process directed to the Registered Entity, or (ii) apply a Reliability Standard violation at the severe violation severity level against the Registered Entity for the Reliability Standard requirement to which the requested or required data, information or report relates.

3. Step 3: If the Registered Entity fails to produce the requested or required data, information or report in response to the notification in Step 2 within the ten (10) business day cure period set forth in the Step 2 notification, NERC or the Regional Entity may take any action of which the Registered Entity was notified in the Step 2 notification.

ATTACHMENT 2 - HEARING PROCEDURES

TABLE OF CONTENTS

1.1 Applicability, Definitions and Interpretation 1
1.1.1 Procedure Governed 1
1.1.2 Deviation 1
1.1.3 Standards for Discretion 1
1.1.4 Interpretation 2
1.1.5 Definitions 2
1.2 General Provisions including Filing, Service, Transcription and Participation 4
1.2.1 Contents of Filings 4
1.2.2 Form of Filings 4
1.2.3 Submission of Documents 5
1.2.4 Service 6
1.2.5 Computation of Time 7
1.2.6 Extensions of Time 7
1.2.7 Amendments 7
1.2.8 Transcripts 7
1.2.9 Rulings, Notices, Orders and Other Issuances 8
1.2.10 Location of Hearings and Conferences 8
1.2.11 Participant Participation 8
1.2.12 Interventions Are Not Permitted 8
1.2.13 Proceedings Closed to the Public 8
1.2.14 Docketing System 9
1.2.15 Hold Harmless 9
1.3 Initiation of the Hearing Process 9
1.3.1 Registered Entities' Option to Request a Hearing 9
1.3.2 Shortened Hearing Procedure 10
1.4 General Hearing Procedure 12
1.4.1 Notice of Hearing 12
1.4.2 Hearing Officer 12
1.4.3 [HEARING BODY] 13
1.4.4 Interlocutory Review 14
1.4.5 Disqualification 15
1.4.6 Technical Advisor 16
1.4.7 No Ex Parte Communications 16
1.4.8 Appearances 17
1.4.9 Failure to Appear or Exercise Diligence 17
1.4.10 Consolidation of Proceedings 17
1.5 Prehearing Procedure 18
1.5.1 [Intentionally Left Blank] 18
1.5.2 Prehearing Conference 18
1.5.3 Summary Disposition 18
1.5.4 Status Hearings 19
1.5.5 Motions 19
1.5.6 Experts 19
1.5.7 Inspection and Copying of Documents in Possession of Staff 19

1.5.8 Other Discovery Procedures 22
1.5.9 Pre-Evidentiary Hearing Submission of Testimony and Evidence 24
1.5.10 Protective Orders 25
1.5.11 Pre-Evidentiary Hearing Memorandum 26
1.6 Evidentiary Hearing Procedure 26
1.6.1 Evidentiary Hearings 26
1.6.2 Order of Receiving Evidence 26
1.6.3 Opening and Closing Statements 26
1.6.4 Right of Participant to Present Evidence 27
1.6.5 Exhibits 27
1.6.6 Witness Attendance at Evidentiary Hearing 27
1.6.7 Admission of Evidence 27
1.6.8 Evidence that is Part of a Book, Paper or Document 28
1.6.9 Stipulations 28
1.6.10 Official Notice 28
1.6.11 Admissibility of Evidence 29
1.6.12 Offer of Proof 29
1.6.13 Reservation of Evidentiary Ruling 29
1.6.14 Cross-Examination 30
1.6.15 Redirect Examination 30
1.6.16 Examination of Adverse Participant 30
1.6.17 Close of the Evidentiary Record 30
1.7 Post-Evidentiary Hearing Procedure 31
1.7.1 Briefs 31
1.7.2 Other Pleadings 31
1.7.3 Draft Initial Opinions 31
1.7.4 Hearing Officer's Initial Opinion 31
1.7.5 Exceptions 32
1.7.6 Oral Argument 32
1.7.7 Additional Hearings 33
1.7.8 [HEARING BODY] Final Order 33
1.7.9 The Record 34
1.7.10 Appeal 35
1.8 Settlement 35
1.9 Remedial Action Directives 35
1.9.1 Initiation of Remedial Action Directive Hearing 35
1.9.2 Remedial Action Directive Hearing Procedure 35

ATTACHMENT 2 - HEARING PROCEDURES

1.1 Applicability, Definitions and Interpretation

1.1.1 Procedure Governed

(a) The provisions set forth in this **Attachment 2** ("Hearing Procedures") shall apply to and govern practice and procedure before the Compliance Enforcement Authority in hearings in the United States conducted into:

(~~i~~1) whether Registered Entities within the Compliance Enforcement Authority's area of responsibility have violated Reliability Standards, and

(~~ii~~2) if so, to determine the appropriate Mitigation Plans as well as any remedial actions, penalties and/or sanctions in accordance with the NERC *Sanction Guidelines* and other applicable penalty guidelines approved by FERC pursuant to 18 C.F.R. Section 39.7(g)(2).

(b) Any hearing conducted pursuant to these Hearing Procedures shall be conducted before a Hearing Officer and a ~~[HEARING BODY]~~Hearing Body established by the Compliance Enforcement Authority. Where the Hearing Body is comprised, in whole or in part, of industry stakeholders, ~~T~~the composition of the ~~[HEARING BODY]~~Hearing Body, after any recusals or disqualifications, shall be such that no two industry segments may control, and no single industry segment may veto, any decision by the ~~[HEARING BODY]~~Hearing Body on any matter brought before it for decision. Where the Hearing Body is comprised solely of independent members and an independent Hearing Officer, decisions shall require a majority vote.

(c) The standard of proof in any proceeding under these Hearing Procedures shall be by a preponderance of the evidence. The burden of persuasion on the merits of the proceedings shall rest upon the Compliance Staff alleging noncompliance with a Reliability Standard, proposing a penalty, opposing a Registered Entity's Mitigation Plan, or requiring compliance with a Remedial Action Directive.

(d) If a final order has been entered by the Hearing Body, or the Hearing Body has issued a ruling determining that there are no issues to be decided regarding the Alleged Violation, proposed Penalty amount, proposed Mitigation Plan or proposed Remedial Action Directive, or the Registered Entity and the Compliance Enforcement Authority have entered into a settlement agreement resolving the matters that are the subject of the hearing, the hearing shall be terminated by the Hearing Body and no further proceedings shall be conducted before the Hearing Body.

1.1.2 Deviation

To the extent permitted by law, any provision in these Hearing Procedures may be waived, suspended or modified by the Hearing Officer~~, as defined in Paragraph 1.1.5,~~ or the ~~[HEARING BODY]~~Hearing Body, for good cause shown, either upon the Hearing Officer's or the ~~[HEARING BODY]~~Hearing Body's own motion or upon the motion of any Participant.

1.1.3 Standards for Discretion

The Compliance Enforcement Authority's discretion under these Hearing Procedures shall be exercised to accomplish the following goals:

(a) Integrity of the Fact-Finding Process - The principal goal of the hearing process is to assemble a complete factual record to serve as a basis for a correct and legally sustainable ruling, decision or order.

(b) Fairness - Persons appearing in Compliance Enforcement Authority proceedings should be treated fairly. To this end, Participants should be given fair notice and opportunity to present explanations, factual information, documentation and legal argument. Action shall be taken as necessary to eliminate any disadvantage or prejudice to a Participant that would otherwise result from another Participant's failure to act diligently and in good faith.

(c) Independence - The hearing process should be tailored to protect against undue influence from any Person, Participant or interest group.

(d) Balanced Decision-Making - Decisions should be based solely on the facts and arguments of record in a proceeding and by individuals who satisfy the Compliance Enforcement Authority's conflict of interest policy.

(e) Impartiality - Persons appearing before the ~~[HEARING BODY]~~Hearing Body should not be subject to discriminatory or preferential treatment. Registered Entities should be treated consistently unless a reasonable basis is shown in any particular proceeding to depart from prior rulings, decisions or orders.

(f) Expedition - Proceedings shall be brought to a conclusion as swiftly as is possible in keeping with the other goals of the hearing process.

1.1.4 Interpretation

(a) These Hearing Procedures shall be interpreted in such a manner as will aid in effectuating the Standards for Discretion set forth in ~~Paragraph~~Section 1.1.3, and so as to require that all practices in connection with the hearings shall be just and reasonable.

(b) Any ruling, order or decision of the Hearing Officer referenced in these Hearing Procedures shall be made by the Hearing Body where the composition of the Hearing Body consists of independent members and an independent Hearing Officer.

(~~b~~c) Unless the context otherwise requires, the singular of a term used herein shall include the plural and the plural of a term shall include the singular.

(~~c~~d) To the extent that the text of a rule is inconsistent with its caption, the text of the rule shall control.

1.1.5 Definitions

Unless otherwise defined, as used in these Hearing Procedures (i) definitions in Section 1.1 of the NERC Compliance Monitoring and Enforcement Program shall apply, and (ii) the following terms shall have the following meanings:

"Clerk," shall mean the personas designated by the Compliance Enforcement Authority to perform administrative tasks relating to the conduct of hearings as described in these Hearing Procedures.

"Compliance Enforcement Authority's area of responsibility" means the Compliance Enforcement Authority's corporate region. If a Regional Entity is the Compliance Enforcement Authority, the Compliance Enforcement Authority's area of responsibility is shown in Exhibit A to the delegation agreement between the Regional Entity and NERC.

"Critical Energy Infrastructure Information" means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (i) relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) could be useful to a person in planning an attack on critical infrastructure; and (iii) does not simply give the location of the critical infrastructure.

"Critical infrastructure" means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.

"Cybersecurity Incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the Reliable Operation of the Bulk-Power System.

"Director of Compliance" means the Director of Compliance of the Compliance Enforcement Authority or other individual designated by the Compliance Enforcement Authority, who is responsible for the management and supervision of Compliance Staff.

"Document" means, in addition to the commonly understood meaning of the term as information written or printed on paper, any electronically stored information, including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained, and shall be translated by the producing party into reasonably usable form.

"ERO" means the Electric Reliability Organization, currently the North American Electric Reliability Corporation, or any successor organization, certified by FERC pursuant to 18 C.F.R. Section 39.3.

"Evidentiary Hearing" means a hearing at which one or more Participants submits evidence for the record. A Testimonial Hearing is an Evidentiary Hearing, but an Evidentiary Hearing does not necessarily include the presentation of testimony by witnesses in person.

"FERC" means the Federal Energy Regulatory Commission.

"Hearing Body" means the body established or designated by the Compliance Enforcement Authority to conduct hearings and issue final orders concerning disputed compliance matters in accordance with these Hearing Procedures.

"Hearing Officer" means an individual employed or contracted by the Compliance Enforcement Authority and designated by the Compliance Enforcement Authority to preside over hearings conducted pursuant to these Hearing Procedures.

"Participant" means a Respondent and any other Person who is allowed or required by the Hearing Body or by FERC to participate as an intervenor in a proceeding conducted pursuant to these Hearing Procedures, and as used herein shall include the members of the Compliance Staff of the Compliance Enforcement Authority that participate in a proceeding.

"Penalty" as used herein includes all penalties and sanctions, including but not limited to a monetary or non-monetary penalty; a limitation on an activity, function, operation or other appropriate sanction; or the addition of the Registered Entity to a reliability watch list composed of major violators. Penalties must be within the range set forth in the NERC *Sanction Guidelines* approved by FERC pursuant to 18 C.F.R. Section 39.7(g)(2), and shall bear a reasonable relation to the seriousness of a Registered Entity's violation and take into consideration any timely efforts made by the Registered Entity to remedy the violation.

"Person" means any individual, partnership, corporation, limited liability company, governmental body, association, joint stock company, public trust, organized group of persons, whether incorporated or not, or any other legal entity.

"Respondent" means the Registered Entity who is the subject of the Notice of Alleged Violation, contested Mitigation Plan or contested Remedial Action Directive that is the basis for the proceeding, whichever is applicable.

"Staff" or "Compliance Staff" means individuals employed or contracted by the Compliance Enforcement Authority who have the authority to make initial determinations of compliance or violation with Reliability Standards by Registered Entities and associated Penalties and Mitigation Plans.

"Technical Advisor" means any Staff member, third-party contractor, or industry stakeholder who satisfies the Compliance Enforcement Authority's conflict of interest policy and is selected to assist in a proceeding by providing technical advice to the Hearing Officer and/or the ~~[HEARING BODY]~~Hearing Body.

"Testimonial Hearing" means an Evidentiary Hearing at which the witness or witnesses on behalf of one or more Participants appears in person to present testimony and be subject to cross-examination.

1.2 General Provisions including Filing, Service, Transcription and Participation

1.2.1 Contents of Filings

All filings made with ~~[HEARING BODY]~~Hearing Body must contain:

(a) A caption that sets forth the title of the proceeding and the designated docket number or, if the filing initiates a proceeding, a space for the docket number;

(b) A heading that describes the filing and the Participant on whose behalf the filing is made;

(c) The full name, address, telephone number and email address of the Participant or the representative of the Participant making the filing;

(d) A plain and concise statement of any facts upon which the filing is based, which facts shall be supported by citations to the record of the hearing, if available, or other evidence~~documents~~; and

(e) The specific relief sought, which may be in the alternative, and the authority that provides for or otherwise allows the relief sought.

1.2.2 Form of Filings

(a) All filings shall be typewritten, printed, reproduced or prepared using a computer or other word or data processing equipment on white paper 8½ inches by 11 inches with inside text margins of not less than one inch. Page numbers shall be centered and have a bottom margin of not less than ½ inch. Line numbers, if any, shall have a left-hand margin of not less than ½ inch. The impression shall be on one side of the paper only and shall be double spaced; footnotes may be single spaced and quotations may be single spaced and indented.

(b) All pleadings shall be composed in either Arial or Times New Roman font, black type on white background. The text of pleadings or documents shall be at least 12-point. Footnotes shall be at least 10-point. Other material not in the body of the text, such as schedules, attachments and exhibits, shall be at least 8-point.

(c) Reproductions may be by any process provided that all copies are clear and permanently legible.

(d) Testimony prepared for the purpose of being entered into evidence shall include line numbers on the left-hand side of each page of text. Line numbers shall be continuous.

(e) Filings may include schedules, attachments or exhibits of a numerical or documentary nature which shall, whenever practical, conform to these requirements; however, any log, graph, map, drawing, chart or other such document will be accepted on paper larger than prescribed in subparagraph (a) if it cannot be provided legibly on letter size paper.

1.2.3 Submission of Documents

(a) Where to File

Filings shall be made with the Clerk of the Compliance Enforcement Authority located at its principal office. The office will be open during the Compliance Enforcement Authority's regular business hours~~from [*Compliance Enforcement Authority business hours*] local time~~ each day except Saturday, Sunday, legal holidays and any other day declared by the Compliance Enforcement Authority.

(b) When to File

Filings shall be made within the time limits set forth in these Hearing Procedures or as otherwise directed by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body. Filings will be considered made when they are date stamped received by the Clerk. To be timely, filings must be received no later than 5:00 P.M. ~~[*Compliance Enforcement Authority close of business*]~~ local time on the date specified.

(c) How to File

Filings may be made by personal delivery, mailing documents that are properly addressed with first class postage prepaid, or depositing properly addressed documents with a private express courier service with charges prepaid or payment arrangements made. Alternatively, filing by electronic means will be acceptable upon implementation of a suitable and secure system by the Compliance Enforcement Authority.

(d) Number of Copies to File

One original and five exact copies of any document shall be filed. The Clerk will provide each member of the ~~[HEARING BODY]~~Hearing Body with a copy of each filing.

(e) Signature

The original of every filing shall be signed by the Participant on whose behalf the filing is made, either by an attorney of the Participant or, by the individual if the Participant is an individual, by an officer of the Participant if the Participant is not an individual, or if the Participant is Staff, by a designee authorized to act on behalf of Staff. ~~The signature on a filing constitutes a certificate that the signer has read the filing and knows its contents, and that the contents are true to the best of the signer's knowledge and belief.~~

(f) Verification

The facts alleged in a filing need not be verified unless required by these Hearing Procedures, the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body. If verification is required, it must be under oath by a person having knowledge of the matters set forth in the filing. If any verification is made by an individual other than the signer, a statement must be included in or attached to the verification explaining why a person other than the signer is providing verification.

(g) Certificate of Service

Filings shall be accompanied by a certificate of service stating the name of the individuals served, the Participants whose interests the served individuals represent, the date on which

service is made, the method of service and the addresses to which service is made. The certificate shall be executed by the individual who caused the service to be made.

1.2.4 Service

(a) Service List

For each proceeding, the Clerk shall prepare and maintain a list showing the name, address, telephone number, and facsimile number and email address, if available, of each individual designated for service. The Hearing Officer, Director of Compliance and the Registered Entity's compliance contact~~designated agent for service [~~ as registered with the Compliance Enforcement Authority~~],~~ shall automatically be included on the service list. Participants shall identify all other individuals whom they would like to designate for service in a particular proceeding in their appearances or other filings. Participants may change the individuals designated for service in any proceeding by filing a notice of change in service list in the proceeding. Participants are required to update their service lists to ensure accurate service throughout the course of the proceeding. Copies of the service list may be obtained from the Clerk.

(b) By Participants

Subject to the provisions of Section 1.5.10, ~~A~~any Participant filing a document in a proceeding must serve a copy of the document on each individual whose name is on the service list for the proceeding. Unless otherwise provided, service may be made by personal delivery, email, deposit in the United States mail properly addressed with first class postage prepaid, registered mail properly addressed with postage prepaid or deposit with a private express courier service properly addressed with charges prepaid or payment arrangements made.

(c) By the Clerk

The Clerk shall serve all issuances of the Hearing Officer and ~~[HEARING BODY]~~Hearing Body upon the members of the ~~[HEARING BODY]~~Hearing Body and each individual whose name is on the service list for the proceeding. Service may be made by personal delivery, email, deposit in the United States mail properly addressed with first class postage prepaid, registered mail properly addressed with postage prepaid or deposit with a private express courier service properly addressed with charges prepaid or payment arrangements made. The Clerk shall transmit a copy of the record of a proceeding to the ERO at the time ~~it serves~~the Compliance Enforcement Authority transmits to the ERO ~~with~~ either (1) a Notice of Penalty, or (2) a ~~[HEARING BODY]~~Hearing Body final order that includes a Notice of Penalty.

(d) Effective Date of Service

Service by personal delivery or email is effective immediately. Service by mail or registered mail is effective upon mailing; service by a private express courier service is effective upon delivery to the private express courier service. Unless otherwise provided, whenever a Participant has the right or is required to do some act within a prescribed period after the service of a document upon the Participant, four (4) days shall be added to the prescribed period when the document is served upon the Participant by mail or registered mail.

1.2.5 Computation of Time

The time in which any action is required to be done shall be computed by excluding the day of the act or event from which the time period begins to run, and by including the last day of the time period, unless the last day is a Saturday, Sunday, legal holiday or any other day upon which the office of the Compliance Enforcement Authority is closed, in which event it also shall be excluded and the date upon which the action is required shall be the first succeeding day that is not a Saturday, Sunday, legal holiday, or day upon which the office of the Compliance Enforcement Authority is closed.

1.2.6 Extensions of Time

Except as otherwise provided by law, the time by which a Participant is required or allowed to act may be extended by the Hearing Officer or ~~[HEARING BODY]~~Hearing Body for good cause upon a motion made before the expiration of the period prescribed. If any motion for extension of time is made after the expiration of the period prescribed, the Hearing Officer or ~~[HEARING BODY]~~Hearing Body may permit performance of the act if the movant shows circumstances sufficient to justify the failure to act in a timely manner.

1.2.7 Amendments

Amendments to any documents filed in a proceeding may be allowed by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body upon motion made at any time on such terms and conditions as are deemed to be just and reasonable.

1.2.8 Transcripts

(a) A full and complete record of all hearings, including any oral argument, shall be transcribed verbatim by a certified court reporter, except that the Hearing Officer may allow off-the-record discussion of any matter provided the Hearing Officer states the ruling on any such matter, and the Participants state their positions or agreement in relation thereto, on the record. The court reporter shall file a copy of each transcript with the Clerk. Upon receipt of a transcript from the court reporter, the Clerk shall send notice to the Participants stating that a transcript has been filed by the court reporter, the date or dates of the hearing that the transcript records, and the date the transcript was filed with the Clerk.

(b) Unless otherwise prescribed by the Hearing Officer, a Participant may file and serve suggested corrections to any portion of a~~the~~ transcript within fourteen (14)~~thirty-five (35)~~ days from the date of the Clerk's notice that the transcript has been filed with the Clerk ~~on which the relevant portion of the transcript was taken~~, and any responses shall be filed within ten (10) days after service of the suggested corrections. The Hearing Officer shall determine what changes, if any, shall be made, and shall only allow changes that conform the transcript to the ~~truth~~statements being transcribed and ensure the accuracy of the record.

(c) The Compliance Enforcement Authority will pay for transcription services, for a copy of the transcript for the record and for a copy of the transcript for Staff. Any other

Participant shall pay for its own copy of the transcript if it chooses to obtain one and, should any Participant seek to obtain a copy of the transcript on an expedited basis, it shall pay for the expedited transcription services.

1.2.9 Rulings, Notices, Orders and Other Issuances

Any action taken by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body shall be recorded in a ruling, notice, order or other applicable issuance, or stated on the record for recordation in the transcript, and is effective upon the date of issuance unless otherwise specified by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body. All notices of hearings shall set forth the date, time and place of hearing.

1.2.10 Location of Hearings and Conferences

All hearings and oral arguments shall be held at the principal office of the Compliance Enforcement Authority unless the Hearing Officer or ~~[HEARING BODY]~~Hearing Body designates a different location.

1.2.11 Participant Participation

Participants may appear at any hearing via teleconference subject to the approval of the Hearing Officer and, in the event of oral argument, the ~~[HEARING BODY]~~Hearing Body, except as~~that witnesses shall personally appear at the evidentiary hearing if~~ required by ~~Paragraph~~Section 1.6.6. Staff may participate and be represented by counsel in hearings, and shall have the rights and duties of any Participant.

1.2.12 Interventions ~~Are Not Permitted~~

(a) The Respondent(s) and Staff shall be Participants to the proceeding. Unless otherwise authorized by the Hearing Body or by FERC, no other Persons shall be permitted to intervene or otherwise become a Participant to the proceeding.

(b) The Hearing Body may allow a Person to intervene only if the Hearing Body determines that the Person seeking intervention has a direct and substantial interest in the outcome of the Alleged Violation, proposed penalty or sanction, Mitigation Plan, or Remedial Action Directive that is the subject of the proceeding. Examples of a direct and substantial interest in the outcome shall include

(1) that the Person seeking intervention has received a Notice of Alleged Violation or a Remedial Action Directive involving the same Reliability Standard requirement(s) and arising out of the same event or occurrence as the existing Respondent(s) that is the subject of the proceeding, or

(2) that the Person seeking intervention will or may be contractually or legally liable to the original Respondent(s) for payment of all or a portion of the proposed penalty or sanction that is the subject of the proceeding, provided, that after the Person seeking intervention sufficiently demonstrates it will or may be contractually or legally liable for payment of all or a portion of the proposed penalty or sanction to be granted intervention, the Person granted intervention and

the existing Respondents will not be allowed to litigate in the proceeding whether the Person granted intervention is contractually or legally liable for payment of all or a portion of the proposed penalty or sanction or the amount of the proposed Penalty or Sanction for which the Person granted intervention is or may be liable.

That the Person seeking intervention has received a Notice of Alleged Violation for the same Reliability Standard requirement(s) as the original Respondent(s) but arising out of a different event or occurrence; or seeks to intervene to advocate an interpretation of the Reliability Standard requirement(s) or provision(s) of the *Sanction Guidelines*, that are at issue in the proceeding, without more, shall not constitute a direct and substantial interest in the outcome and shall not be grounds on which the Hearing Body may allow the Person to intervene.

(c) A Person seeking intervention shall do so by filing a motion to intervene with the Clerk. The motion shall state the Person's interest in sufficient factual detail to demonstrate that the Person should be allowed to intervene pursuant to Section 1.2.12(b). The motion to intervene shall also state the Person's agreement to maintain the confidential and non-public nature of the hearing, including all pleadings and other documents filed or exchanged in connection with the request for intervention. Any facts alleged in, or offers of proof made in, the motion to intervene shall be supported by affidavit or verification.

(d) The Clerk shall promptly provide copies of the motion to intervene to the Hearing Officer and the Participants. The Hearing Officer shall promptly set a time period, not to exceed seven (7) days, within which the Participants may file responses to the motion to intervene. Within seven (7) days following the end of the response period, the Hearing Officer shall issue a recommendation to the Hearing Body as to whether or not the motion to intervene should be granted.

(e) The Hearing Body may, within seven (7) days following the date of the Hearing Officer's recommendation, issue a decision granting or denying the motion to intervene. If the Hearing Body does not issue a decision granting or denying the motion to intervene within seven (7) days following the date of the Hearing Officer's recommendation, the Hearing Officer's recommendation shall become the decision of the Hearing Body and the motion to intervene shall be deemed granted or denied by the Hearing Body in accordance with the Hearing Officer's recommendation.

(f) The Hearing Officer, on motion of a Participant or on his or her own motion, or the Hearing Body, on recommendation by the Hearing Officer or its own motion, may stay or suspend the proceeding while a request to intervene, including a request to intervene filed directly with FERC, and including any appeal of the grant or denial of the request to intervene, is being resolved.

(g) A Person allowed to intervene and become a Participant to a proceeding shall be designated as a Respondent and deemed to be aligned with the existing Respondent(s), unless the Hearing Body, in the decision granting intervention, states that the Person allowed to intervene shall be deemed to be aligned with another Participant to the proceeding.

(h) A Person allowed to intervene and become a Participant to a proceeding is required to take the record and the procedural status of the proceeding as it stands on the date the Person's motion to intervene is granted by the Hearing Body.

(i) A Person may appeal a decision of the Hearing Body denying the Person's motion to intervene, and the Compliance Staff, the Respondent or any other Participant may appeal a decision granting or denying a motion to intervene, in accordance with Section 414 of the NERC Rules of Procedure. A notice of appeal shall be filed with the NERC director of enforcement no later than seven (7) days following the date of the decision of the Hearing Body granting or denying the motion to intervene.

1.2.13 Proceedings Closed to the Public

No hearing, oral argument or meeting of the ~~[HEARING BODY]~~Hearing Body shall be open to the public, and no notice, ruling, order or any other issuance of the Hearing Officer or ~~[HEARING BODY]~~Hearing Body, or any transcript, made in any proceeding shall be publicly released unless the ERO (within the U.S., in accordance with the authorization previously granted by FERC to release information about a non-public proceeding) or FERC (in the case of U.S.-related information) or another Applicable Governmental Authority (in the case of non-U.S.-related information) determines that public release is appropriate. Only the members of the ~~[HEARING BODY]~~Hearing Body, the Participants, the Hearing Officer and the Technical Advisors, if any, shall be allowed to participate in or obtain information relating to a proceeding.

1.2.14 Docketing System

The Clerk shall maintain a system for docketing proceedings. A docketed proceeding shall be created upon the filing of a request for a hearing~~issuance of a Notice of Alleged Violation~~. Unless NERC provides a different docketing system that will be used uniformly by the Compliance Enforcement Authorities, docket numbers shall be assigned sequentially beginning with a two digit number that relates to the last two digits of the year in which the docket is initiated, followed by a dash ("-"), followed by the letters "[RE]", followed by a dash ("-"), followed by a four digit number that will be "0001" on January 1 of each calendar year and ascend sequentially until December 31 of the same calendar year.

1.2.15 Representations Deemed to be Made in All Pleadings

A Participant presenting any pleading to the Hearing Officer or Hearing Body shall be deemed to certify that to the best of the Participant's knowledge, information and belief, formed after and based on an inquiry that is reasonable under the circumstances:

(a) the factual allegations set forth in the pleading have or will have support in the evidence or the Participant believes they will have support in the evidence after reasonable opportunity for further investigation or discovery;

(b) the denials in the pleading of factual allegations made by another Participant are warranted by or will be warranted by the evidence or, if specifically so identified, are reasonably based on belief or on a lack of information;

(c) the claims, defenses and other contentions set forth in the pleading are warranted based on the applicable Reliability Standard requirement(s) or Rules of Procedure provisions; and

(d) the pleading is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of the hearing or the cost incurred by any Participant.

1.2.~~15~~16 Hold Harmless

A condition of a Participant invoking these Hearing Procedures and participating in a hearing is that the Participant agrees that the Compliance Enforcement Authority, including without limitation its members, board of directors or trustees, compliance committee, any other committees or subcommittees, Staff, contracted employees, ~~[HEARING BODY]~~Hearing Body members, Hearing Officers and Technical Advisors, shall not be liable, and shall be held harmless against the consequences of, or any action or inaction arising out of, the hearing process, or of any agreement reached in resolution of a dispute or any failure to reach agreement as a result of a proceeding. This "hold harmless" provision does not extend to matters constituting gross negligence, intentional misconduct or breach of confidentiality.

1.3 Initiation of the Hearing Process

1.3.1 Registered Entity's Option to Request a Hearing

(a) Except when contesting a Remedial Action Directive pursuant to ~~s~~Section 1.9 of these Hearing Procedures, a Registered Entity may file a statement, in accordance with Section 1.3.1(e), with the Compliance Enforcement Authority requesting a hearing if either:

(1~~a~~) The Registered Entity files a response to a Notice of Alleged Violation that contests either the Alleged Violation, the proposed Penalty, or both; or

(2~~b~~) The Compliance Staff submits to the Registered Entity a statement rejecting the Registered Entity's proposed revised Mitigation Plan submitted after Compliance Staff rejected the Registered Entity's initial proposed Mitigation Plan.

(b) A Registered Entity must file its hearing request within forty (40) days after

(~~i~~1) the Registered Entity files its response to the Notice of Alleged Violation; or

(~~ii~~2) the Compliance Staff submits to the Registered Entity its statement identifying a disagreement with the Registered Entity's proposed Mitigation Plan, whichever is applicable.

(c) If the Registered Entity does not file a hearing request within the time period set forth in this ~~Paragraph~~Section, then the Registered Entity will be deemed to have agreed and waived any objection to the proposed Penalty, the Alleged Violation or the Compliance Staff's rejection of the revised Mitigation Plan, whichever is applicable.

(d) In accordance with Section 5.3 of the Compliance Program, ~~Either~~ a Notice of Alleged Violation issued to a Registered Entity or a Staff statement setting forth its rejection of a Registered Entity's proposed revised Mitigation Plan shall clearly state that the Registered Entity has the option to contest the Alleged Violation, proposed Penalty, or both, or the Compliance Staff's rejection of the proposed revised Mitigation Plan, using either the shortened hearing procedure pursuant to Section 1.3.4~~Paragraph 1.3.2~~ or the general~~full~~ hearing procedure described in Sections 1.4 to 1.7. ~~If the Registered Entity files a hearing request within the requisite time period, it shall state within its hearing request whether it requests the shortened hearing procedure pursuant to Paragraph 1.3.2 or the full hearing procedure described in Sections 1.4 to 1.7. If the Registered Entity (or any Respondent if there are more than one Respondent) requests the full hearing procedure, the full hearing procedure shall apply. If the Registered Entity (or all Respondents if there are more than one Respondent) requests the shortened hearing procedure, Compliance Staff and any other Participant shall submit a filing within five (5) days of the Registered Entity's hearing request that states whether Staff or such other Participant agrees to use the shortened hearing procedure. If Staff or another Participant makes a filing requesting the full hearing procedure, then the full hearing procedure shall apply; otherwise the shortened hearing procedure requested by the Registered Entity or Entities shall be used. Once either the full or shortened hearing procedure has been selected, the Participants shall not be allowed to revert to the non-selected hearing procedure unless the Participants mutually agree.~~

(e) The Registered Entity's statement requesting a hearing shall:

(1) contain a plain and concise statement of the facts and arguments supporting the Registered Entity's position, as applicable, that it did not violate the Reliability Standard requirement(s) set forth in the Notice of Alleged Violation, that the proposed penalty or sanction is too high and should be reduced, or that the Registered Entity's proposed Mitigation Plan should be approved;

(2) state the relief that the Registered Entity requests the Hearing Body to grant; and

(3) state whether the Registered Entity requests the shortened hearing procedure or the general hearing procedure.

The Registered Entity's statement may set forth two or more alternative grounds on which the Registered Entity bases its position, as applicable, that it did not violate the Reliability Standard requirement(s) set forth in the Notice of Alleged Violation, that the proposed penalty or sanction is too high and should be reduced, or that the Registered Entity's proposed Mitigation Plan should be approved.

(f) If the Registered Entity (or any Respondent if there are more than one Respondent) requests the general hearing procedure, the general hearing procedure shall apply. If the Registered Entity (or all Respondents if there are more than one Respondent) requests the shortened hearing procedure, Compliance Staff and any other Participants shall submit a filing within five (5) days of the Registered Entity's hearing request that states whether Staff or such other Participant agrees to use the shortened hearing procedure. If Staff or another Participant makes a filing requesting the general hearing procedure, then the general hearing procedure shall apply; otherwise the shortened hearing procedure requested by the Registered Entity or Entities shall be used. Once either the general or shortened hearing procedure has been selected, the

Participants shall not be allowed to revert to the non-selected hearing procedure unless the Participants mutually agree.

(g) A Registered Entity shall attach to a request for hearing whichever of the following are applicable:

(1a) The Registered Entity's Self-Report~~ing~~ of a violation;

(2b) The Notice of Alleged Violation and the Registered Entity's response thereto; and/or

(~~c~~3) The Registered Entity's proposed revised Mitigation Plan and the Compliance Staff's statement rejecting the proposed revised Mitigation Plan.

1.3.2 Compliance Staff's Response to Request for Hearing

(a) If the Registered Entity's request for hearing requests that the shortened hearing procedure be used, the Compliance Staff shall file a response stating whether it agrees to the use of the shortened hearing procedure.

(b) If the Registered Entity's request for hearing requests that the Registered Entity's proposed revised Mitigation Plan should be approved, the Compliance Staff shall file a response stating the Compliance Staff's position as to why the Registered Entity's proposed revised Mitigation Plan should not be approved and setting forth any additional terms that the Compliance Staff believes should be included in the Mitigation Plan.

(c) If the Registered Entity's request for hearing does not request that the shortened hearing procedure be used and does not request that the Registered Entity's proposed revised Mitigation Plan should be approved, the Compliance Staff may, but is not required to, file a response stating, as applicable, the basis for the Compliance Staff's position that the Registered Entity violated the Reliability Standard requirement(s) specified in the Notice of Alleged Violation or that the proposed penalty or sanction is appropriate under the *Sanction Guidelines* and should not be reduced.

(d) Any response by the Compliance Staff required or permitted by this Section shall be filed within fifteen (15) days after the date the request for hearing was filed, unless the Hearing Officer or Hearing Body allows a longer time to file the response.

1.3.3 Notice of Hearing

(a) The Clerk shall issue a notice of hearing not less than sixteen (16) days, and not more than twenty-one (21) days, after the Registered Entity files its request for hearing.

(b) The notice of hearing shall state whether the shortened hearing procedure or the general hearing procedure will be used.

(c) The notice of hearing shall identify the Hearing Officer and the date, time and place for the initial prehearing conference.

(1) If the shortened hearing procedure is to be used, the initial prehearing conference shall be set for a date within seven (7) days following the date of the notice of hearing.

(2) If the general hearing procedure is to be used, the initial prehearing conference shall be set for a date within fourteen (14) days following the date of the notice of hearing.

1.3.~~2~~4 Shortened Hearing Procedure

The shortened hearing procedure shall be as set forth in this ~~Paragraph~~Section. The rules applicable to the general~~full~~ hearing procedure shall apply to the shortened hearing procedure unless the context of such a rule is inconsistent with the procedure set forth in this Section~~Paragraph~~ or otherwise renders it inapplicable to the shortened hearing procedure. The rules concerning ex parte communications in Section~~Paragraph~~ 1.4.7 are hereby expressly made applicable to the shortened hearing procedure under this Section~~Paragraph~~.

The ~~[HEARING BODY]~~Hearing Body shall~~may~~ utilize a Hearing Officer to preside over the shortened hearing procedure in accordance with Section~~Paragraph~~ 1.4.2. But, no Testimonial~~evidentiary~~ ~~h~~Hearing will be held in the shortened hearing procedure and the Participants will not present witness testimony or file briefs, except that briefs on exceptions and briefs in reply to exceptions may be allowed pursuant to ~~Subparagraph~~subsection (g). Instead, the following events shall take place within the following periods:

(a) The initial prehearing conference shall be held within seven (7) days after the date on which the notice of hearing is issued. In addition to any other matters set forth in ~~Paragraph~~Section 1.5.2 that may apply, the initial prehearing conference will be used to develop a schedule for the preparation and submission of comments in accordance with ~~Subparagraphs~~subsections (c) through (e).

(b) Within ~~five (5)~~ten (10) days after the date on which the notice of hearing is issued, Staff shall make documents available to the Registered Entity for inspection and copying pursuant to Section~~Paragraph~~ 1.5.7.

(c) Within twenty-one (21) days after the initial prehearing conference, the Staff shall file:

(1) initial comments stating Staff's position on all issues and the rationale in support of its position, including all factual and legal argument;

(2) all documents that Staff seeks to introduce in support of its position that have not already been submitted in the proceeding; and

(3) a verification attesting to the truthfulness of the facts alleged in the filing.

(d) Within fourteen (14) days of Staff's initial comment filing pursuant to ~~Subparagraph~~subsection (c), the Registered Entity shall file:

(1) responsive comments stating the Registered Entity's position on all issues and the rationale in support of its position, including all factual and legal argument, which comment also may respond to Staff's initial comments;

(2) all documents that the Registered Entity seeks to introduce in support of its position that have not already been submitted in the proceeding; and

(3) a verification attesting to the truthfulness of the facts alleged in the filing.

(e) Within seven (7) days after the Registered Entity's responsive comment filing pursuant to ~~Subparagraph~~subsection (d), Staff shall file reply comments that shall be limited in scope to responding to the Registered Entity's responsive comments and be supported by a verification attesting to the truthfulness of the facts alleged in the filing. Staff shall not submit any additional documents in support of its position as part of this filing except upon motion and good cause shown. If Staff is allowed to file additional documents in support of its position based upon such a motion, the Registered Entity shall have the right to file additional documents in support of its position that are responsive to the additional documents that Staff is allowed to file provided that any additional Registered Entity filing also shall be verified.

(f) The Hearing Officer shall issue an initial opinion within twenty-one (21) days after the Staff's reply comments filing or any additional filing by the Registered Entity pursuant to ~~Subparagraph~~subsection (e).

(g) If either Participant requests, the Hearing Officer shall allow each Participant to file, within seven (7) days after the Hearing Officer's initial opinion, exceptions to the Hearing Officer's initial opinion in a brief designated "brief on exceptions" in accordance with Section~~Paragraph~~ 1.7.5 and within seven (7) days thereafter, a reply brief designated "Brief in Reply to Exceptions."

(h) The ~~[HEARING BODY]~~Hearing Body shall strive, but is not required, to issue a final order within ~~ninety (90)~~one hundred twenty (120) days of the notice of hearing.

The Hearing Officer or ~~[HEARING BODY]~~Hearing Body may modify any time period set forth within this Paragraph as warranted by the circumstances but it will be the objective of the ~~[HEARING BODY]~~Hearing Body to issue the final order within ~~ninety (90)~~one hundred twenty (120) days of the notice of hearing.

1.4 General Hearing Procedure

1.4.1 ~~Notice of Hearing~~[Intentionally Left Blank]

~~Within seven (7) days of a Registered Entity requesting a hearing pursuant to Paragraph 1.3, the Clerk shall issue a notice of hearing in the docket. The notice of hearing shall identify the Hearing Officer, if designated at that time, and the date, time, and place for the prehearing~~

~~conference, which should occur no later than fourteen (14) days after the notice of hearing is issued.~~ [Blank.]

1.4.2 Hearing Officer

(a) The Compliance Enforcement Authority ~~may~~shall utilize a Hearing Officer to preside over each hearing conducted pursuant to these Hearing Procedures, provided that the Hearing Officer's actions shall be subject to the authority of the ~~[HEARING BODY]~~Hearing Body as set forth in ~~Paragraph~~Section 1.4.3. Members of the ~~[HEARING BODY]~~Hearing Body may attend any aspect of the hearing.

(b) The ~~[HEARING BODY] may delegate to the~~ Hearing Officer is responsible for~~authority over~~ the conduct of the hearing, including administering the hearing from the initial prehearing conference through the issuance of the Hearing Officer's initial opinion~~, and~~ any administrative hearing functions thereafter, and ~~the responsibility for~~ submission of the matter to the ~~[HEARING BODY]~~Hearing Body for final decision through the presentation to the ~~[HEARING BODY]~~Hearing Body of an initial opinion. The Hearing Officer shall have those duties and powers necessary to those ends, consistent with and as further enumerated in these Hearing Procedures, including the following:

(1) To administer oaths and affirmations;

(2) To schedule and otherwise regulate the course of the hearing, including the ability to call to recess, reconvene, postpone or adjourn a hearing;

(3) Consistent with any timing or deadline requirements imposed by these Hearing Procedures or by applicable law, to separate any issue or group of issues from other issues in a proceeding and treat such issue(s) as a separate phase of the proceeding;

(4) Consistent with any timing or deadline requirements imposed by these Hearing Procedures or by applicable law, to modify any time period, if such modification is in the interest of justice and will result in no undue prejudice to any other Participant;

(5) To supervise and issue orders concerning discovery;

(6) To conduct prehearing conferences, status hearings and E~~e~~videntiary ~~h~~Hearings;

(7) To hear argument on all objections, motions and other requests, and to rule upon all objections, motions and other requests that do not result in the final determination of the proceeding;

(8) To rule on and receive evidence;

(9) To call upon a Participant to produce further evidence that is material and relevant to any issue;

(10) To issue protective orders pursuant to Section~~Paragraph~~ 1.5.10;

(11) To issue initial opinions; and

(12) To ensure that hearings are conducted in a full, fair and impartial manner, that order is maintained and that unnecessary delay is avoided in the disposition of the proceedings.

(c) ~~If the [HEARING BODY] uses a Hearing Officer to preside over a hearing, the [HEARING BODY]~~The Compliance Enforcement Authority shall disclose the~~ identity,~~ employment history and professional affiliations of the Hearing Officer within two (2) days of the Hearing Officer's assignment to the proceeding, and Participants to the hearing may raise objections to the Hearing Officer's participation in accordance with Section~~Paragraph~~ 1.4.5.

1.4.3 ~~[HEARING BODY]~~Hearing Body

(a) The composition of the Hearing Body, after any recusals or disqualifications, shall be such that no two industry segments may control, and no single industry segment may veto, any decision of the Hearing Body on any matter brought before it for decision.

(b) The ~~[HEARING BODY]~~Hearing Body is vested with the authority to issue a final order resolving the issue(s) in all cases. To that end:

(1) Upon receiving a filing by a Participant, ~~T~~the Clerk shall promptly send a notice to the members of the ~~[HEARING BODY]~~Hearing Body identifying the date of the filing and the Participant making the filing and briefly describing the nature of the filing. Any member of the Hearing Body may request of, and shall receive from, the Clerk, a copy of any filing by a Participant. ~~shall receive all filings in a hearing, including but not limited to all issuances of the Hearing Officer, all motions and responses thereto, and all written comments, testimony and evidence.~~ The Hearing Body shall not receive documents made available by Staff for inspection and copying by the Respondent, or other responses to discovery between the Participants, unless such documents are placed into the record pursuant to ~~Paragraph~~Section 1.6.7.

(2) The Clerk shall send all issuances of the Hearing Officer to the members of the Hearing Body.

(~~2~~3) The ~~[HEARING BODY]~~Hearing Body or any individual member thereof may, but is not required to, attend any prehearing conference, status hearing or E~~e~~videntiary ~~h~~Hearing, and/or to submit questions to the Hearing Officer to submit to a Participant or any witness at any ~~such~~ hearing. At any prehearing conference or hearing attended by a member of the Hearing Body, any member of the Hearing Body may ask questions directly of any Participant or witness.

(4~~3~~) The ~~[HEARING BODY]~~Hearing Body shall have the same authority as the Hearing Officer, as set forth in these Hearing Procedures, to require the Participants or any individual Participant to: (i) address a specific issue in testimony, evidence or briefs; (ii) present oral argument on an issue; (iii) file pre-~~e~~Evidentiary ~~h~~Hearing memorandums; or (iv) produce further evidence that is

material and relevant to any issue. To this end, the ~~[HEARING BODY]~~Hearing Body shall be entitled to issue questions or requests for information to any Participant or any witness at any time until the issuance of a final order.

(5~~4~~) To the extent that the ~~[HEARING BODY]~~Hearing Body disagrees with any issuance or ruling of the Hearing Officer, it may, on its own motion or upon petition for interlocutory review meeting the requirements of Section~~Paragraph~~ 1.4.4, reverse or modify the issuance or ruling in whole or in part, or take any other action as may be appropriate.

(6~~5~~) The ~~[HEARING BODY]~~Hearing Body shall resolve the issue(s) in every hearing through the issuance of a final order. In issuing a final order, the ~~[HEARING BODY]~~Hearing Body shall consider the Hearing Officer's initial opinion but shall have the authority to reject, modify or approve the initial opinion in whole or in part.

1.4.4 Interlocutory Review

(a) A Participant shall be allowed to seek interlocutory review by the ~~[HEARING BODY]~~Hearing Body of any ruling of the Hearing Officer where the ruling for which interlocutory review is sought presents an extraordinary circumstance which makes prompt review necessary to prevent prejudice to a Participant's ability to present its position in the proceeding. Failure to seek such review shall not operate as a waiver of any objection to such ruling.

(b) Unless good cause is shown or unless otherwise ordered by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body, the Participant seeking review shall file a petition for interlocutory review within fourteen (14) days after the date of the action that is the subject of the petition. The petition shall contain, in a separately identified section, a demonstration that the ruling for which interlocutory review is sought presents an extraordinary circumstance which makes prompt review necessary to prevent prejudice to the Participant's ability to present its position in the proceeding. The petition shall be filed with any offer of proof and supported by references to the record, or by affidavit if based on facts that do not appear ~~of~~in the record. Responses to petitions for interlocutory review shall be filed within seven (7) days after service of the petition. No replies to responses ~~are~~shall be allowed.

(c) The Hearing Officer shall file a report to the ~~[HEARING BODY]~~Hearing Body within fourteen (14) days from the filing of the petition. The Hearing Officer's report shall set forth the relevant facts and other background information relating to the ruling on which interlocutory review is sought, the basis for the Hearing Officer's ruling, a summary of the Participants' arguments on the petition for interlocutory review, and the recommendation of the Hearing Officer for the disposition of the petition by the ~~[HEARING BODY]~~Hearing Body.

(d) On review of a Hearing Officer's ruling, the ~~[HEARING BODY]~~Hearing Body may affirm or reverse the ruling in whole or in part, and may take any other just and reasonable action with respect to the ruling, such as declining to act on an interlocutory basis. The ~~[HEARING BODY]~~Hearing Body may reject the petition for interlocutory review on the grounds that the ruling for which review is sought does not present an extraordinary circumstance which makes

prompt review necessary to prevent prejudice to a Participant's ability to present its position in the proceeding, without considering or ruling on the substance of the petitioner's arguments.

(e) Issuance of a ruling on a petition for interlocutory review shall require (i) a quorum (as defined in Section~~Paragraph~~ 1.7.8) of the ~~[HEARING BODY]~~Hearing Body, and (ii) majority vote of the members of the ~~[HEARING BODY]~~Hearing Body voting on the final order (which number of members voting shall not be less than a quorum). Petitions to rehear or reconsider the ~~[HEARING BODY'S]~~Hearing Body's action taken on interlocutory review shall not be allowed. Filing and disposition of a petition for interlocutory review of a ruling of the Hearing Officer shall not suspend or otherwise delay a hearing or any other scheduled dates in the proceeding except as authorized by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body based on a finding of exceptional circumstances.

(f) A non-Participant that has been ordered by the Hearing Officer pursuant to Section~~paragraph~~ 1.5.8 to produce or provide documents, information or testimony, and has failed to obtain the relief sought from the Hearing Officer through filing objections to or a motion to quash the order, shall also be entitled to seek interlocutory review by the ~~[HEARING BODY]~~Hearing Body of the Hearing Officer's order, with respect to (i) whether the non-Participant is within the class of Persons subject to such orders pursuant to Section~~paragraph~~ 1.5.8, and (ii) the reasonableness of the Hearing Officer's order to produce or provide document, information or testimony.

1.4.5 Disqualification

(a) A Hearing Officer, Technical Advisor or member of the ~~[HEARING BODY]~~Hearing Body shall recuse himself or herself from a proceeding if participation would violate the Compliance Enforcement Authority's applicable conflict of interest policy.

(b) Any Participant may file a motion to disqualify or for recusal of a Hearing Officer, Technical Advisor or member of the ~~[HEARING BODY]~~Hearing Body from a proceeding on grounds of a conflict of interest, an ex parte communication prohibited by ~~s~~Section 1.4.7, or the existence of other circumstances that could interfere with the impartial performance of his or her duties. The Participant shall set forth and support its alleged grounds for disqualification by affidavit. A motion for disqualification shall be filed within fifteen (15) days after the later of: (1) the time when the Participant learns of the facts believed to constitute the basis for disqualification; or (2) the time when the Participant is notified of the assignment of the Hearing Officer or Technical Advisor.

(c) The Hearing Officer shall issue a proposed ruling for the ~~[HEARING BODY]~~Hearing Body's consideration upon the filing of a motion for disqualification unless the Hearing Officer is the subject of the motion. The ~~[HEARING BODY]~~Hearing Body, without the participation of any member who is the subject of the motion, shall issue a final ruling on the motion. If the Hearing Officer ~~is recused~~recuses himself or herself or is disqualified, the ~~[HEARING BODY]~~Hearing Body will appoint a replacement Hearing Officer. To ensure fairness to the Participants and expedite completion of the proceeding when a replacement Hearing Officer is appointed after a hearing has commenced, the replacement Hearing Officer may recall any witness or may take other steps necessary to ensure~~certify~~ familiarity with any part or all of the record.

(d) If a quorum (as defined in Section~~Paragraph~~ 1.7.8) of the ~~[HEARING BODY]~~Hearing Body does not remain after any recusals and rulings on motions for disqualification, then the Compliance Enforcement Authority shall appoint at least the number of ~~a~~ new member~~(s)~~ to the ~~[HEARING BODY]~~Hearing Body necessary to create a quorum~~.~~. ~~which~~The new member(s) shall serve on the ~~[HEARING BODY]~~Hearing Body through the conclusion of the proceeding but not thereafter. ~~The Compliance Enforcement Authority shall only appoint the number of new members as are necessary to create a quorum.~~ Any new member of the ~~[HEARING BODY]~~Hearing Body shall be subject to the provisions applicable herein to all ~~[HEARING BODY]~~Hearing Body members.

1.4.6 Technical Advisor

(a) The Hearing Officer and/or the ~~[HEARING BODY]~~Hearing Body may elect to use one or more Technical Advisors to assist in any proceeding. Such an election may be made at any time during the course of a proceeding. Any Staff member who serves as a Technical Advisor shall not have been involved in or consulted at any time in regard to any Compliance Staff investigation, determination of a Possible Violation, Alleged Violation or Penalty, or assessment of a Registered Entity's proposed Mitigation Plan that resulted in the proceeding in which technical advice would be rendered, and shall not be a member of Staff participating in the proceeding on which such technical advice would be rendered.

(b) If the Hearing Officer or ~~[HEARING BODY]~~Hearing Body uses a Technical Advisor to assist in any hearing, the Hearing Officer or ~~[HEARING BODY]~~Hearing Body shall disclose the identity, employment history and professional affiliations of the Technical Advisor within two (2) days of the Technical Advisor's assignment to the proceeding, and Participants to the hearing may raise objections to the Technical Advisor's participation in accordance with Section~~Paragraph~~ 1.4.5.

1.4.7 No Ex Parte Communications

(a) Once a Registered Entity requests a hearing pursuant to ~~Paragraph~~Section 1.3.1:

(1) neither the ~~[HEARING BODY]~~Hearing Body, the Hearing Officer, nor the Technical Advisor(s), if any, may communicate either directly or indirectly with any Person concerning any issue in the proceeding outside of the hearing process; except that

(2) the ~~[HEARING BODY]~~Hearing Body, the Hearing Officer, and the Technical Advisor(s), if any, may communicate outside of the hearing process either directly or indirectly with a Participant or a Participant's representative:

(A) in writing if the writing is simultaneously provided to all Participants; or

(B) orally if a representative for every Participant is present in person or by telephone;

(C) subject to the requirement that the substance of any ruling on any issue discussed shall be memorialized on the record or by the issuance of a

notice or ruling, and that any Participant objecting to the ruling shall have the opportunity to state its objection on the record.

(b) Exceptions

(1) The proscription in ~~Subparagraph~~subsection (a)(1) does not prohibit members of the Compliance Staff from communicating with the Registered Entity, and representatives, agents or employees thereof on any topic, provided that any member of the Compliance Staff involved in any such communication relating to the subject matter of the proceeding may not be, and may not subsequently serve as, a Technical Advisor.

~~c~~(2) The proscription in ~~Subparagraph~~subsection (a)(1) ~~also~~ does not prohibit communications between or among members of the ~~[HEARING BODY]~~Hearing Body, the Hearing Officer and any Technical Advisor.

(3) The proscription in subsection (a)(1) does not prohibit communications between the Hearing Officer or members of the Hearing Body to the Clerk for the purpose of transmitting documents, giving instructions to the Clerk, or discussing scheduling and other procedural matters relating to the proceeding.

(4) The proscription in subsection (a)(1) does not prohibit communications between or among the Clerk, the Hearing Body and representatives of the Compliance Enforcement Authority for purposes of establishing the hearing forum.

(~~d~~c) Any member of the ~~[HEARING BODY]~~Hearing Body, the Hearing Officer or any Technical Advisor who receives or who makes or knowingly allows~~causes to be made~~ a communication prohibited by this Section~~Paragraph~~ shall, within seven (7) days of the communication, file and serve on the Participants in the proceeding a notice of ex parte communication setting forth the date, time and place of communication, a summary of the substance and nature of the communication and all responses thereto, and a list of each Person who made or received the communication and, if the communication or any response thereto was in writing, a copy of the written communication shall be attached.

1.4.8 Appearances

(a) Participants shall file written appearances within seven (7) days after the notice of hearing is issued. A Participant's written appearance shall identify the name(s) of each individual authorized to represent the Participant in the proceeding exclusive of witnesses. An individual may appear on his or her own behalf. A corporation, limited liability company, association, partnership or governmental body may appear by any bona fide officer or designee who has the authority to act on behalf of the Participant. A Participant also may appear by an attorney.

(b) A Participant's written appearance shall state, with respect to each individual that the Participant identifies for service, the individual's name, address, telephone number, and facsimile number and email address, if available, where service shall be made.

A Participant may withdraw any individual from the Participant's representation or otherwise change the identity of individuals authorized to represent the Participant in a proceeding by filing a notice of a change in service list.

(c) Any attorney appearing on behalf of a Participant shall be licensed to practice law and in good standing before the Supreme Court of the United States or the highest court of any State, territory of the United States or the District of Columbia. All representatives appearing before the Hearing Body or Hearing Officer shall conform to the standards of ethical conduct required of practitioners before the courts of the United States.

(d) Individuals representing Participants in any hearing also shall enter their appearances at the beginning of the hearing by stating their names, addresses, telephone numbers and email addresses orally on the record.

1.4.9 Failure to Appear or Exercise Diligence

The failure of any Participant to appear during any hearing without good cause and without notification may be grounds for dismissal or deciding against the interests of such Participant.

1.4.10 Consolidation of Proceedings

(a) In the event that more than one Registered Entity receives a Notice of Alleged Violation for the same event or occurrence~~transaction~~, and each Registered Entity selects the general~~full~~ hearing procedure described in Sections 1.4 to 1.7, the Hearing Body on its own motion or on motion of a Participant may exercise its discretion to examine the actions of all such Registered Entities in a single proceeding as long as an initial opinion has not been rendered by the Hearing Officer pursuant to Section 1.7.4 in any proceeding to be consolidated.

(b) A Participant may file a motion ~~pursuant to Paragraph 1.5.5~~ to consolidate into a single proceeding Allegations of Violations of different Reliability Standards against a single Respondent, and related contests of Penalties or Mitigation Plans, arising out of the same event or occurrence~~transaction~~. Such consolidation may be allowed in the discretion of the Hearing Officer or ~~[HEARING BODY]~~Hearing Body, as applicable.

1.5 Prehearing Procedure

1.5.1 [Intentionally left blank]

1.5.2 Prehearing Conferences

(a) The Hearing Officer shall hold at least one ~~The purpose of the~~ prehearing conference, which may be the initial prehearing conference or a subsequently scheduled prehearing conference, for the following purposes ~~shall be to~~:

(1) Preliminarily identify the issues and discuss the anticipated format of the hearing;

(2) Discuss a schedule for any discovery to be conducted and address any discovery issues that are raised at that time;

(3) Explore the possibility of obtaining admissions of fact and of the authenticity~~genuineness~~ of documents that would avoid unnecessary proof;

(4) Develop a schedule for the preparation and submission of evidence and witness testimony, including the disclosures of witnesses and exhibits and whether the use of pre-filed testimony may not be appropriate, in advance of the E~~e~~videntiary ~~h~~Hearing;

(5) Develop a schedule or schedules for any anticipated motions

(6~~5~~) Schedule a date(s) for the E~~e~~videntiary H~~h~~earing, which shall be within ninety (90) days of the prehearing conference described in this subsection, unless a different date or dates is specified by the Hearing Officer or the Hearing Body with the consent of all Participants or for good cause shown; and

(7~~6~~) Address such other matters as may aid in the simplification of the evidence and disposition of the proceeding.

(b) The Hearing Officer shall also hold a final prehearing conference prior to the Evidentiary Hearing, for the purpose of discussing:

(1) the anticipated duration of the hearing;

(2) the scheduling of witnesses' appearances to testify;

(3) the issues anticipated to be presented at the hearing;

(4) whether prehearing memoranda should be filed and if so, the schedule; and

(5) any other matters identified by the Hearing Officer for the management of the Evidentiary Hearing.

Participants may submit to the Hearing Officer, at least ten (10) days prior to the scheduled date of the final prehearing conference, a proposed list or lists of matters to be discussed at the final prehearing conference.

1.5.3 Summary Disposition

(a) Availability

A Hearing Officer, on the Hearing Officer's own motion or on the motion of a Participant, may issue an initial opinion granting, in whole or in part, summary disposition if it appears that there are no issues of material fact and a Participant is entitled to issuance of a final order in its favor. ~~If the Hearing Officer is considering summary disposition in the absence of a Participant motion, the Hearing Officer shall request the Participants to identify in writing any issues of material fact and to comment on the proposed disposition. Factual information in the Participants' comments shall be supported by affidavit. Following review of the Participants' comments, if it still appears to the Hearing Officer that there are no genuine issues of material fact, the Hearing~~

~~Officer may proceed without an evidentiary hearing. The Hearing Officer shall, however, allow the Participants the opportunity to file briefs.~~

(b) Motion for Summary Disposition and Responses

(1) A Participant moving for summary disposition must clearly identify the material facts that are not in dispute, demonstrate that there are no other material facts in dispute, and demonstrate that on the basis of the undisputed material facts, the Participant is entitled to issuance of a final order in its favor.

(2) A Participant opposing a motion for summary disposition must clearly identify in its response to the motion the material facts that the Participant contends remain in dispute, and/or explain why the moving Participant is not entitled to issuance of a final order in its favor even though there are no disputed issues of material fact.

(c) Summary Disposition on the Hearing Officer's Own Motion

If the Hearing Officer is considering summary disposition in the absence of a Participant motion, the Hearing Officer shall request the Participants to identify in writing any issues of material fact and to comment on the proposed disposition. Factual information in the Participants' comments shall be supported by affidavit. Following review of the Participants' comments, if it still appears to the Hearing Officer that there are no genuine issues of material fact, the Hearing Officer may proceed without an Evidentiary Hearing. The Hearing Officer shall, however, allow the Participants the opportunity to file briefs.

(d) Hearing Officer's Initial Opinion Granting Summary Disposition

When the Hearing Officer issues an initial opinion granting ~~a motion for~~ summary disposition in whole or in part, the ruling shall set forth the rationale for the grant. An initial opinion of the Hearing Officer granting summary disposition shall be confirmed, rejected or modified in a final order issued by the ~~[HEARING BODY]~~Hearing Body.

1.5.4 Status Hearings

Any Participant may request, and the Hearing Officer may call, a status hearing at any time subsequent to the initial prehearing conference to address issues that have arisen between the Participants or other matters relevant to the conduct of the hearing. Such issues may include, but are not limited to, discovery disputes and scheduling matters. A Participant requesting a status hearing to resolve a dispute shall include in its request a certification that it has made a good faith effort to resolve the dispute with the other Participant(s) before requesting the status hearing. The Hearing Officer shall direct the Clerk to issue a notice of status hearing that sets forth the date, time and place for the hearing, and identifies the matters to be addressed at the hearing.

1.5.5 Motions and Responses

(a) Unless otherwise provided in these Hearing Procedures or by the procedural schedule established by the Hearing Officer or Hearing Body, a Participant may file a motion at any time requesting any relief as may be appropriate. Unless ~~a~~the Hearing Officer allows a motion to be made orally on the record, motions shall be filed in writing. Motions based on facts that do not appear of record shall be supported by affidavit.

(b) Unless otherwise specified by the Hearing Officer or Hearing Body, responses to motions shall be filed within fourteen (14) days after service of the motion, and replies to responses shall be filed within seven (7) days after service of the responses~~;~~. ~~however, a~~A Hearing Officer or Hearing Body may deny dilatory, repetitive, or frivolous motions without awaiting a response. Unless otherwise ordered by a Hearing Officer or Hearing Body, the filing of a motion does not stay the proceeding or extend any scheduled dates in the proceeding.

1.5.6 Experts

(a) A Participant may employ an expert(s) to testify or consult in a proceeding. Any expert utilized in either capacity shall sign an agreement evidencing the expert's understanding and acknowledgement of the non-public nature of the proceeding and that unauthorized public disclosure of information obtained in connection with the expert's participation in the proceeding is prohibited.

(b) The Participant employing the expert shall propose the agreement for approval by~~via a~~ motion, and its approval shall be subject, in addition to consideration of any objections by other Participants, to ensuring that appropriate safeguards are maintained to protect the confidentiality of the proceeding and the information disclosed therein.

1.5.7 Inspection and Copying of Documents in Possession of Staff

(a) Documents to be Available for Inspection and Copying

(1) Within twenty-five (25) days after the date the ~~issuance of the notice of~~request for hearing is filed, Staff shall make available for inspection and copying by the ~~Respondent~~other Participants, all Documents prepared or obtained by Staff through or in connection with any compliance monitoring process~~(~~es~~)~~ that led to the institution of proceedings. Such Documents shall include but are not limited to:

(A) requests for information to the Respondent;

(B) every written request, including e-mail, directed to persons not employed by the Compliance Enforcement Authority to provide information or Documents or to be interviewed;

(C) the Documents provided in response to any such requests described in (A) and (B) above;

(D) all transcripts of testimony recorded during the Staff investigation and all exhibits to the transcript;

(E) all other Documents obtained from the Respondent; and

(F) all other Documents obtained from persons not employed by the Compliance Enforcement Authority.

The sole grounds on~~bases pursuant to~~ which Staff is ~~shall be~~ authorized to withhold Documents from inspection and copying are~~shall be~~ the bases set forth in subsection~~Paragraph 1.5.7~~(b); provided, however, that the Documents made available for inspection and copying need not include (i) exact copies of Documents the Respondent previously provided to Staff, and (ii) any Documents provided to the Respondent with or as part of the Notice of Alleged Violation, Notice of Penalty, assessment of proposed Mitigation Plan or Remedial Action Directive.

(2) Where there are Participants in a proceeding in addition to a single Respondent and Compliance Staff, the Hearing Officer ~~or [HEARING BODY]~~ shall oversee the Staff's designation of Documents to be produced to such other Participants and the development, execution and enforcement of any protective order deemed necessary.

(3) Staff shall promptly inform the Hearing Officer and each other ~~Respondent~~Participant if, after the issuance of a notice of hearing, requests for information are issued by Staff related to the same compliance monitoring process(es) that led to the institution of the proceeding. If Staff receives Documents pursuant to a request for information after Staff has made Documents ~~have been made~~ available ~~to a Respondent~~ for inspection and copying as set forth in ~~Subparagraph~~subsection (a)(1), the additional Documents shall be made available to the ~~Respondent~~Participants not later than fourteen (14) days after Staff receives such Documents. If a date for the ~~e~~Evidentiary ~~h~~Hearing has been scheduled, Staff shall make the additional Documents available to the ~~Respondent~~other Participants not less than ten (10) days before the Evidentiary ~~h~~Hearing. If Staff receives such Documents ten or fewer days before the Evidentiary ~~h~~Hearing is scheduled to begin or after the Evidentiary ~~h~~Hearing begins, Staff shall make the additional Documents available immediately to the ~~Respondent~~other Participants.

(4) Nothing in subsection~~paragraph~~ (a)(1) shall limit the discretion of the Compliance Enforcement Authority to make any other Document available to the ~~Respondent~~Participants or the authority of the Hearing Officer to order the production of any other Documents or information by any Participant.

(b) Documents That May Be Withheld by Staff

(1) Staff may withhold a Document from inspection and copying by ~~the Respondent~~a Participant if:

(A) the Document is privileged to the Compliance Enforcement Authority~~Staff~~ or constitutes attorney work product of ~~Staff's~~ counsel for the Compliance Enforcement Authority (in applying this provision, the attorney-client privilege shall be recognized as absolute and any demand for production of attorney work product shall be granted only after a showing of substantial need by the Respondent or other Participant);

(B) the Document is an examination or inspection report, an internal memorandum, or other note or writing prepared by a Staff member that ~~shall~~ will not be offered in evidence or otherwise relied on by Staff in the Hearing;

(C) the Document would disclose

(i) ~~(i)~~ an examination, investigatory or enforcement technique or guideline not otherwise made public of the Compliance Enforcement Authority, a federal, state, or foreign regulatory authority, or a self-regulatory organization;

(ii) the identity of a source, including a federal, state, or foreign regulatory authority or a self-regulatory organization, that furnished information or was furnished information on a confidential basis regarding an investigation, an examination, an enforcement proceeding, or any other type of civil or criminal enforcement action; or

(iii) an examination, an investigation, an enforcement proceeding, or any other type of civil or criminal enforcement action under consideration by, or initiated by, the Compliance Enforcement Authority, a federal, state, or foreign regulatory authority, or a self-regulatory organization; or

(D) the Hearing Officer grants leave to withhold a Document or category of Documents as not relevant to the subject matter of the proceeding, or for other good cause shown.

Provided, that where a Document contains information of the type listed in ~~Subparagraphs~~subsections (A), (B), (C) or (D) that is capable of being redacted, Staff shall make the document available for inspection and copying by the other Participants~~Respondent~~ in redacted form.

(2) Nothing in ~~Subparagraph~~subsections (b)(1)(B), (C) or (D) authorizes Staff to withhold a Document, or a part thereof, that contains exculpatory evidence.

Nothing in ~~Subparagraph~~subsection (b)(1) requires Staff to withhold a Document from disclosure.

(c) ___Withheld Document List

–At the time it is required to make Documents available for inspection and copying, Staff shall also provide to the Hearing Officer, the Respondent and any other Participant to which Documents are being made available, a list of Documents withheld by Staff pursuant to ~~Subparagraph~~subsection (b)(1), with a statement of the grounds that support withholding the Document. Upon review, for good cause shown, the Hearing Officer may order Staff to make any Document withheld, other than a Document that is subject to the attorney-client privilege, available to the ~~Respondent(s)~~other Participants for inspection and copying.

(d) ___Timing of Inspection and Copying

Except as set forth in this ~~Paragraph~~Section, the Hearing Officer shall determine the schedule of production of Documents for inspection and copying, provided that the Hearing Officer may modify any time period for production set forth in this Section~~Paragraph~~ as warranted by the circumstances.

(e) ___Place and Time of Inspection and Copying

Documents subject to inspection and copying pursuant to this ~~Paragraph~~Section shall be made available to the Respondent and other Participants for inspection and copying at the Compliance Enforcement Authority office where the Documents are ordinarily maintained, or at such other office as the Hearing Officer, in his or her discretion, shall designate, or as the Participants otherwise agree. A ~~Respondent~~Participant shall be given access to the Documents at the Compliance Enforcement Authority's offices during normal business hours. A ~~Respondent~~Participant shall not be given custody of the Documents or be permitted to remove the Documents from the Compliance Enforcement Authority's offices, other than copies of Documents made available by the Compliance Enforcement Authority for that purpose.

(f)____ Copying Costs

A ~~Respondent~~Participant may obtain a photocopy of all Documents made available for inspection. A ~~Respondent~~Participant shall be responsible for the cost of photocopying. Unless otherwise ordered by the Hearing Officer, charges for copies made at the request of a Participant~~Respondent~~ shall be at a rate to be established by the Compliance Enforcement Authority.

-(g) ___Failure to Make Documents Available — Harmless Error

In the event that a Document required to be made available to a Participant~~Respondent~~ pursuant to this Section~~Paragraph~~ is not made available by Staff, no rehearing or amended decision of a proceeding already heard or decided shall be required where the failure to make the Document available was harmless error. Should a dispute arise as to whether a rehearing or amended decision is required due to the failure of Staff to produce a Document, the burden shall be on

Staff to show that such failure was harmless error. The Hearing Officer, or, upon review, the ~~[HEARING BODY]~~Hearing Body shall determine whether the failure to make the Document available was harmless error.

1.5.8 Other Discovery Procedures

(a) In addition to the production of Documents by Staff for inspection and copying by Respondent and other Participants pursuant to ~~Paragraph~~Section 1.5.7, the Participants shall be entitled to utilize all other discovery methods provided for in Rules 402 through 409 of the FERC Rules of Practice and Procedure, 18 C.F.R. §385.402 through 385.409, including data requests, written interrogatories and requests for production of Documents or things, depositions by oral examination, requests for inspection of Documents and other property, requests for admissions, and requests for issuance of orders to one or more Registered Entities to produce Documents for inspection and copying or at the hearing or to provide testimony by an authorized representative in deposition or at the hearing.

(b) Unless otherwise directed by the Hearing Officer or ~~[HEARING BODY]~~Hearing Body upon motion by a Participant, or by the Hearing Officer, or by the ~~[HEARING BODY]~~Hearing Body on its own motion, such discovery, and the resolution of any disputes concerning such discovery, shall be conducted in accordance with the provisions of Rules 402 through 410 and 510(e) of the FERC Rules of Practice and Procedure, 18 C.F.R. §385.402 through 385.410 and 385.510(e), which are hereby incorporated by reference into these Hearing Procedures, subject to the following limitations and modifications to such Rules:

~~(a)~~(1) The provisions of ~~Subparagraphs~~subsections (d), (e) and (f) of ~~Paragraph~~Section 1.5.7 shall apply to any such discovery.

~~(b)~~(2) Rule 403(b)(2) (18 C.F.R. §385.403(b)(2)) and Rule 410(d)(2) (18 C.F.R. §385.410(~~b~~d)(2)) shall not be applicable.

~~(c)~~(3) The Hearing Officer and the ~~[HEARING BODY]~~Hearing Body have the authority to issue orders to compel the appearance by or production of Documents or information by, only a Person that (i) is a Participant or (ii) is a Registered Entity (including an authorized representative thereof) that is not a Participant. The Hearing Officer and the ~~[HEARING BODY]~~Hearing Body do not have authority to require a United States marshal or deputy marshal to serve an order to produce or provide Documents, information or testimony.

~~(d)~~(4) References to "subpoena" in Rules 404, 409, 410 and 510(e) shall be deemed to be to an order to a non-Participant Registered Entity to produce or provide Documents, information or testimony.

(~~e~~5) References to the "Commission" in Rules 402 through 410 and 510(e) shall be to FERC except as follows:

(i) the references in Rules 402(a), 404(b)(1) and 405(b), the second reference in Rule 410(d), and the references in Rule 510(e)(1) and (2) shall be deemed to be to the ~~[HEARING BODY]~~Hearing Body,

(ii) the reference in Rule 385.406(b)(4) to "Commission trial staff" shall be deemed to be to Compliance Staff, and

(iii) the reference in Rule 510(e)(3) shall be deemed to be to the Hearing Officer or ~~[HEARING BODY]~~Hearing Body.

(~~f~~6) Unless otherwise ordered by the Hearing Officer or ~~[HEARING BODY]~~Hearing Body, a data request, set of interrogatories, request for production of Documents or things, request for inspection of Documents or other property, request for admissions, or order to produce or provide Documents, information or testimony, shall not specify a due date or response date that is fewer than 21 days from the date of service of the request or date of the order.

(~~g~~)(7) A list of withheld Documents, if any, shall be provided by any Participant required to produce Documents, at the time the documents are required to be produced, to the Hearing Officer and to each Participant entitled to receive production of the Documents. Upon review, for good cause shown, the Hearing Officer may order the Participant to make any Document withheld available to any other Participant or Participants for inspection and copying.

(~~h~~)(8) In the event a Document or information required to be produced or provided by a Participant pursuant to discovery is not produced or provided by the Participant, no rehearing or amended decision of a proceeding already heard or decided shall be required where the failure to produce or provide the Document or information was harmless error. Should a dispute arise as to whether a rehearing or amended decision is required due to the failure of a Participant to produce or provide a Document or information, the burden shall be on the Participant that failed to produce or provide the Document or information to show that such failure was harmless error. The Hearing Officer or, upon review, the ~~[HEARING BODY]~~Hearing Body shall determine whether the failure to make the Document available was harmless error.

(~~i~~9) Unless otherwise ordered by the Hearing Officer or ~~[HEARING BODY]~~Hearing Body, all such discovery shall be requested, scheduled and conducted so as to be completed within six (6) months following the date ~~of~~ the request for hearing was filed~~initial prehearing conference held pursuant to Paragraphs 1.4.1 and 1.5.2~~.

(~~j~~10) Notwithstanding ~~(f)~~subsections (b)(6) and ~~(i)~~(b)(9), however, if the shortened hearing procedure in Section 1.3.4~~Paragraph 1.3.2~~ is used in a proceeding, the Hearing Officer, on his or her own motion or on motion of a Participant, shall establish a schedule for discovery, including response periods for responding to discovery requests, that are consistent with the expedited nature of the proceeding contemplated by the shortened hearing procedure.

(c) The Hearing Officer's ruling on all motions relating to disputes concerning such discovery shall consider the following objectives:

(~~i~~1) full disclosure of all relevant Documents and information;

(2~~ii~~) the exercise of due diligence in the conduct of discovery by a Participant; and

(~~iii~~3) disallowing use of discovery as a means to delay the proceeding or to harass or burden any other Participant.

1.5.9 Pre-Evidentiary Hearing Submission of Testimony and Evidence

(a) Unless the Hearing Officer orders otherwise and with the exception of (i) any adverse Participant examination pursuant to ~~Paragraph~~Section 1.6.16 and (ii) the testimony and Documents of a non-Participant provided pursuant to an order to produce or provide Documents, information or testimony, all witness direct testimony to be submitted in an Evidentiary ~~h~~Hearing must be prepared in written form, may have exhibits, schedules and attachments thereto, and shall be filed in advance of the ~~e~~Evidentiary ~~h~~Hearing pursuant to a schedule determined by the Hearing Officer, as it may be amended.

(b) Where a Participant intends to use a Document or other demonstrative evidence that has not been filed as part of written testimony in the conduct of cross-examination (other than Documents that are to be produced by a non-Participant at the hearing pursuant to an order to produce Documents), the Participant intending to use such Document or demonstrative evidence shall provide it to the other Participants and the Hearing Officer at least three (3) business days prior to the date at which the witness will be cross-examined at ~~the~~a ~~evidentiary~~Testimonial H~~h~~earing.

(c) Compliance Staff shall file the Documents it intends to offer into evidence as its direct case, including the written testimony of its witnesses along with exhibits, schedules and attachments thereto, first. The Registered Entity shall file the Documents it intends to offer into evidence as its direct case, which also may be responsive to Staff's direct case, including the written testimony of its witnesses along with exhibits, schedules and attachments thereto, second. Staff shall file as its rebuttal case the Documents it intends to offer into evidence in response to the Registered Entity's direct case, including the written testimony of its witnesses along with exhibits, schedules and attachments thereto, third.

(d) If appropriate due to the number and/or complexity of the issues, the Hearing Officer may allow for the Registered Entity to submit a rebuttal case that responds to Staff's rebuttal case, in which event the Hearing Officer shall also allow Staff to submit a surrebuttal case that responds to the Registered Entity's rebuttal case.

(e) Each round of evidence shall be limited in scope to responding to the preceding round of evidence, except that the Registered Entity's direct case may exceed the scope of Staff's direct case if necessary for the Registered Entity to set forth its direct case fully.

(f) The Participants shall file the Documents they intend to offer into evidence in accordance with the Hearing Officer's schedule, as it may be amended. Such filings of written testimony and other evidence in advance of the ~~e~~Evidentiary ~~h~~Hearing shall not entitle the Documents to be admitted into the evidentiary record. The Participants must offer their witnesses' testimony and other proposed evidence for admission into the evidentiary record during the ~~e~~Evidentiary ~~h~~Hearing.

(g) Any Participant who fails, without good cause shown, to comply with the Hearing Officer's schedule for the filing of written testimony and other evidence in advance of the ~~e~~Evidentiary ~~h~~Hearing may be limited in the presentation of its evidence during the ~~e~~Evidentiary ~~h~~Hearing or have its participation in the ~~e~~Evidentiary ~~h~~Hearing otherwise restricted by the Hearing Officer to avoid undue prejudice and delay.

1.5.10 Protective Orders

(a) All proceedings conducted pursuant to these Hearing Procedures, and any written testimony, exhibits, other evidence, transcripts, comments, briefs, rulings and other issuances, shall be non-public and shall be held in confidence by all Participants, except as the ERO (within the U.S., in accordance with the authorization previously granted by FERC to release information about a non-public proceeding) or FERC (in the case of U.S.-related information) or another Applicable Governmental Authority (in the case of non-U.S.-related information) authorizes or directs public disclosure of any portion of the record. In addition to this general proscription, at any time during a proceeding, the Hearing Officer, on his or her own motion or on the motion of any Participant or of any non-Participant ordered to produce Documents, information or testimony, may enter a protective order to designate as proprietary and protect the confidential, proprietary or trade secret nature of any data, information or studies, or any other information the public release of which may cause a security risk or harm to a Participant.

(b) The following types of information will be considered entitled to protection through a protective order:

(~~i~~1) confidential business and market information, including information that is proprietary, commercially valuable, or competitively sensitive;

(~~ii~~2) Critical Energy Infrastructure Information;

(~~iii~~3) information related to a Cybersecurity Incident;

(~~iv~~4) personnel information that identifies or could be used to identify a specific individual, or that reveals personnel, financial, medical or other personal information;

(~~v~~5) audit work papers;

(~~vi~~6) investigative files or Documents that would disclose investigative techniques of Staff, any Compliance Enforcement Authority, the ERO or any federal, state or foreign regulatory authority.

Nothing in this ~~Subparagraph~~subsection 1.5.10(b) shall require Staff to produce any Documents it is entitled to withhold under ~~Subparagraph~~subsection 1.5.7(b).

(c) A motion for a protective order shall specify the proposed expiration date for the proprietary status of the data, Documents or information, if any, and shall propose requirements or safeguards to be met for individuals participating in the proceeding to review the protected information while maintaining its proprietary status.

(d) A Document submitted and marked as proprietary, or a statement made at a hearing and identified as proprietary, shall be afforded proprietary treatment pending the timely submission of a motion to protect the confidential, proprietary or trade secret nature of that Document or statement and a ruling on such a motion by the Hearing Officer.

(e) The protective order shall identify the data, Documents or information that will be accorded proprietary treatment; the individuals participating in the proceeding, by category or otherwise, entitled to view the proprietary information; and the requirements, conditions or safeguards that must be met before an individual may view the information.

(f) A public redacted version of each Document and transcript that contains information that is protected pursuant to this ~~Paragraph~~Section must be filed with the proprietary version and must be served on each Participant for distribution to those individuals participating in the proceeding who are not entitled to view the proprietary information.

(g) Should it be necessary to address proprietary information during a hearing, the Hearing Officer shall, while the information is being addressed, close the hearing to all individuals other than those entitled to view or hear the proprietary information in accordance with the protective order.

1.5.11 Pre-Evidentiary Hearing Memorandum

(a) The Hearing Officer or the ~~[HEARING BODY]~~Hearing Body may request~~, as needed on a case by case basis due to the number or complexity of the issue(s),~~ the submission of memoranda prior to the ~~e~~Evidentiary ~~h~~Hearing that set forth ~~outline~~ each Participant's position on the issue(s) in dispute, the key facts and arguments, ~~and~~ the applicable Reliability Standard, rules, orders or other authority, and such other matters as may be directed by the Hearing Officer or the Hearing Body.

(b) The purpose of such memoranda will be to aid the Hearing Officer and ~~[HEARING BODY]~~Hearing Body in preparation for the ~~e~~Evidentiary ~~h~~Hearing. A Participant will not be deemed to have waived any issue, fact or argument that is not set forth in a pre-~~e~~Evidentiary ~~h~~Hearing memorandum.

(c) The Hearing Officer may establish ~~page~~word limitations on such submissions.

1.5.12 Certification of Questions to the NERC Board of Trustees

(a) Should a hearing present a significant question of law, policy or procedure the resolution of which may be determinative of the issues in the proceeding in whole or in part, or as to which there are other extraordinary circumstances that make prompt consideration of the question by

the NERC Board of Trustees appropriate, the Hearing Officer, on his or her own motion or on motion of a Participant, may recommend to the Hearing Body that it certify, or the Hearing Body on its own motion may decide to certify, the question to the NERC Board of Trustees for determination pursuant to Section 412 of the NERC Rules of Procedure.

(b) If the Hearing Officer, on his or her own motion, or the Hearing Body, on its own motion, wishes to present a question to the Hearing Body for certification to the NERC Board of Trustees, the Hearing Officer shall first provide the Participants the opportunity to submit memoranda addressing whether the question should be certified and the precise terms of the question to be certified.

(c) If a Participant files a motion requesting, or the Hearing Officer determines on his or her own motion, that a question should be certified to the NERC Board of Trustees, the Hearing Officer shall submit a written recommendation on the matter to the Hearing Body. If the request for certification is based on the motion of a Participant, the Hearing Officer shall also submit to the Hearing Body the motion and any answers to the motion that were filed. If the request for certification is on the Hearing Officer's own motion, the Hearing Officer shall also submit to the Hearing Body the Participants' memoranda that were filed pursuant to subsection (b).

(d) Questions of fact presented by the particular matter in dispute in a hearing shall not be the subject of a certification to the NERC Board of Trustees.

(e) The Hearing Body shall determine, based on the criteria specified in subsection (a), whether the proposed question shall be certified to the NERC Board of Trustees for determination. If the Hearing Body determines that the proposed question should be certified to the NERC Board of Trustees, the Hearing Body shall also determine whether the hearing should be suspended, in whole or in part, while the question is pending before the NERC Board of Trustees for determination.

(f) As provided in NERC Rule of Procedure Section 412, the NERC Board of Trustees may decide to reject a proposed certification from a Hearing Body.

(f) If the NERC Board of Trustees accepts certification of a question and issues a determination on the question, the hearing shall proceed following the determination in accordance with the NERC Board of Trustees' decision.

1.6 Procedure at Evidentiary Hearing ~~Procedure~~

1.6.1 Purpose of Evidentiary Hearings~~s~~

The purpose of the E~~e~~videntiary H~~h~~earing shall be to admit the Participants' evidence into the record, and for each Participant to have the opportunity to cross-examine the other Participant's witnesses. A schedule for briefs, unless waived by the Participants, shall be set at the conclusion of the ~~e~~Evidentiary ~~h~~Hearing. ~~The evidentiary hearing also may be used to address any other issue pending between the Participants.~~

1.6.2 Order of Receiving Evidence

In all proceedings Compliance Staff shall open and close.

1.6.3 Opening and Closing Statements

Opening and closing statements will not be made during the ~~e~~Evidentiary ~~h~~Hearing as a matter of course except that such statements may be allowed when requested by a Participant, and shall be required when requested by the Hearing Officer or the ~~[HEARING BODY]~~Hearing Body. Any Participant's request for such statements, or a Hearing Officer or ~~[HEARING BODY]~~Hearing Body notice requiring such statements, shall be made at least ten (10) days in advance of the start of the ~~e~~Evidentiary ~~h~~Hearing.

1.6.4 Right of Participant to Present Evidence

Subject to compliance with the requirements of these Hearing Procedures concerning the timing of submission of written testimony and other evidence, a Participant has the right to present such evidence, to make such objections and arguments, and to conduct such cross-examination as may be necessary to assure the true and full disclosure of the facts.

1.6.5 Exhibits

(a) All material offered in evidence, except oral testimony allowed by the Hearing Officer or the testimony of a non-Participant pursuant to an order to produce or provide Documents, information or testimony, shall be offered in the form of an exhibit.

(b) Each exhibit must be marked for identification. A Participant must provide the court reporter with two (2) copies of every exhibit that the Participant offers into evidence, and will provide copies of any exhibit not served in advance of the ~~e~~Evidentiary ~~h~~Hearing to the Participants and the Hearing Officer.

1.6.6 Witness Attendance at Testimonial~~Evidentiary~~ Hearing

(a) Each witness shall attend the Testimonial~~evidentiary~~ ~~h~~Hearing in person unless a Participant has been informed in advance of the Testimonial~~evidentiary~~ ~~h~~Hearing that all other Participants waive cross-examination of the witness and neither the Hearing Officer nor the members of the ~~[HEARING BODY]~~Hearing Body have any questions for the witness, in which event the witness does need not be present at the ~~evidentiary~~Testimonial ~~h~~Hearing.

(b) A person compelled to appear, voluntarily testifying, or making a statement may be accompanied, represented and advised by an attorney.

(c) All testimony offered at ~~a~~the Testimonial~~evidentiary~~ ~~h~~Hearing is to be under oath or affirmation. If a witness is not required to attend ~~the evidentiary~~a Testimonial ~~h~~Hearing, then the Participant on whose behalf the witness prepared testimony shall submit an affidavit of the witness attesting to the veracity of the witness' testimony, and the Participant shall be allowed to introduce the witness' testimony, and the exhibits, schedules and attachments thereto, into the evidentiary record based on such affidavit.

1.6.7 Admission of Evidence

(a) Compliance Staff shall offer its exhibits into evidence first and the Registered Entity second, unless the Participants agree otherwise.

(b) Except for witnesses who are not required to attend the Testimonial~~evidentiary~~ ~~h~~Hearing, the Participants shall call each witness in turn. Following the witness' swearing in, the witness shall attest to the veracity of his or her written testimony. The witness may identify any language and/or figures in his or her written testimony or exhibits that the witness would like to change or correct. Subject to objection, such changes or corrections may be allowed at the Hearing Officer's discretion for the purpose of obtaining a full, accurate and complete record without imposing undue delay or prejudice on any Participant. The Participant whose witness has made changes or written corrections to written testimony and exhibits shall file corrected copies with the Clerk and provide corrected copies to the Hearing Officer and other Participant.

(c) Once a witness has attested to the veracity of his or her testimony, the Participant on whose behalf the witness is testifying shall move for admission of the witness' testimony, including all exhibits, schedules and attachments thereto, into evidence. Other Participants may object to the introduction of the witness' testimony, or any part thereof, as set forth in ~~Paragraph~~Section 1.6.11. Subject to the Hearing Officer's ruling on the objection, the witness' testimony shall be admitted into evidence.

(d) The witness shall then be turned over for cross-examination by other Participants, and for any questions by the Hearing Officer or any member of the ~~[HEARING BODY]~~Hearing Body, in accordance with Section~~Paragraph~~ 1.6.14, and then for redirect examination in accordance with Section~~Paragraph~~ 1.6.15. Witnesses shall be cross-examined on all previously-served testimony (direct, rebuttal or surrebuttal) when they first take the witness stand.

(e) Except (i) in exceptional cases and upon a showing of good cause, and (ii) witnesses testifying pursuant to an order to produce or provide Documents, information or testimony issued to a non-Participant, no witness shall be allowed to testify ~~during the evidentiary hearing~~ unless a Participant has served the witness' written testimony in advance of the ~~evidentiary~~Testimonial ~~h~~Hearing in accordance with the schedule established by the Hearing Officer. Due to the undue prejudice such surprise witness testimony would impose on other Participants, it is the Compliance Enforcement Authority's policy to discourage witness testimony at a~~n~~ ~~evidentiary~~Testimonial H~~h~~earing when a Participant has not served the witness' written testimony in advance of the Testimonial~~evidentiary~~ H~~h~~earing. If such testimony is allowed, sufficient procedural steps shall be taken by the Hearing Officer to provide the other Participants with a fair opportunity for response and cross-examination.

1.6.8 Evidence that is Part of a Book, Paper or Document

(a) When relevant and material matter offered in evidence is embraced in a book, paper or Document containing other matter that is not material or relevant, the Participant offering the same must plainly designate the matter offered as evidence, and segregate and exclude the material not offered to the extent practicable.

(b) If the material not offered is in such volume as would unnecessarily encumber the record, such book, papers or Document will not be received in evidence but may be marked for identification and, if properly authenticated, the relevant or material matter may be read into the

record, or, if the Hearing Officer so directs, a separate copy of such matter in proper form shall be offered as an exhibit.

(c) All other Participants shall be afforded an opportunity to examine the book, paper or Document and to offer in evidence in like manner other portions thereof if found to be material and relevant.

1.6.9 Stipulations

The Participants may stipulate to any relevant fact or the authenticity of any relevant Document. Stipulations may be made in writing or entered orally in the record. Notwithstanding stipulation, the Hearing Officer may require evidence of the facts stipulated in order to provide a complete evidentiary record on which to base the final order.

1.6.10 Official Notice

(a) Where relevant and material to the subject matter of the proceeding, the Hearing Officer may, upon request of a Participant, take official notice of any of the following:

(1) Rules, regulations, administrative rulings and orders, written policies of governmental bodies, and rulings and orders of other Compliance Enforcement Authorities.

(2) The orders, transcripts, exhibits, pleadings or any other matter contained in the record of other docketed proceedings of the Compliance Enforcement Authority.

(3) State, provincial and federal statutes and municipal and local ordinances.

(4) The decisions of state, provincial and federal courts.

(5) Generally recognized scientific or technical facts within the specialized knowledge of the Compliance Enforcement Authority.

(6) All other matters of which the courts of the United States may take judicial notice.

(b) All requests to take official notice shall be submitted in advance of the ~~e~~Evidentiary ~~h~~Hearing in accordance with a schedule established by the Hearing Officer. Before ruling on a request to take official notice, the Hearing Officer shall afford the other Participant opportunity to object or to show the contrary to the matter for which official notice is requested.

(c) An accurate copy of any item officially noticed shall be introduced into the record in the form of an exhibit presented by the Participant requesting official notice unless waived by the Participants and approved by the Hearing Officer. Any information officially noticed and not presented as an exhibit shall be set forth in a statement on the record.

1.6.11 Admissibility of Evidence

(a) Any evidence offered, including that included in a book, paper or Document pursuant to ~~Paragraph~~Section 1.6.8, shall be subject to appropriate and timely objections. Any Participant objecting to the admission or exclusion of evidence must state the grounds for objection.

(b) The admission of evidence shall not be limited by the generally recognized rules of evidence as applied in the courts of the United States or of the states, although the Hearing Officer may take such rules of evidence into consideration in ruling on the admissibility of evidence. The Hearing Officer will exercise discretion in the admission of evidence based upon arguments advanced by the Participants, and shall admit evidence if it is of a type commonly relied upon by reasonably prudent persons in the conduct of their affairs. The Hearing Officer may only exclude material from the record in response to a motion or objection by a Participant.

(c) Formal exception to a ruling on admissibility of evidence need not be taken to be preserved.

1.6.12 Offer of Proof

Any Participant who has had evidence excluded may make an offer of proof on the record. The offer of proof may consist of a statement made on the record of the substance of the evidence that the Participant claims would have been adduced, or any written or documentary exhibit that the Participant sought to introduce. Any such exhibit shall be retained as part of the record.

1.6.13 Reservation of Evidentiary Ruling

(a) The Hearing Officer shall rule upon any objection to the admissibility of evidence at the time the objection is made; provided that the Hearing Officer has discretion to reserve such a ruling or to require the Participants to file written arguments in relation thereto.

(b) If the Hearing Officer reserves the ruling, appropriate steps shall be taken during the ~~e~~Evidentiary ~~h~~Hearing to ensure a full, complete and accurate record in relation to the objected to evidence in the event the objection to the evidence's admissibility is overruled.

1.6.14 Cross-Examination

(a) Each witness shall be tendered for cross-examination subsequent to the admission of the witness' testimony into the evidentiary record. Each Participant shall have the right to cross-examine each witness of any other Participants. A Participant may waive cross-examination of any witness. Leading questions are permitted on cross-examination.

(b) The credibility of a witness may be attacked by any Participant, including the Participant calling the witness.

(c) The Hearing Officer and any member of the ~~[HEARING BODY]~~Hearing Body may ask the witness questions following the conclusion of the witness' cross-examination by the other Participant, and prior to the witness' redirect examination pursuant to Section~~Paragraph~~ 1.6.15. ~~If a member of the [HEARING BODY] seeks to ask a witness questions, the member shall do so by submitting the question in writing to the Hearing Officer, and the Hearing Officer shall ask the question of the witness.~~

1.6.15 Redirect Examination

A Participant shall be entitled to conduct redirect examination of each of the Participant's witnesses who are subject to cross-examination or questions of the Hearing Officer or a member of the ~~[HEARING BODY]~~Hearing Body. Any redirect examination shall be limited in scope to the witness' cross-examination and questions of the Hearing Officer and members of the ~~[HEARING BODY]~~Hearing Body. ~~If a member of the Hearing Body seeks to ask a witness questions, the member shall do so by submitting the question in written form to the Hearing Officer, and the Hearing Officer shall ask the question of the witness.~~

1.6.16 Examination of Adverse Participant

(a) Any Participant may call any adverse Participant, or any employee or agent thereof, during ~~the evidentiary~~a Testimonial ~~h~~Hearing to provide oral testimony on the Participant's behalf, and may conduct such oral examination as though the witness were under cross-examination.

(b) If a Participant intends to call an adverse Participant for examination, it shall give notice to the Hearing Officer and all other Participants setting forth the grounds for such examination at least fourteen (14) days in advance of the ~~evidentiary~~Testimonial ~~h~~Hearing, and the Participant who, or whose employee or agent, is sought to be called shall file any objection at least seven (7) days in advance of the ~~evidentiary~~Testimonial ~~h~~Hearing.

(c) Any Participant may conduct oral examination of a witness testifying pursuant to an order to produce or provide Documents, information or testimony issued to a non-Participant, as though the witness were under cross-examination.

1.6.17 Close of the Evidentiary Record

(a) The Hearing Officer shall designate the time at which the evidentiary record will be closed, which will typically be at the conclusion of the ~~e~~Evidentiary ~~h~~Hearing.

(b) Evidence may not be added to the evidentiary record after it is closed, provided that, prior to issuance of the Hearing Body's final order, the Hearing Officer may reopen the evidentiary record for good cause shown by any Participant. For the purpose of reopening the evidentiary record, newly discovered evidence that is material to the issues in dispute and could not, by due diligence, have been discovered prior to or during the Evidentiary Hearing, shall constitute good cause.

1.7 Post- Evidentiary Hearing Procedure

1.7.1 Briefs

(a) At the close of the ~~e~~Evidentiary ~~h~~Hearing, Participants may file initial and reply briefs.

(b) Briefs shall be concise, and, if in excess of twenty (20) pages, excluding appendices, shall contain a table of contents. Statements of fact should be supported by record citations.

(c) The Hearing Officer will prescribe the time for filing briefs, giving due regard to the nature of the proceeding, the extent of the record, the number and complexity of the issues, and the objective of expedition.

(d) Unless the Hearing Officer prescribes otherwise, all Participants shall file initial and reply briefs simultaneously.

(e) Participants' reply briefs shall be limited in scope to responding to arguments and issues raised in other Participants' initial briefs.

(f) The Hearing Officer may~~, with the agreement of the Participants,~~ allow oral closing statements to be made on the record in addition to or in lieu of briefs.

(g) The Hearing Officer may establish reasonable word~~page~~ limitations applicable to briefs.

1.7.2 Other Pleadings

Post-hearing pleadings other than briefs are permitted, but, absent good cause shown, such pleadings may not seek to introduce additional evidence into the record.

1.7.3 Draft Initial Opinions

The Hearing Officer may permit or require Participants to file draft initial opinions that set forth the Participants' proposed findings of fact and conclusions.

1.7.4 Hearing Officer's Initial Opinion

(a) ~~Except as otherwise ordered by the [HEARING BODY], a~~At the conclusion of the ~~e~~Evidentiary ~~h~~Hearing, and following the submission of initial and reply briefs and draft orders, if any, the Hearing Officer shall prepare an initial opinion for the ~~[HEARING BODY]~~Hearing Body's review and consideration.

(b) The initial opinion shall include a statement of each finding and conclusion, and the reasons or basis therefore, for all material issues~~ of fact, law or discretion~~ presented on the record. The initial opinion also shall contain the appropriate orders to dispose of the proceeding, including any Penalty, Mitigation Plan or Remedial Action Directive that the Hearing Officer proposes the ~~[HEARING BODY]~~Hearing Body require.~~ If the initial opinion proposes a Penalty, the initial opinion shall include a proposed Notice of Penalty.~~

(c) The initial opinion shall note if the subject of the proceeding has been deemed to involve a Cybersecurity Incident, if any information in the proceeding was deemed to be Critical Energy Infrastructure Information, or if any information in the proceeding is the subject of a protective order pursuant to ~~Paragraph~~Section 1.5.10.

1.7.5 Exceptions

(a) Within twenty-one (21) days after service of the initial opinion, or such other time as is fixed by the Hearing Officer, any Participant may file exceptions to the initial opinion in a brief designated "brief on exceptions" and, within fourteen (14) days after the time for filing briefs on

exceptions or such other time as is set by the Hearing Officer, any Participant may file as a reply, a "brief in reply to exceptions."

(b) Exceptions and replies thereto with respect to statements, findings of fact or conclusions in the initial opinion must be specific and must be stated and numbered separately in the brief. With regard to each exception, the Participant must specify each error asserted, and include a concise discussion of any policy considerations applicable and any other evidence and arguments in support of the Participant's position. Suggested replacement language for all statements to which exception is taken must be provided. Exceptions and arguments may be filed (1) together in one brief; or (2) in two separate documents, one designated as the brief containing arguments, and the other designated "Exceptions," containing the suggested replacement language.

(c) Arguments in briefs on exceptions and replies thereto shall be concise and, if in excess of twenty (20) pages, shall contain a table of contents.

(d) Participants shall not raise arguments in their briefs in reply to exceptions that are not responsive to any argument raised in any other Participant's brief on exceptions.

(e) Statements of fact should be supported by citation to the record.

(f) The Hearing Officer may establish reasonable ~~page~~word limitations applicable to arguments included in briefs on exception and briefs in reply to exceptions. Such ~~page~~word limitations shall not apply to a Participant's proposed replacement language.

(g) Unless good cause is shown, if a Participant does not file a brief on exceptions, or if a Participant filed a brief on exceptions that does not object to a part of the initial opinion, the Participant shall be deemed to have waived any objection to the initial opinion in its entirety, or to the part of the initial opinion to which the Participant did not object, whichever applies. This provision shall not prohibit the Participant, in its brief in reply to exceptions, from responding to another Participant's exceptions to such part of the initial opinion or from proposing alternative replacement language to the replacement language proposed by the other Participant for such part of the initial opinion.

1.7.6 Oral Argument

(a) The ~~[HEARING BODY]~~Hearing Body may elect to hear oral argument. If oral argument is held without briefs having been filed, Participants will be given the opportunity to present argument on all issues.

(b) If oral argument is held where briefs have been filed, argument may be limited to issues identified by the ~~[HEARING BODY]~~Hearing Body. The ~~[HEARING BODY]~~Hearing Body will direct the Clerk to issue a notice of oral argument that identifies the date, time, place and issues for the argument.

(c) The presentation of written materials or visual aids is permitted at oral argument. To the extent such materials or aids contain factual information, they shall be supported by the record, and ~~shall~~ contain accurate ~~record~~ citations to the record. Such materials or aids may not contain new calculations or quantitative analyses not presented in the record, unless they are based on

underlying data contained in the record. Copies of all written materials or visual aids to be presented at oral argument shall be served on all Participants not less than forty-eight (48) hours prior to the time and date of oral argument.

1.7.7 Additional Hearings

After the evidentiary record has been closed but before issuance of the Hearing Body's final order~~an initial opinion~~, the Hearing Officer may reopen the evidentiary record and hold additional hearings. Such action may be taken on the Hearing Officer's or the ~~[HEARING BODY]~~Hearing Body's own motion if there is reason to believe that reopening is warranted by any changes in conditions, or by the need to compile a complete evidentiary record on which to base the final order. Any Participant may file a motion to reopen the record, which shall contain the reasons for reopening, including material changes in conditions or the identification of additional evidence that should be included in the record, and a brief statement of proposed additional evidence and an explanation why such evidence was not previously adduced.

1.7.8 ~~[HEARING BODY]~~Hearing Body Final Order

(a) Following the receipt of the initial opinion, any exceptions and replies thereto, and oral argument, if any, the ~~[HEARING BODY]~~Hearing Body shall issue its final order.

(b) Issuance of a final order shall require (i) a quorum of the ~~[HEARING BODY]~~Hearing Body, which shall be (after any recusals, disqualifications and appointments of replacement members) at least fifty (50) percent of the number of members normally assigned to the ~~[HEARING BODY]~~Hearing Body, and (ii) majority vote of the members of the ~~[HEARING BODY]~~Hearing Body voting on the final order (which number of members voting shall not be less than a quorum).

(c) The ~~[HEARING BODY]~~Hearing Body shall strive, but shall not be required, to issue its final order within thirty (30) days following the last to occur of the initial opinion, exceptions or replies thereto, or oral argument. The final order may adopt, modify, amend or reject the initial opinion in its entirety or in part. The final order shall include a statement of each finding and conclusion, and the reasons or basis therefore, for all material issues ~~of fact, law or discretion~~ presented on the record.

(d) The ~~[HEARING BODY]~~ Hearing Body will base its determinations in the final order on the record. The final order also shall contain the appropriate orders to dispose of the proceeding, including any Penalty, ~~sanction,~~ Remedial Action Directive or Mitigation Plan required. ~~If the final order imposes a Penalty, it shall be entitled "Final Order and Notice of Penalty".~~

(e) The final order shall note if the subject of the proceeding has been deemed to involve a Cybersecurity Incident, if any information in the proceeding was deemed to be Critical Energy Infrastructure Information, or if any information in the proceeding is the subject of a protective order issued pursuant to ~~Paragraph~~Section 1.5.10.

(f) ~~The [HEARING BODY] shall direct the Clerk to serve the final order on the Participants.~~ The service of the final order shall include a notice informing the Participants of their appeal rights to the ERO or to FERC, as applicable.

1.7.9 The Record

The Clerk shall maintain the record for all dockets. The record shall include any of the following, including all attachments thereto and ~~d~~Documents filed therewith, that exist in any docket:

(1) Notice of Alleged Violation and Registered Entity's response thereto;

(2) Registered Entity's proposed Mitigation Plan and Staff's statement identifying its disagreement(s) therewith;

(3) Remedial Action Directives and the Registered Entity's notice contesting the Remedial Action Directive;

(4) Registered Entity's request for a hearing;

(5) Participant filings, motions, and responses;

(6) Notices, rulings, orders and other issuances of the Hearing Officer and ~~[HEARING BODY]~~Hearing Body;

(7) Transcripts;

(8) Evidence received;

(9) Written comments submitted in lieu of written testimony;

(10) Matters officially noticed;

(11) Offers of proof, objections and rulings thereon, and any written or documentary evidence excluded from the evidentiary record;

(12) ~~Briefs, p~~Pre-~~e~~Evidentiary ~~h~~Hearing memorandums, briefs, and draft opinions;

(13) Post-hearing pleadings other than briefs;

(14) The Hearing Officer's initial opinion;

(15) Exceptions to the Hearing Officer's initial opinion, and any replies thereto;

(16) The ~~[HEARING BODY]~~Hearing Body's final order~~, any Notice of Penalty issued therewith,~~ and the Clerk's notice transmitting the final order to the Participants;

(17) All notices of ex parte communications; and

(18) Any notifications of recusal and motions for disqualification of a member of the ~~[HEARING BODY]~~Hearing Body or Hearing Officer of Technical Advisor and any responses or replies thereto.

1.7.10 Appeal

A Participant, or a Regional Entity acting as the Compliance Enforcement Authority, may appeal a ~~F~~final ~~O~~order of the ~~[HEARING BODY]~~Hearing Body ~~may be appealed~~ to NERC in accordance with NERC's Rules of Procedure, Section 409. ~~The Clerk shall transmit to NERC the record of any docket that is the subject of an appealed final order.~~

1.8 Settlement

Settlements may be entered into at any time pursuant to Section 5.6 of the NERC Compliance Monitoring and Enforcement Program and the Compliance Enforcement Authority's settlement procedures, provided, that the Compliance Enforcement Authority (i) may decline to engage in or continue settlement negotiations after a Possible Violation or Alleged Violation becomes a Confirmed Violation, and (ii) may terminate settlement negotiations at any time.

1.9 Remedial Action Directives

1.9.1 Initiation of Remedial Action Directive Hearing

(a) Staff~~]~~ may issue a Remedial Action Directive to a Registered Entity at any time, including during any proceeding related to an Alleged Violation of a Reliability Standard. The Remedial Action Directive shall be delivered to the Registered Entity in accordance with Section 7.0 of the NERC Compliance Monitoring and Enforcement Program. The Compliance Enforcement Authority will notify NERC within two (2) business days after its Staff issues a Remedial Action Directive.

(b) The Registered Entity may contest the Remedial Action Directive by filing a written notice with the Clerk of the Compliance Enforcement Authority that states that the Registered Entity contests the Remedial Action Directive and that the Registered Entity requests a Remedial Action Directive hearing. The Registered Entity shall attach a copy of the Remedial Action Directive to its written notice. The Registered Entity must provide such notice within two (2) business days following the date of actual receipt (as defined in Section 7.0 of the NERC Compliance Monitoring and Enforcement Program) of the Remedial Action Directive. If the Registered Entity does not give written notice to the Compliance Enforcement Authority within the required time period, the Registered Entity shall be deemed to have waived its right to contest the Remedial Action Directive.

(c) The Clerk shall assign a docket number, and issue a notice of hearing that sets forth the date, time and place at which the hearing will convene ~~pursuant to Paragraph 1.4.1~~.

1.9.2 Remedial Action Directive Hearing Procedure

(a) Hearings to address Remedial Action Directives shall be conducted only under the expedited hearing process set forth in this Section~~Paragraph~~ 1.9.2. The ~~full~~general hearing procedures described in Sections 1.4 to 1.7 are applicable to the Remedial Action Directive hearing unless the context of a provision is inconsistent with or otherwise renders it inapplicable to the procedures set forth in this Section~~Paragraph~~.

(b) The Remedial Action Directive hearing ~~may~~shall be presided over by a Hearing Officer and will be conducted according to the following guidelines:

~~a)~~(1) The Hearing Officer ~~or the [HEARING BODY]~~ will hold a prehearing conference within two (2) business days after receipt of the Registered Entity's request for a hearing.

~~a)~~(2) A~~n evidentiary~~Testimonial ~~h~~Hearing will be conducted on the matter, in person or by teleconference, within seven (7) business days after the prehearing conference.

~~b)~~(3) At the ~~evidentiary~~Testimonial ~~h~~Hearing, Staff shall present oral witness testimony and evidence to show why the Remedial Action Directive should be complied with, and the Registered Entity shall present oral witness testimony and evidence to show why the Remedial Action Directive is not necessary or should be modified. All witness testimony shall be rendered under oath.

~~c)~~(4) At the ~~evidentiary~~Testimonial ~~h~~Hearing, the Participants shall have the opportunity to make opening statements. In addition, the Participants shall have the opportunity to make closing arguments, and Staff shall have the opportunity to make a rebuttal to the Registered Entity's closing argument.

~~d)~~(5) The Participants may file initial briefs and reply briefs, and/or draft opinions, on an expedited schedule set by the Hearing Officer ~~or the [HEARING BODY]~~. Oral argument shall not be held.

~~e)~~(c) The ~~[HEARING BODY]~~Hearing Body shall issue a summary written decision within ten (10) days following submission of the last brief~~the hearing~~, stating whether the Registered Entity shall or shall not be required to comply with the Remedial Action Directive and identifying any modifications to the Remedial Action Directive that ~~it~~the Hearing Body finds appropriate. Upon issuance of the summary written decision, the Registered Entity is required to comply with the Remedial Action Directive as specified in the summary written decision.

(d) Within thirty (30) days following issuance of its summary written decision, the ~~[HEARING BODY]~~Hearing Body shall issue a full written decision. The written decision shall state the conclusions of the ~~[HEARING BODY]~~Hearing Body with respect to the Remedial Action Directive, and shall explain the reasons for the ~~[HEARING BODY]~~Hearing Body's conclusions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Revisions 11-7-2011

Appendix 5A

Organization Registration and Certification Manual

Effective: ~~June 10, 2010~~ _____, 2012

116 -390 Village Boulevard, Princeton, New Jersey 08540-5721

Phone: 609.452.8030 · Fax: 609.452.9550 · www.nerc.com

Table of Contents

Section I — Executive Summary 1
Overview 1
To Whom Does This Document Apply? 1
When did These Processes Begin? 2
Where to Access and Submit Form(s)? 2
Roles and Responsibilities 2
Section II — Introduction to Organization Registration and Organization Certification Processes ... 4
Organization Registration — Entities Required to Register 4
Organization Certification 4
Section III — Organization Registration Process 5
Section IV — Organization Certification Process 8
Section V — NERC Organization Registration Appeals Process 14
Section VI — NERC Organization Certification Appeals Process 18
Definitions 21

Section I — Executive Summary

Overview

The purpose of this document is twofold: (1) to define the process utilized in the Organization Registration Program by identifying which functional entities must register as owners, operators, and users of the bulk power system (BPS) for compliance with reliability standards; and (2) to define the process utilized in the Organization Certification Program for certifying the following entities: Reliability Coordinator (RC), Balancing Authority (BA), and Transmission Operator (TOP). The NERC Compliance and Certification Committee (CCC) is responsible for approving and forwarding these processes to the NERC Board of Trustees for its approval. Where a proposal for revisions to these processes comes to the Board of Trustees from sources other than the CCC, the Board of Trustees will seek the concurrence of the CCC before taking action on the proposal.

To Whom Does This Document Apply?

All industry participants responsible for or intending to be responsible for, the following functions must register with NERC through the Organization Registration Process. The entities are defined in the NERC Glossary of Terms used in reliability standards with responsibilities designated by the individual standards.

	Entities that Must Register	Entities that Need to be Certified
Reliability Coordinator (RC)	√	√
Transmission Operator (TOP)	√	√
Balancing Authority (BA)	√	√
Planning Coordinator (PC)	√	
Transmission Planner (TP)	√	
Transmission Service Provider (TSP)	√	
Transmission Owner (TO)	√	
Resource Planner (RP)	√	
Distribution Provider (DP)	√	
Generator Owner (GO)	√	
Generator Operator (GOP)	√	
Load-Serving Entity (LSE)	√	
Purchasing-Selling Entity (PSE)	√	
Interchange Authority (IA)	√	
Reserve Sharing Group (RSG)	√	

When did These Processes Begin?

The initial registration process began in January of 2006. Registration of new entities is an ongoing process. If a Registered Entity's information changes, these changes must be submitted to the applicable Regional Entity(s).

Certification is ongoing for new entities in accordance with Section IV of this manual.

Where to Access and Submit Form(s)?

Registration and certification forms are provided on each Regional Entity's ~~website~~website. Completed forms are to be sent electronically to the ~~compliance and certification manager~~website location and/or individual(s) responsible for registration and/or certification of the applicable Regional Entit~~y~~(ies). It is desirable that entities operate within a single Regional Entity ~~reliability~~ region; however, if an entity operates in more than one Region, separate registration applications must completed and submitted to each of the Regional Entities.

Roles and Responsibilities

The following is a high-level overview of the roles and responsibilities in the registration and certification processes:

NERC

1. Oversight of entity processes performed by the Regional Entities, including:
   a. Governance per the Regional Entity's delegation agreement with NERC.
   b. Coordination of process execution when an entity is registering and/or certifying with multiple Regional Entities.
2. Manage each entity's NERC Compliance Registry identification number (NERC ID) including:
   a. Sending a registration or certification letter that contains the NERC ID to the applicable Regional Entity(ies) for review and approval. If the Regional Entit~~y~~(ies) agrees with all the information provided, it will notify NERC to issue the NERC ID to the ~~r~~Registered ~~e~~Entity and will send a copy of the notification being provided to the Regional Entit~~y~~(ies).
   b. Ensuring each entity has only one NERC ID for all Regional Entit(ies) in which registered.
3. Make modeling changes based on registration information.
4. Maintain accurate registration and certification records including granting certification certificates for the entity(ies) responsible for compliance (including JRO/CFR).
5. Maintain published up-to-date list of ~~r~~Registered ~~e~~Entities (i.e. the NERC Compliance Registry) on the NERC website.

Regional Entity

Registration

1. Performs data collection and mapping of ~~Bulk Power System~~BPS facilities and those facilities that have a material impact on the BPS~~Bulk Power System~~ within its Regional Entity defined reliability region boundaries.
2. ~~Approves or disapproves~~Reviews entity registration applications.

~~1.Reviews entity certification applications for completeness.~~

~~1.~~3.Notifies NERC of entities that should be registered ~~with the Regional Entity~~.

~~4. Approves or denies Certification Team (CT) recommendations and notifies the entity and NERC of the decision.~~

~~4. Provides leadership to the CT throughout the certification process.~~Notifies NERC of functional changes to registered entities in the Regional Entity's boundaries.

Certification

1. Reviews entity certification applications for completeness.
2. Approves or denies Certification Team (CT) recommendations and notifies the entity and NERC of the decision.
3. Provides leadership to the CT throughout the certification process.

Entity Submitting the Application

1. Completes and submits registration and/or certification application.
2. Submits updates to registration and/or certification information as necessary and/or requested.
3. Responds to Regional Entity and/or NERC questions pertaining to registration and/or certification.
4. Provides documentation or other evidence requested or required to verify compliance with certification requirements.

Section II — Introduction to Organization Registration and Organization Certification Processes

The processes utilized to implement the Organization Registration and Organization Certification Programs are administered by each Regional Entity. Pursuant to its delegation agreement with NERC, each Regional Entity is responsible for (i) identifying entities that should be registered~~ing~~ and (ii) certifying industry participants, within its Regional Entity reliability region boundaries. Each Regional Entity must use the following NERC processes.

Organization Registration — Entities Required to Register

All industry participants responsible for one or more of the functions below must register for each function through the Organization Registration Program. These entities are defined in the NERC Glossary of Terms used in reliability standards with responsibilities designated by the individual standards and the NERC *Statement of Compliance Registry Criteria* document.

- Reliability Coordinator
- Transmission Operator
- Balancing Authority
- Planning Coordinator
- Transmission Planner
- Transmission Service Provider
- Transmission Owner
- Resource Planner
- Distribution Provider
- Generator Owner
- Generator Operator
- Load-Serving Entity
- Purchasing-Selling Entity
- Interchange Authority
- Reserve Sharing Group

The registration procedure is in Section III of this manual.

Organization Certification

All entities registered in the NERC Compliance Registry (NCR) for the RC, ~~TOP~~BA, and/or ~~BA~~TOP functions, and entities that perform some or all of the reliability functions for or with the RC, BA or TOP, shall be certified. Certification requires the entity to start operation within 12 months of being NERC certified. This certification process is described in Section IV of this manual.

Section III — Organization Registration Process

Purpose and Scope

The purpose and scope of this process is to provide guidance on how a user, owner, and/or operator of the BPS~~bulk power system~~ should be registered in the NCR.

Overview

Section 39.2 of the Commission's regulations, and Title 18 of the C.F.R. § 39.2, require~~s~~ each ~~owner, operator, and user~~user, owner and operator of the BPS~~bulk power system~~ to be registered with NERC and to comply with approved reliability standards.

~~Owners, operators, and users~~Users, owners and operators of the BPS~~bulk power system~~ will be registered by function(s) and are:

1. Responsible for compliance with all applicable requirements/sub-requirements within reliability standards approved by applicable government authorities, for the applicable functions for which the applicable entity is registered; and,
2. Subject to the compliance monitoring and enforcement requirements of Section 400 of the Rules of Procedure.

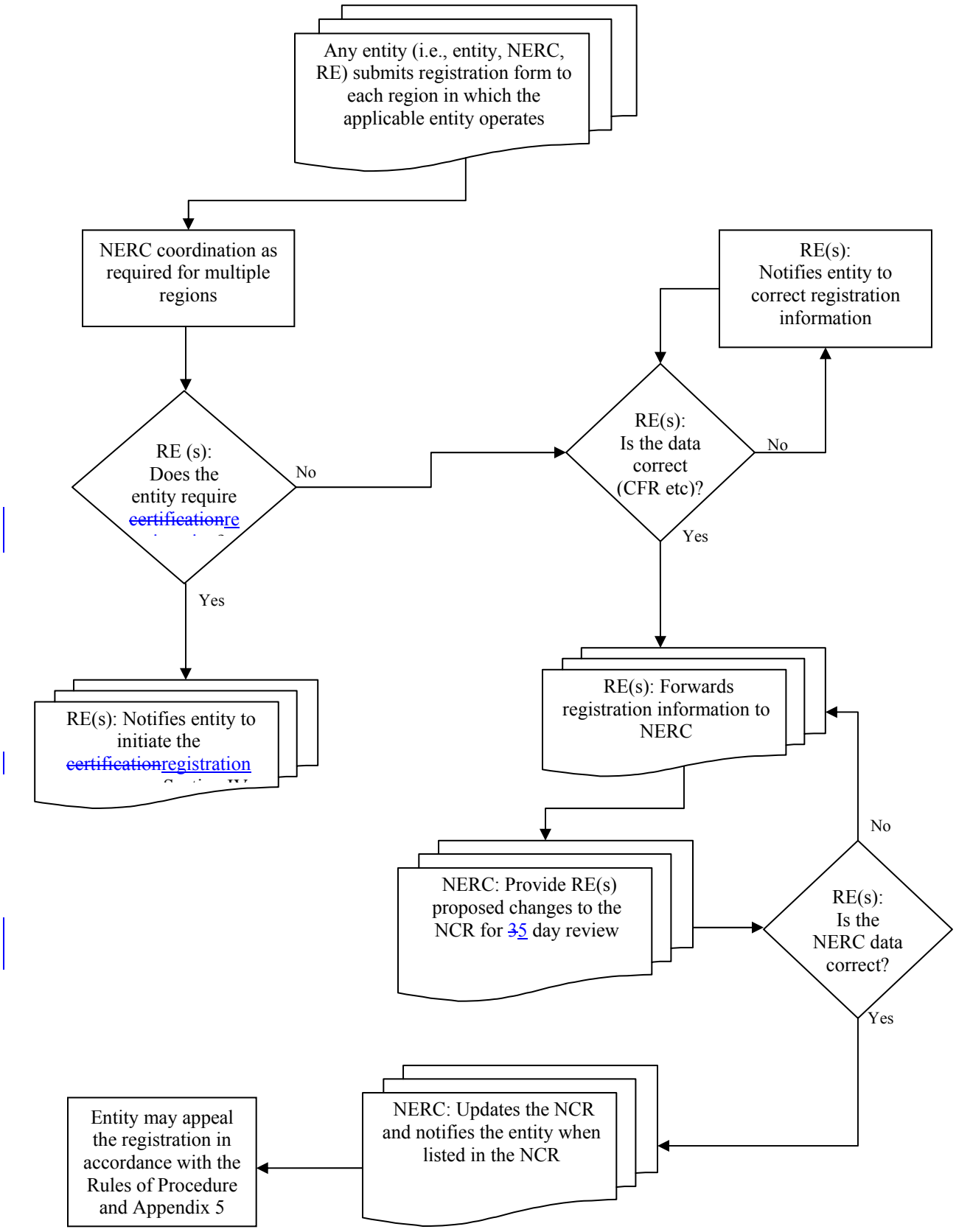
See Figure 1 *Organization Registration Process Overview.*

Organization Registration Process

1. Applicable entities shall begin the registration process by submitting a completed registration application~~-~~ to the Regional Entit~~y~~(ies) ~~of the reliability region(s)~~ where the entity intends to perform its function(s) (registration forms are provided on each Regional Entity's ~~website~~website).
    a. At any time an entity may recommend in writing, with supporting documentation, to the Regional Entit~~y~~(ies) that an entity be added to or removed from the compliance registry.
    b. The registration process for an entity may also be initiated by a Regional Entity, NERC, or applicable governmental authority.
2. NERC shall coordinate registration of entities that are required to register with multiple Regional Entities in order to ensure consistency of the registration process.
3. For entities that are required to be certified, the applicable Regional Entit~~y~~(ies) shall ensure that the registration information provided is accurate for updating the NCR per~~-~~ items 4 through 12 below and notifies the entity to initiate the certification process per Section IV of this manual.
4. Entities that have a NERC ID shall use it on the form**.**
    a. If an entity does not have a NERC ID, NERC shall assign one.
    b. An entity responsible for more than one function will use a single NERC ID.

5. Regional Entities shall evaluate the submitted information and determine if the information is complete and ~~/~~correct. If the information is not complete and ~~/~~correct, the entity will be notified to ~~complete/~~correct ~~or~~ or clarify the registration information.
6. A single entity must register for all functions that it performs itself. In addition, that entity may register as a Joint Registration Organization (JRO) on behalf of one or more of its members or related entities for one or more functions for which such members or related entities would otherwise be required to register and, thereby, accept on behalf of such members or related entities all compliance responsibility for all requirements/sub-requirements of reliability standards applicable to that function or those functions including reporting requirements ~~.~~(Rules of Procedure Section 507).
7. Multiple entities may each register using a Coordinated Functional Registration (CFR) for one or more reliability standard(s) and/or for one or more requirements/sub-requirements within particular reliability standard(s) applicable to a specific function ~~.~~(Rules of Procedure Section 508).
8. In completing the regional entity responsibilities for the registration process, the following are key items the Regional Entity must verify:
    a. That Regional Entity registrations meet the geographical and electrical registration boundaries requirements of the Rules of Procedure Section 501(1.4).
    b. The registration submission includes all data requested by NERC that is necessary for accurately identifying and contacting the registered entity.
9. The Regional Entity shall forward all registration information to NERC:
    a. NERC forwards the proposed additions or changes to the NCR to the Regional Entity for review and comments.
    b. The Regional Entity has five (5) working days to respond to the proposed changes.
    c. If NERC does not receive any comments, the NCR will be revised.
10. NERC updates the NCR and notifies the applicable entity(ies) within 5 days of the update.
11. The entity may appeal the registration in accordance with the Rules of Procedure Section 500 and Section V of Appendix 5A.
12. The NCR shall be dynamic and will be revised as necessary to take account of changing circumstances such as corrections, revisions, and or deletions. Per the Regional Entity's delegation agreement, the Regional Entity will take any recommendation received under Section 1.a, and other applicable information, under advisement as it determines whether an entity should be ~~on the NCR~~registered, and, if so, advises NERC.
    a. Each entity identified in the NCR shall notify its corresponding Regional Entity and/or NERC of any corrections, revisions, deletions, changes in ownership, corporate structure, or similar matters that affect the entity's responsibilities with respect to the reliability standards. Failure to notify will not relieve the entity from any responsibility to comply with the reliability standards or shield it from any penalties or sanctions associated with failing to comply with the standards. (Rules of Procedure Section 400).

Figure 1: Organization Registration Process Overview



Section IV — Organization Certification Process

Purpose and Scope

The purpose and scope of this process is to provide guidance for completing the certification of a new entity that will become NERC certified and registered as an RC, ~~TOP, or BA~~BA or TOP or those entities that perform some or all of the reliability functions of an RC, BA or TOP.

Overview

See Figure 2 *Organization Certification Process Overview* for an overview of the certification process.

Organization Certification Process

1. Certification:

    a. An entity in a single ~~Regional Entity reliability~~ region shall initiate the certification process by completing a certification application (certification applications are provided on each Regional Entity's ~~website~~website) and sending it to the Regional Entity which will manage the certification process.

    b. An entity in multiple ~~Regional Entity reliability~~ regions shall initiate the certification process by completing a certification application (certification applications are provided on each Regional Entity's ~~website~~website) and sending it to the Regional Entities in those ~~reliability~~ regions. Each Regional Entity will inform NERC of the request. The Regional Entities will determine which Regional Entity will provide the leadership to manage the certification process.

    c. ~~Provisional Certification Process - All Reliability Coordinator Balancing Authorities, and/or Transmission Operators that were already registered and operating on June 18,2007 become "NERC Certified" upon completion of (1) a NERC Readiness Evaluation (on site activities completed by the evaluation team); and (2) a CMEP audit (on site activities completed by the audit team) after June 18, 2007. Recertification on a periodic basis of these entities will not be required. Demonstration of ongoing satisfactory performance of applicable RC, BA, and TOP functional requirements shall be accomplished by completion of a CMEP audit every three years per the requirements of the NERC Rules of Procedure~~.

~~2.~~

2. For an entity that is not required to be certified, the Regional Entit~~y~~(ies) shall reject the application and notify the entity that certification is not required.

3. If the application is not complete or accurate, the Regional Entity will notify the entity to revise the application as needed. When the application is deemed complete and accurate, it will be accepted. The entity, ~~and~~ the Regional Entity and NERC shall agree to a timeline including specific milestones for the certification process.

4. The decision to certify changes to an already operating and certified entity is a collaborative decision between NERC and the affected Regional Entit~~y~~(~~s~~ies) ~~and NERC~~. NERC has the

final authority regarding this decision. Items to consider for this decision include one or more of the following:

a. Changes to an entity's footprint or operational challenges (i.e., TLRs) due to the changes

b. Organizational restructuring that could impact the BPS reliability

c. Relocation of the control center(s)

d. Changes to entity ownership requiring major operating procedure changes

e. Significant changes to JRO / CFR assignments or agreements changes

f. Addition or removal of member JRO / CFR utilities or entities

g. Complete replacement of a SCADA/EMS system

5. The certification process shall be completed within nine months of the date of acceptance of the application unless agreed to by all parties involved in the process and approved by NERC.

6. The Regional Entit~~y~~(ies) shall notify NERC that the certification process has begun to enable NERC to carry out its roles and responsibilities.

7. The Regional Entity will send a questionnaire with a submission deadline and a statement of expectations to all entities participating in the certification process. These questionnaires and other related documents are located on the ~~NERC Web site~~NERC website. The Regional Entity shall distribute questionnaires and other related documents to the following entities, as required:

   a. Entity seeking certification.

   b. Participating ~~BAs~~RCs, ~~RCs~~BAs, and TOPs in footprints in which the entity intends to operate or with which the entity intends to interconnect transmission facilities.

   c. Participating TOs, TSPs, PAs, GOs, IAs, GOPs, TPs, DPs, and/or other applicable entities.

8. The Regional Entity shall assemble a Certification Team (CT) that will be responsible for performing the activities included in the certification process.

   a. The CT members shall adhere to NERC's confidentiality agreements for any data or information made available to the CT member through the certification process. Team members shall not be employees of or have a direct financial interest in the entity or any of its affiliates.

   b. The Regional Entity, with concurrence of NERC, may increase or decrease the distribution of the questionnaires and other related documents based upon the complexity of the certification.

   c. If the entity objects to any member of the CT, the entity must make that known, in writing, to the ~~Regional Entity~~Certification Team Lead listing the reasons for the objection. The Regional Entity will either replace the team member or respond with written justification for keeping the member on the team.

   d. CT composition

      i. The BA CT shall consist of representatives from an existing BA, the entity's proposed RC, TOP, each affected Regional Entity, and NERC.

ii. The RC CT shall consist of representatives from an existing RC, a BA and a TOP in the proposed RC area, each affected Regional Entity, and NERC.

iii. The TOP CT shall consist of representatives from an existing TOP, the entity's proposed RC, each affected Regional Entity, and NERC.

iv. Additional CT members with expertise in the any of the NERC registry functional areas can be added as necessary.

v. Additional CT members from NERC or Regional Entity staff may be added as necessary.

vi. Entities such as government representatives or other stakeholders may be observers in the certification process.

e. CT composition – Existing certified entity seeking to expand footprint

i. Where an existing certified, operating entity seeks to expand the footprint in which it operates and seeks certification for the expanded footprint, the CT shall consist, at a minimum, of representatives from NERC and from the Regional Entity or Regional Entities in which the proposed expanded footprint area lies.

ii. The CT may also include one or more representatives of an existing BA, RC and/or TOP.

~~i.~~iii. NERC and the Regional Entity or Regional Entities will consult with the entity seeking certification for an expanded footprint and reach consensus on composition of the CT.

9. Each CT member must complete the NERC auditor training prior to participation.

10. The CT will review the entity's submitted documentation and address any issues prior to the site visit.

11. The CT shall inform the entity before the on-site visit of any documentation or clarification that is necessary to support the questionnaires.

12. The entity shall identify to the CT prior to the on-site visit all standards or requirements/sub-requirements which have been delegated to another entity.

a. The CT will review the entity~~(ies)~~'s ability to perform those delegated requirements/sub-requirements or standards.

13. The CT shall conduct at least one on-site visit to the entity's facilities (unless only a minor change in the footprint of an existing certified entity is under review, in which case the CT may determine that an on-site visit is not necessary). At a minimum, the team will:

a. Review with the entity the data collected through the questionnaires, and such data that is available only onsite;

b. Interview the operations and management personnel;

c. Inspect the facilities and equipment associated with the applicable reliability standards referenced in the questionnaire;

d. Request demonstration of all tools identified in the certification process;

e. Review documents and data including agreements, processes, and procedures identified in the certification process;

f. Verify operating personnel NERC certification documents and proposed work schedules; and,

g. Review any additional documentation resulting from inquiries arising during the site-visit.

14. The entity, in conjunction with the CT, shall attempt to resolve any deficiencies prior to issuance of the draft report.

15. The draft report is provided to the entity for review for fourteen (14) days and any resulting comments will be assessed by the CT for possible inclusion in the report.

16. The Regional Entit~~y~~(ies) may grant a time extension, not to exceed 180 days, to the entity to allow the entity to resolve any open certification issues.

17. The CT shall provide a certification recommendation and identification of audit deficiencies in the final written report. All members of the CT shall have an equal voice in the certification recommendation. This allows for a minority opinion if the review team cannot reach a consensus. The final written certification report is distributed to NERC, the entity, and the other affected Regional Entities, as applicable.

18. The following is the format for the final report:

- Title ~~page~~Page
- Table of Contents
- Introduction – A brief discussion on the Regional Entit~~y~~(ies) involved, the entity being certified, a description of the function the entity(ies) are being certified for, and a brief timeline of the certification project
- Certification Team (CT) – Provide the team makeup.
- Objective and Scope – Discussion on entity application (who, what, when, & how).
- Overall Conclusion – Recommendation being made by the CT.
- Certification Team Findings – Any item(s) needing to be closed prior to operation that do not hinder the certification team from making a recommendation.
- Positive Observations.
- Company History – Discussion on the applicant's company history.
- Company Details– Specific details regarding why the entity is being certified and its relationship with other entities (BAs, RCs, and TOPs etc).
- Documentation List – Provide a list of critical documentation reviewed by the CT used to make the CT's conclusion and the documentation retention requirements.
- Attachments – Describe those attachments that are for public viewing and those that are separated from the report due to confidentiality issues such as Critical Infrastructure documentation.

19. Certification recommendation and approval.

a. If the entity intends to operate in a single Regional Entity's reliability region, the CT shall make a certification recommendation to that Regional Entity. The Regional Entity shall approve or disapprove the recommendation. The Regional Entity shall notify the entity and NERC of the certification decision.

b. If the entity intends to operate in multiple Regional Entities, the CT shall make a certification recommendation to all applicable Regional Entities in a single report. Certification recommendation by the Regional Entities must be unanimous. The Regional Entities shall notify the entity and NERC of the certification decision.

c. NERC shall approve or disapprove all final certification recommendations and notify the entity of the decision.

20. The entity may appeal the decision in accordance with the NERC Rules of Procedure and Section VI of this manual.

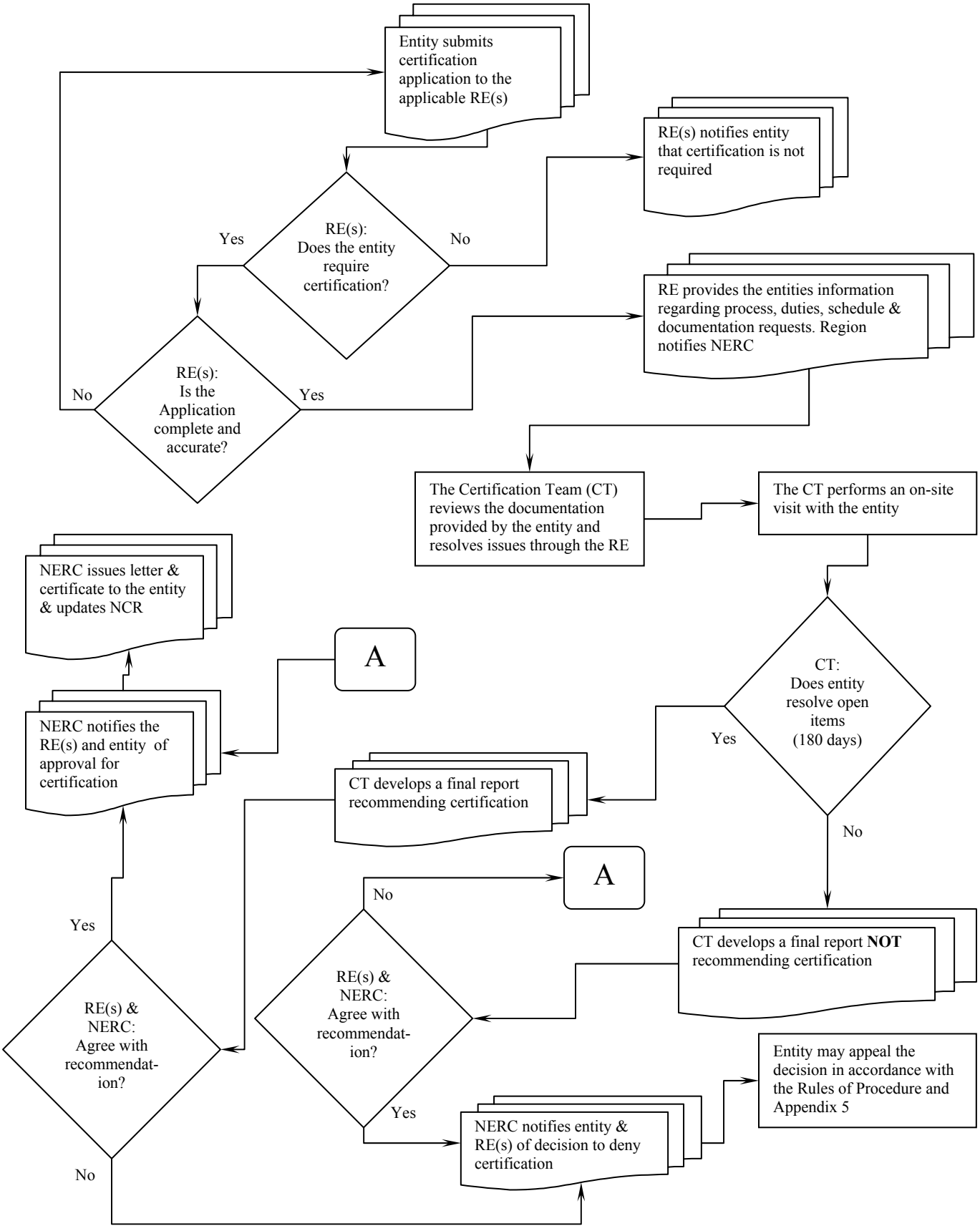
21. If the entity is approved for certification, NERC shall provide the entity a certification letter and a NERC certificate indicating that that entity is NERC certified as a BA, RC, and/or TOP as applicable.

    a. For those CFR entities that agree upon a division of compliance responsibilities for one or more reliability standards or requirements/sub-requirements, NERC shall provide all entities responsible for BA, RC and/or TOP requirements/sub-requirements and approved for certification as BA, RC and/or TOP a NERC certificate indicating that those entities are NERC certified as a BA, RC, and/or TOP.

    b. NERC shall update the registry ~~prior to the entity(s) going operational~~in accordance with the registration rules.

22. After the entity has been awarded certification, ~~the Regional Entity(ies)~~ NERC shall notify all applicable entities as to the date that the entity may begin its operation as a certified entity. The entity must commence operation within 12 months of certification. Failure to begin operation within the 12-month period shall require the entity to reapply for certification.

Figure 2: Organization Certification Process Overview



Section V — NERC Organization Registration Appeals Process

Purpose and Scope

This section describes the process that any organization may appeal its listing and functional assignment on the NCR.

Overview

NERC has established documented procedures to ensure a fair and impartial appeals process. No one with a direct interest in a dispute may participate in the appeals process except as a party or witness. See Figure 3, *Organization Registration Appeals Process Overview*.

Organization Registration Appeals Procedure

Any entity included on the NCR may challenge its listing and functional assignments with NERC.

1. All registration appeals must be filed in writing to NERC, via registered mail. Appeals are sent to:

   ~~Vice President and~~ Director of Compliance Operations
   North American Electric Reliability Corporation
   ~~116-390 Village Blvd.~~ 3353 Peachtree Rd NE
   Suite 600, North Tower
   ~~Princeton, New Jersey, 08540~~Atlanta, GA 30326

2. Each party in the appeals process shall pay its own expenses for each step in the process.

3. A stipulation of invoking the appeals process is that the Regional Entity or entity requesting the appeal agrees that NERC (its members, Board of Trustees, committees, subcommittees, and staff), any person assisting in the appeals process, and any company employing a person assisting in the appeals process, shall not be liable for, and shall be held harmless against the consequences of or any action or inaction or of any agreement reached in resolution of the dispute or any failure to reach agreement as a result of the appeals proceeding. This "hold harmless" clause does not extend to matters constituting gross negligence, intentional misconduct, or a breach of confidentiality.

4. Parties retain the right to seek further review of a decision in whatever regulatory agency or court that may have jurisdiction.

5. All appeals must be received within 21 days of receipt of the NERC letter informing the entity that it is listed on the NCR. The appeal must state why the entity believes it should not be registered based on the NERC Rules of Procedure and the *NERC Statement of Compliance Registry Criteria.*

6. After receipt of the appeal, the ~~r~~Registered ~~e~~Entity has a 30 day period to work with the Regional Entity to resolve the appeal, if possible. If the appeal is resolved, the Regional Entity will notify NERC with the details of the resolution and NERC will close the appeal.

7. At any time through this appeals process, an entity may agree with the decision and/or agree to close the appeal. NERC shall notify the involved parties and the NERC Board of Trustees Compliance Committee (BOTCC) that the appeal is resolved and update the NCR as applicable.

8. NERC will notify the entity and the applicable Regional Entit~~y~~(ies) regarding the appeal with the following expectations:

    a. The entity will provide NERC and the applicable Regional Entit~~y~~(ies) any additional data supporting its appeal within 10 days of the date of the NERC appeal notification.

    b. The applicable Regional Entit~~y~~(ies) will provide a copy of its assessment directly to the entity, as well as to NERC, within 20 days of the date of the NERC appeal notification.

    c. The entity may submit a response to the Regional Entit~~y~~(ies) assessment, with copies to the Regional Entit~~y~~(ies) and NERC, within 30 days of the date of the NERC appeal notification.

    d. To ensure there is no confusion with respect to the rights and responsibilities of the entity during the appeal process, the notification also confirms whether the entity will remain on the NERC Compliance Registry and will be responsible for compliance with approved reliability standards applicable to the function under appeal during the appeal.

9. Hearing and Ruling by the BOTCC

    a. The BOTCC will resolve registration disputes.

    b. The BOTCC may request additional data from NERC, the relevant Regional Entit~~y~~(ies) or the entity, and prescribe the timeframe for the submitting the requested data.

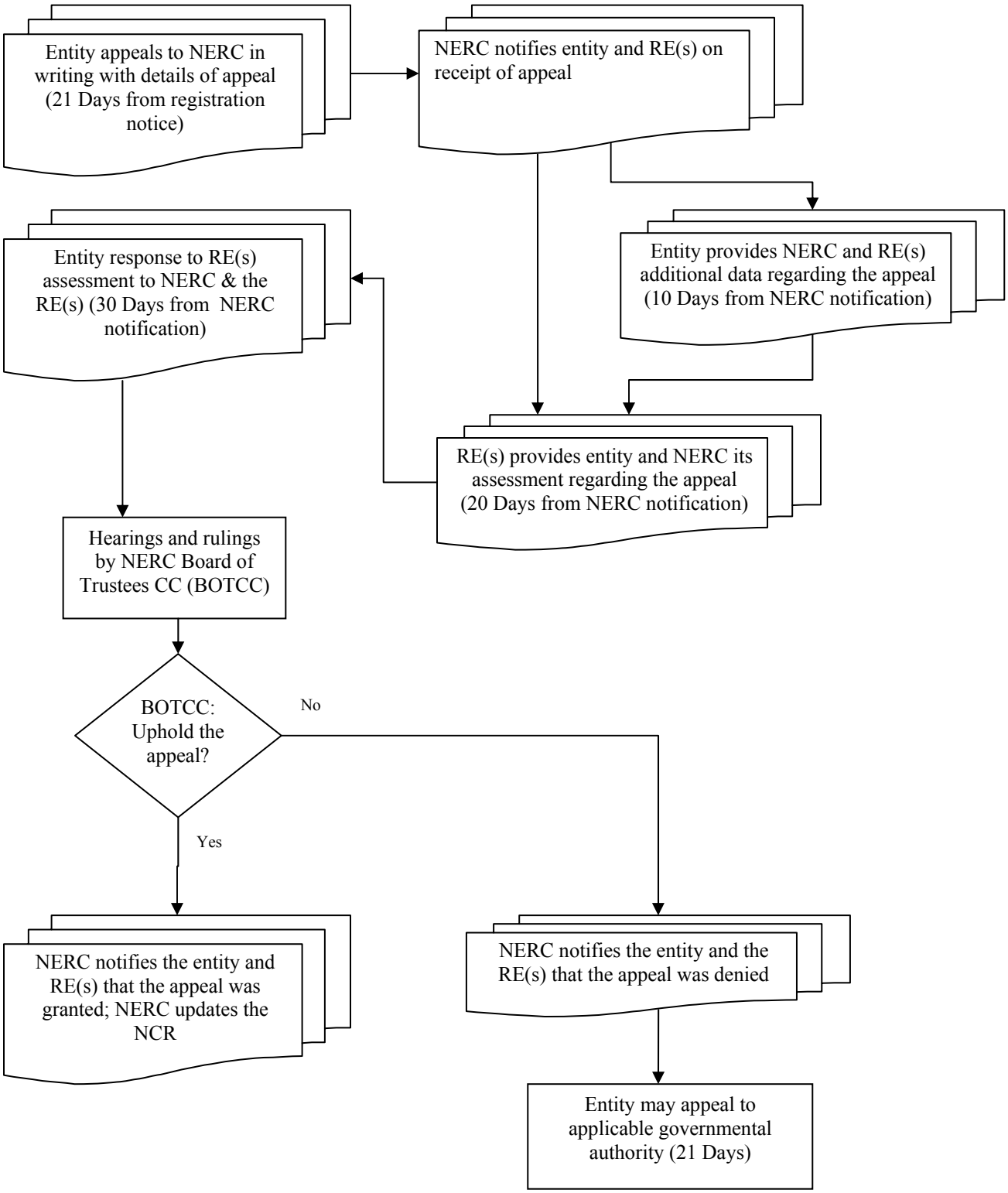
    c. The BOTCC will provide a written decision regarding any appeals, along with the basis for its decision.

    d. If the BOTCC upholds the appeal, NERC will:
        - Notify the entity and Regional Entit~~y~~(ies) that the appeal was granted.
        - Update the NCR.

    e. If the BOTCC does not uphold the appeal, NERC will:
        - Notify the entity and the Regional Entit~~y~~(ies) that the appeal was denied.
        - The entity may appeal to FERC or applicable Canadian Provincial regulator within 21 days of the notification of the decision.

f. A record of the appeals process shall be maintained by NERC. Confidentiality of the record of the appeal will be based on the NERC Rules of Procedure Section 1500.

Figure 3: Organization Registration Appeals Process Overview



Section VI — NERC Organization Certification Appeals Process

Purpose and Scope

This section describes the process for an organization to appeal the certification decision that was determined in the certification process.

Overview

The NERC Organization Certification Program provides a key means to fulfill NERC's mission. In conducting this program, NERC has established documented procedures to ensure a fair and impartial appeals process. No one with a direct interest in a dispute may participate in the appeals process except as a party or witness. See Figure 4 *Organization Certification Appeals Process Overview*.

Organization Certification Appeals Procedure

1. Appeal for an Organization Certification Finding.

   Any entity can appeal an organization certification decision issued as a result of the certification process.

2. Requirements and Conditions for Appeals.

   a. For all appeals under the NERC Organization Certification Program, the appeals process begins when an entity notifies the NERC ~~Vice President and~~ Director of Compliance Operations, in writing, that it wishes to use the NERC appeals process.

      - The ~~Vice President and~~ Director of Compliance Operations is the main contact for all parties in all steps of the appeals process.
      - If an appeal is not filed within twenty one (21) days ~~of~~following (i) the date that the certification report or finding is issued, or (ii) the date that a final ruling in a Regional Entity appeals process ~~ruling~~ is made, the finding shall be considered final and un-appealable.

   b. Each party in the appeals process shall pay its own expenses for each step in the process.

   c. A stipulation of invoking the appeals process is that the Regional Entity or entity requesting the appeal agrees that NERC (its members, Board of Trustees, committees, subcommittees, and staff), any person assisting in the appeals process, and any company employing a person assisting in the appeals process, shall not be liable, and shall be held harmless against the consequences of or any action or inaction or of any agreement reached in resolution of the dispute or any failure to reach agreement as a result of the appeals proceeding. This "hold harmless" clause does not extend to matters constituting gross negligence, intentional misconduct, or a breach of confidentiality.

   d. Parties retain the right to seek further review of a decision in whatever regulatory agency or court that may have jurisdiction.

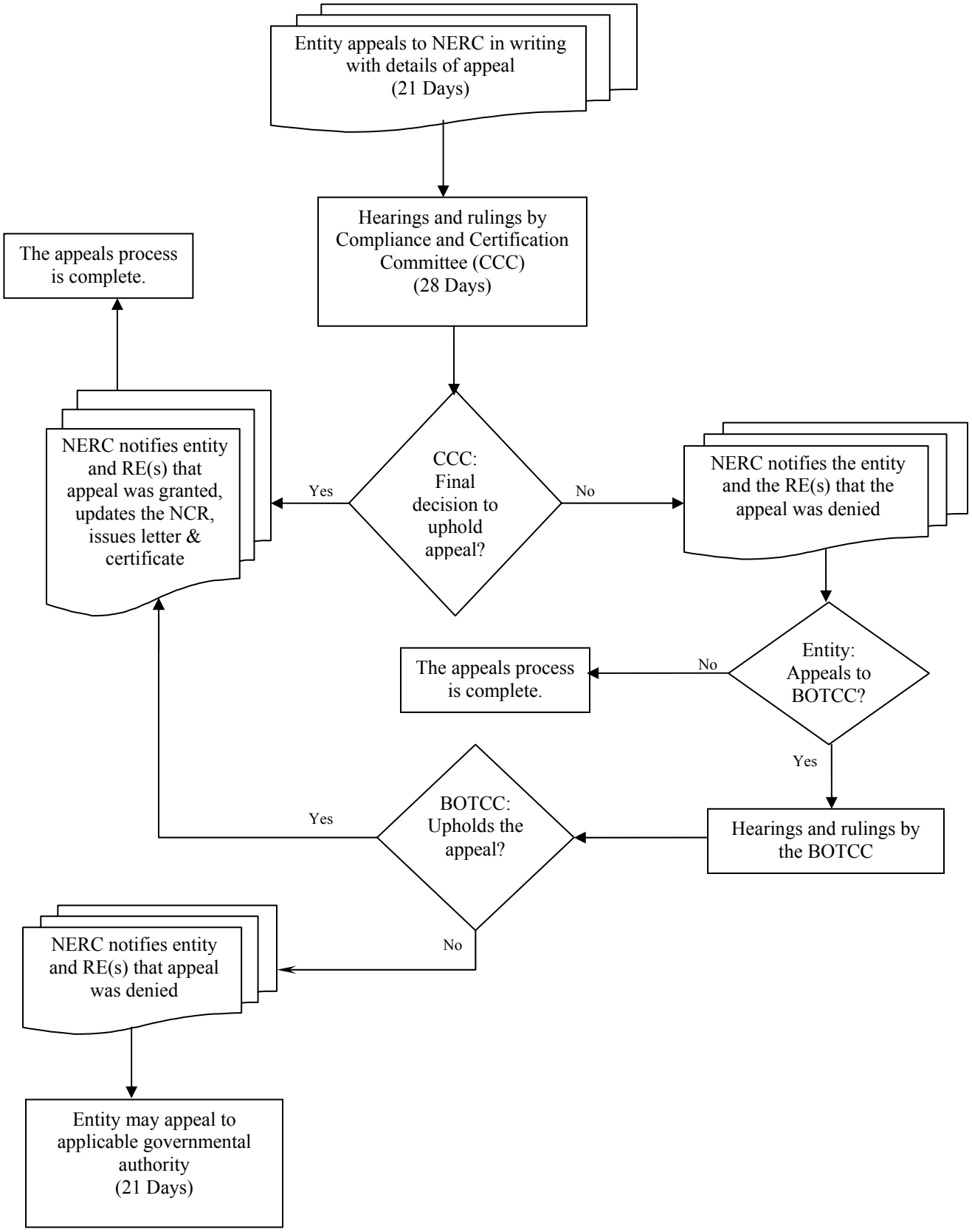
3. At any time through this appeals process, an entity may withdraw its appeal.
4. Hearing and Ruling by the Compliance and Certification Committee.
   a. Within twenty-eight (28) days of receiving notice from the NERC ~~Vice President and~~ Director of Compliance Operations, the CCC will conduct a hearing where all the parties or representatives of the disputing parties will present the issue in question, in accordance with CCC procedure CCCPP-005, *Hearing Procedures for Use in Appeals of Certification Matters*.
   b. If the appeal is upheld, NERC notifies the entity and RE(s), updates the NCR, and issues any appropriate letter and certificate to the entity.
   c. If the appeal is denied, NERC notifies the entity and RE(s).
5. Hearings and Ruling by the BOTCC.
   a. The BOTCC will be asked to resolve a dispute related to the NERC Organization Certification Program if any party to the appeal contests the CCC final order.
   b. The BOTCC may request additional data from NERC, RE(s) or the entity and prescribe the timeframe for the submitting the requested data.
   c. At the next regularly scheduled BOTCC meeting, or at a special meeting if the Board determines it is necessary, the Chairman of the CCC will present a summary of the dispute and the actions taken to the Board.
      - Each party will have an opportunity to state its case.
      - The BOTCC will then rule on the dispute.
   d. Based on~~If~~ the BOTCC's ruling on ~~upholds~~ the ~~appeal~~dispute, NERC will:
      - Notify the entity and the Regional Entit~~y~~(ies) as to the BOTCC's ruling and provide copies of the decision~~that the appeal was upheld~~.
      - Update the NCR as necessary based on the BOTCC's decision.
      - Issue a certification letter and a certificate to the entity ~~as~~if applicable based on the BOTCC's decision.

   ~~□~~eIf the BOTCC denies an~~does not uphold the~~ appeal by an entity, ~~NERC will notify the entity and the Regional Entity(ies) that the appeal was denied.~~

   ~~□~~ Tthe entity may appeal to the applicable governmental ~~authorities~~authority within 21 days ~~of~~following the issuance of the decision.

   f. A record of the appeals process shall be maintained by NERC and available upon request. Confidentiality of the record of the appeal will be based on the NERC Rules of Procedure Section 1500.

Figure 4: Organization Certification Appeals Process Overview



Definitions

NERC Organization Certification	The process undertaken by NERC and a Regional Entity to verify that a new entity is capable of responsibilities for tasks associated with a particular function such as a Balancing Authority, Transmission Operator, and/or Reliability Coordinator.
Compliance and Certification Manager	The individual/individuals within the Regional Entity that is/are responsible for monitoring compliance of entities applicable NERC Reliability Standards.
Days	Days as used in the registration and certification processes are defined as calendar days.
Footprint	The geographical or electric area served by an entity.
Functional Entity	An entity responsible for a function that is required to ensure the reliable operation of the electric grid as identified in the NERC Reliability Standards.
Mapping	The process of determining whether a Regional Entity's footprint is being served by Registered Entities.
NERC Identification Number (NERC ID)	A number given to NERC Registered Entities that will be used to identify the entity for certain NERC activities. Note: corporate entities may have multiple NERC IDs to show different corporate involvement in NERC activities.
Regional Entity	NERC works with eight Regional Entities to improve the reliability of the BPS ~~bulk power system~~. The members of the Regional Entities come from all segments of the electric industry. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. NERC delegates enforcement authority to these Regional Entities (FRCC, RFC, SPP, TRE, NPCC, MRO, SERC, & WECC).
Registration	Process undertaken by a Regional Entity to identify which entities are responsible for reliability functions within the Regional Entity's footprint.
Coordinated Functional Registration (CFR)	Where two or more entities (parties) agree in writing upon a division of compliance responsibility among the parties for one or more reliability standard(s) applicable to a particular function, and/or for one or more requirement(s)/sub-requirement(s) within particular reliability standard(s).

Appendix 8

Proposed Revisions 11-7-2011

NERC Event Response Procedures

Effective _____, 2012

North American Electric Reliability Corporation

NERC Event Response Procedures

Introduction

This Appendix provides a structured and detailed framework which defines the roles and responsibilities of NERC, the Regional Entities, and registered entities in conducting analyses of events that occur on the bulk power system (BPS).

The Electric Reliability Organization (ERO) enterprise-wide event analysis program is based on the recognition that BPS system events that occur, or have the potential to occur, have varying levels of significance. The manner in which registered entities, Regional Entities and NERC evaluate, respond and process these events is intended to reflect either the significance of the event or specific system conditions germane to the reliability of the BPS and the circumstances involved, or both.

When a BPS event occurs, the entities involved must first recognize it, then respond to it, and ultimately stabilize the system. Once the system has been stabilized, event analysis can begin.

Event analysis is the aggressive critical self analysis of BPS events that have occurred or have the potential to cascade. This analysis produces findings, lessons learned and best practices that provide experience-based insight in order to prevent repeat occurrences, provide informational material for entity training and industry learning, and institutionalize knowledge.

Event analysis begins with the registered entities that experienced the event, or circumstances surrounding a potential event, and depends upon collaboration between the registered entities, the Regional Entities, and NERC. The delineation between event categories is based on event significance and potential impact to the BPS. The significance and potential impact will drive the level of analysis for a particular event.

Critical components of an effective event analysis effort include the following:

- Prioritization of events affecting reliability of the BPS – detailed analysis for significant events and concise reviews for minor events
- Establishment of a clear timeline illustrating the sequence of events
- Specific identification of the causal factors of the event
- Identification and timely implementation of corrective actions
- Development and dissemination of alerts, quality lessons learned and best practices to the industry
- Emphasis on an aggressive critical self analysis by registered entities
- Emphasis on being a learning organization, including proactive improvement of BPS reliability
- Process transparency and predictability
- Proper confidentiality of data and information
- Identification of emerging trends discovered through event analysis

- Clarity and certainty about event analysis roles, responsibilities, and expectations for respective entities, including target timeframes for completing certain actions
- Appropriate Regional Entity and NERC review and oversight of registered entity event analysis results

Categorization of Events

Events are classified into one of five categories referred to as Category 1 (least significant) to Category 5 (most significant) based on the criteria specified in the "Event Category and Level of Analysis" Appendix to the NERC *ERO Event Analysis Process*. The categories of events and the criteria for determining the category into which an event should be classified may be revised by NERC based on experience and technical input. Any such revisions will be implemented in the *ERO Event Analysis Process*. However, an event may be assigned to a higher or lower Category based on the significance of the event. For these purposes, the following levels of significance will be considered: Significant, Conditionally Significant, Consequential and Noteworthy, Non-Consequential but Noteworthy, or Not Consequential:

Significant – The event caused or had the potential to cause an appreciable reduction in bulk power system reliability, excessive risk to generation and/or transmission facilities and serious harm to individuals. A Significant event results from the breakdown of multiple defenses and barriers and/or a non-adherence to one or more reliability standards. A Significant event will normally correspond to a Category 4 or 5 event. However, even if an event does not meet the criteria to be classified as a Category 4 or Category 5 event, it may be determined to be Significant based on the above-described cause(s) and impact(s) and one or more or the following considerations:

Significant by Act of Sabotage – The event involves a coordinated effort of sabotage or terrorism to the bulk power system.

Significant by Recurring – The event is similar to a previously-reported Significant event and should have been avoided by implementation of NERC Alerts or recommendations or lessons learned from previous event analysis.

Significant by Alert – The event is of a type that has been described in a previously-issued NERC Alert, usually in the format of a Recommendation or a Essential Action.

The NERC Director of Reliability Risk Management, with input from applicable Regional Entity management and applicable governmental authority staff and subject to approval by the NERC President and CEO, will determine if an event should be classified as Significant.

Conditionally Significant – An event is classified as Conditionally Significant based on the uniqueness of the event and other factors outside of common occurrences or reliability concerns. Among other factors, an event may be classified as Conditionally Significant (i) based on the event drawing substantial attention from federal or state governmental authorities and from the media, or (ii) due to the presence of unusual external conditions such as tornados, hurricanes, earthquakes, fires, floods or explosions

that create lengthy unplanned outages of generation or transmission elements or result in operation of the bulk power system at a significantly reduced capability.

The NERC Director of Event Analysis and Investigations, with input from applicable Regional Entity management and Applicable Governmental Authority staff and subject to approval by the NERC President and CEO, will determine if an event should be classified as Conditionally Significant.

Consequential and Noteworthy– The event caused an unexpected change in generation or other bulk power system conditions. The event should produce lessons learned and the possibility of a NERC Alert for dissemination. A Consequential and Noteworthy event will normally correspond to a Category 1, 2 or 3 Event.

Non-Consequential but Noteworthy – The event did not result in notable consequences but had the potential to be an event that would have more severe consequences under slightly different circumstances (e.g., a "near miss"). The event may produce lessons learned for bulk power system users, owners and operators.

Not Consequential – The event resulted in minimal or no consequences and there would be no value to analyzing it.

In this Appendix, the term "major event" is intended to refer to a Category 4 or 5, or a Significant or Conditionally Significant, event; and the term "other event" is intended to refer to a Category 1, 2 or 3, or a Consequential and Noteworthy, Non-Consequential but Noteworthy, or Not Consequential event. However, for purposes of determining and assigning responsibilities for the analysis of an event, an event may be determined to be "major" even though it does not meet the criteria or have the characteristics of a Category 1 or 2, or a Significant or Conditionally Significant event.

Responsibility for Event Analysis Based on Category or Significance of Event

NERC's role following an event affecting the bulk power system, including a major event such as a significant loss of load or generation, significant bulk power system disturbance, or other emergency on the bulk power system, is to provide leadership, coordination, technical expertise, and assistance to the industry in responding to the major event. Generally, NERC will take the lead role in the analysis of a major event, while the applicable Regional Entity or the registered entity will be responsible for the event analysis in the case of another event.

Response to and Analysis of Major Events

In the case of a major event, NERC, working closely with the Regional Entities and Reliability Coordinators, will coordinate efforts among industry participants, and with state, federal, and provincial governments in the United States and Canada to support the industry's response.

When responding to any major event where physical or cyber security is suspected as a cause or contributing factor to the major event, NERC will immediately notify appropriate government agencies and coordinate its analysis with them.

Following the occurrence of a major event, a planning meeting involving the affected registered entities, applicable Regional Entities, NERC, and other applicable governmental authorities (AGA) is held to discuss the event and to determine how the event analysis should proceed. The analysis of major events will be conducted by an event analysis team led by the applicable Regional Entities or NERC.

As specified in the ERO Rules of Procedure, Section 807.f, the NERC President and CEO has the authority to determine whether any event warrants analysis at the NERC level. A Regional Entity may request that NERC elevate an analysis of a major event to the NERC level.

If the analysis is led by a Regional Entity, then NERC staff and other appropriate technical experts from the NERC community will participate, as needed, as members of the Regional Entity analysis team.

During the conduct of NERC-level analyses, assistance may be needed from government agencies. Collaborative analysis with certain government agencies may be appropriate in some cases; e.g., collaborating with the Nuclear Regulatory Commission technical staff when a major event involves a nuclear unit. This assistance could include: authority to require data reporting from affected or involved parties; communications with other agencies of government; analyses related to possible criminal or terrorist involvement in the major event; resources for initial data gathering immediately after the major event; authority to call meetings of affected or involved parties; and technical and analytical resources for studies. If a federal or multi-national government analysis is called for, government agencies should work in primarily an oversight and support role, in close coordination with the NERC analysis.

If any Applicable Governmental Authority initiates a formal review process in conjunction with NERC, the decision on the composition of the event analysis team, the team lead, the information needed from affected registered entities, and the required scope of the analysis will be discussed and agreed upon by the Applicable Governmental Authority and NERC executive staff.

NERC may lead analyses of occurrences other than major events as needed based on specific facts and circumstances such as insufficient Regional Entity resources. In addition, a Regional Entity may request NERC to elevate an analysis of an occurrence other than a major event to the NERC level. In such cases, the leadership of the analysis team will shift to NERC, and the Regional Entity may continue to participate.

Responding to major events involves four phases:

1. situation assessment and communications;
2. situation tracking and communications;
3. data collection, investigation, analysis and reporting (event analysis); and
4. Publishing of recommendations (lessons learned, best practices, and Alerts, if applicable).

Phase 1 — Situation Assessment and Communications

When leading an event analysis, NERC's primary roles in Phase 1 are to:

- Lead or coordinate an initial situation assessment;
- issue a data retention hold notice;
- call for the collection of and analyze necessary initial data and information for the major event;
- assist the Regional Entity-led analysis with determining the need for supplemental technical expertise from the NERC community;
- issue initial findings, conclusions, and recommendations;
- maintain detailed data records (not subject to Freedom of Information Act);
- assist government agencies in criminal analyses when relevant;
- provide technical expertise for modeling and analyzing the major event; and
- follow up on recommendations (responsibility of both NERC and the Regional Entity).

While conducting its initial situation assessment, NERC will make an early determination as to whether the cause of the major event may be related to physical or cyber security, and communicate as appropriate with government agencies.

Notice of a major event is typically received by the NERC Bulk Power System Awareness person on duty and relayed to other appropriate NERC personnel.[1] NERC performs an initial situation assessment by contacting the appropriate party or parties, and makes a decision as to whether to activate its crisis communications plan. At the initial stage in gathering information about an incident, it is critical to minimize interference with bulk power system operators who are in the process of restoring the system. To minimize interference with their work, NERC, in its capacity as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), should serve as the primary communications link with government agencies.

The ES-ISAC Concept of Operations (ConOps) specifies the operations plan, communications procedures, and logistics NERC will follow during normal conditions, emergencies, and National Security Special Events. The ConOps includes the primary points of contact (24x7) for the Federal Energy Regulatory Commission, U.S. Department of Energy, U.S. Department of Homeland Security, U.S. Nuclear Regulatory Commission, and Public Safety and Emergency Preparedness Canada.

It is important that during these early hours that NERC Bulk Power System Awareness, in coordination with government agencies, determines whether the major event was caused by the actions of criminal or terrorist parties. The results of this criminal assessment are essential to operators because if there is a possibility that the "attack" is still ongoing, restoration and response actions would need to be tailored to these circumstances. If NERC and government agencies deem it necessary for further criminal analyses, NERC will issue a formal notice to affected systems to retain all relevant information gathered during this phase and subsequent phases of analysis.

NERC Reliability Standards set forth specific criteria and procedures for reporting the bulk power system disturbances and events. These criteria and procedures are intended to provide a common basis for consistent reporting of abnormal system conditions and events that occur in North America. All registered entities that are subject to the requirements of NERC Reliability

[1] NERC maintains 24x7 contact information for its key personnel to facilitate such contacts.

Standard EOP-004 must report the information required by that Reliability Standard within the time periods specified. Reliability coordinators will use the Reliability Coordinator Information System (RCIS) as their primary method of communications to NERC. The NERC Bulk Power Situational Awareness Group is responsible for monitoring the RCIS for such notifications.

Depending on the scope and magnitude of the major event, NERC will issue media advisories in accordance with its NERC Crisis Action Plan and the NERC Communications Protocol Document.

Phase 2 — Situation Tracking and Communications

Based on the nature and severity of the major event, in Phase 2 NERC will continue to track progress in restoring the bulk power system and service to customers, and keep industry, government agencies, and the public informed. The most important thing to recognize in this phase is that the primary focus of Reliability Coordinators and Transmission Operators is the prompt restoration of the bulk power system. NERC will coordinate requests by government agencies for information from Reliability Coordinators and Transmission Operators, and serve as a conduit and coordinator between industry and government for regular status reports on the restoration.

As the major event continues, NERC will determine whether a detailed analysis of the major event should be conducted, and start to identify manpower requirements, data collection and retention requirements, and at what level the analysis should be conducted. If the major event is localized within a region, NERC will participate in the analysis of the major event led by the Regional Entity.

Phase 3 — Data Collection, Investigation, Analysis, and Reporting

Based on the scope, magnitude, and impact of a major event, during Phase 3 NERC may:

1. perform an overview analysis of bulk power system and generator response;
2. rely on one of its Regional Entities to lead the analysis and monitor the analysis results;
3. work with a Regional Entity in its analysis; or
4. conduct a NERC-level analysis.

The NERC President and CEO will decide, based on the initial situation assessment and consultation with others, including the NERC technical committee officers[2], if the situation constitutes a major event and whether a NERC-level analysis is warranted. If a NERC-level analysis is to be conducted, the NERC President and CEO will appoint the analysis team leader.

NERC reserves the right to elevate or augment an analysis performed by a Regional Entity pending the results of the Regional Entity analysis. Additional requests for analyses or supporting data may be made by NERC at any time in the analysis process.

A NERC-level analysis will comprise (a) collecting pertinent data on the major event; (b) constructing a detailed sequence of events leading to and triggering the major event; (c)

[2] NERC will maintain a list of 24x7 contact information for its technical committee officers.

assembling bulk power system models and data and conducting detailed bulk power system analysis to simulate conditions before and after the major event; (d) conducting a root cause analysis to determine causal factors, necessary corrective actions and any needed reliability mitigation; and (e) issuing findings, conclusions, and recommendations. The details of these five phases of the analysis are:

a. Collecting Pertinent Data on the Major Event

- Collect all pertinent logs, disturbance recorders, operator transcripts, and other bulk power system data pertaining to the major event.

b. Detailed Sequence of Events Leading to and Triggering the Major Event

- Construct a detailed sequence of events leading to and triggering the major event. Reconcile logs, disturbance recorders, operator transcripts, and other bulk power system data to create an accurate sequence of events.
- Enter and preserve all data in a secure data warehouse.

c. Detailed Bulk Power System Analysis

- Assess the sequence of events to determine critical times for study.
- Assemble the necessary bulk power system models and data from Regional Entity and registered entities to accurately model (with power flow and dynamic simulations) the conditions prior to the major event. Determine conditions at critical times prior to initiation of the major event, including an assessment of reliability margins in the time period preceding the major event.
- Analyze data from phasor measurement units, high-speed data recorders, digital fault recorders, digital relays, and system relay targets.
- Analyze generator and load performance, including underfrequency and undervoltage relay actions.
- Use the model information and sequence of events to dynamically model the trigger occurrences and the outage sequence. Identify the bulk power system phenomena that propagated the failure. Provide graphical results showing the nature of the cascade. Conduct additional analyses as initial findings identify the need for further study.

d. Cause Analysis

Cause analysis methodology and the tools used guides the overall analysis process by providing a systematic approach to evaluating root causes, causal factors and contributing factors leading to the event. Cause analysis enables the analysis process to develop a factual record leading to logical and defensible conclusions in the final events analysis (EA) report regarding the causes of the event.

e. Findings, Conclusions, and Recommendations

- Identify and assess causal factors contributing to the major event, including possible instability conditions, system protection mis-operations, generator actions, etc.
- Either identify or rule out man-made/criminal cyber or physical attacks on the bulk power system.

- Determine if the bulk power system components were being operated within equipment and system design criteria at the time of the major event.
- Assess the qualifications, training, SCADA/EMS tools, and communications available to bulk power system operators and Reliability Coordinators, and how effective these were leading up to and during the major event.
- Assess the adequacy of communications system and communications among bulk power system operators.
- Identify any issues regarding maintenance or equipment conditions that may have contributed to the outage.
- Determine whether bulk power system restoration procedures were available and adequate. Identify any issues that caused unexpected delays in the restoration of generators and loads.
- Identify the root causes[3] and contributing factors of the major event.
- Recommend actions to prevent major events in the future and to improve bulk power system reliability.
- Determine whether the design of bulk power system components was a contributing factor to the event.
- All compliance issues will be referred to the NERC Director of Enforcement.

Phase 4 — Follow-up on Recommendations

For Phase 4 NERC and the Regional Entities will follow up on specific recommendations coming from all analyses, whether done at the Regional Entity or NERC level. In certain cases, where government agencies have taken a direct role in the analysis, reports will be made to those agencies on progress in addressing the recommendations.

Event Analysis of Other Events

For events (category 1 – 3) the registered entity should follow the methodology and steps outlined in the current version of the ERO event analysis process. The basic steps are outlined below.

1. The registered entity makes an initial assessment of an event, which includes determining the initial event category.
2. If the event is a "qualifying event" (*i.e.* Category 1-5), a planning meeting is held with all involved parties.
3. The registered entity submits a brief report.
4. If the qualifying event is a Category 3 or higher, the registered entity must also submit an event analysis report (EAR).
5. Lessons learned and best practices (if any) are developed and shared with industry.
6. The event is closed.

For lower tiered events, registered entities perform the event analysis. Coordination of the analysis becomes more complicated for events that involve a broader geographic area, involve multiple registered entities, or include a complex set of facts and circumstances.

A planning meeting should be held by the registered entity and the applicable Regional Entity as soon as possible following the occurrence of a qualifying event. During the meeting, agreement should be reached on the event category, the level of analysis, a timeline for completion of the report, and the need for a data retention hold and draft or preliminary reports. The event analysis should have a level of detail and target timeframe commensurate with the nature and scope of the event. Although the category of the event provides general guidance on the level of analysis needed, these guidelines may be adjusted based on the overall significance of the event and the potential for valuable lessons learned.

Registered entities that reside in two Regional Entity footprints should notify both Regional Entities of an event that spans both Regions. Following the notification, the two Regional Entities will determine which one will coordinate the remaining steps of the event analysis process. When multiple registered entities are involved in or affected by an event, they should collaborate with the Regional Entity to determine if it is appropriate for each entity to prepare a report or for the entities to work together to prepare a single report.

Weather-Related Occurrences - If a weather-related occurrence falls within any of the categories it should be reported. The affected registered entities should focus on restoration efforts. After restoration is complete, the affected entities, in coordination with Regional Entities, will determine if any additional information or event analysis steps are needed.

Development of Lessons Learned from Events

Lessons learned as a result of an event analysis should be shared with the industry as soon as practical. Proposed lessons learned should be drafted by a registered entity and should be submitted to the applicable Regional Entity. The lessons learned should be detailed enough to be of value to others and should not contain data or information that is deemed confidential. When possible, one-line diagrams, other diagrams and representations should be included to enhance the information provided in the lessons learned. Vendor-specific information should not be included unless it is discussed and coordinated with the vendor. If dissemination of vendor-specific information is beneficial, it may be pursued outside the event analysis process.

Lessons learned will be reviewed by selected technical groups and NERC staff for completeness and appropriateness prior to posting.

In normal operations, events may occur on the bulk power system that do not meet the reporting thresholds of the defined event categories but may yield lessons of value to the industry. These lessons learned can include the adoption of unique operating procedures, the identification of generic equipment problems, or the need for enhanced personnel training. In such cases, an event analysis report would not be required; however, registered entities are encouraged to share with their Regional Entities any potential lessons learned that could be useful to others in the industry, and to work with the Regional Entity and NERC to develop the lessons learned for dissemination.

Reporting and Analysis Requirements for Registered Entities in Connection with Events

Registered entities are required to report the occurrence of defined BPS disturbances and unusual occurrences to the applicable Regional Entity and NERC in accordance with various NERC and Regional reliability standards and other requirements. **It should be noted that following the event analysis process does not relieve the registered entity from mandatory reporting requirements dictated by regulatory authorities or NERC standards.**

In addition, a registered entity involved in an event will be required to submit one or more of the following reports, depending on the category of the event: a Brief Report; an Event Analysis Report; and proposed lessons learned. The following table shows the reports and timing requirements, by category of event:

Event Category	Brief Report	Event Analysis Report	Lessons Learned	Close Event Analysis
1	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Not required	Within 30 business days (if applicable)	10 business days following receipt of Brief Report
2	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	(If requested) Within 30 business days of the event	Within 30 business days	30 business days following receipt of EAR
3	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 60 business days of the event	Within 60 business days	30 business days following receipt of EAR
4	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 180 business days of the event	Within 180 business days	60 business days following receipt of EAR
5	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 180 business days of the event	Within 180 business days	60 business days following receipt of EAR

The final Event Analysis Report should address corrective actions and recommendations related to the event's causal factors and any identified lessons learned. Positive outcomes identified during an event should be documented as a best practice. These are key parts of a continuous learning and improvement program.

Event Analysis Interface with Compliance

To support a strong culture of compliance, registered entities are expected to perform a compliance analysis and to develop a compliance self-assessment report proportional to the significance of the event/risk to the BPS for categorized events in which there could be a gap between actual system or human performance and the requirements of NERC or regional reliability standards. Registered entities are encouraged to submit a compliance self-assessment report to the Regional Entity compliance liaison proportional to the significance of the event/risk to the BPS for categorized events. This report should encompass a sufficiency review, proportional to the event's significance, of applicable standards associated with the event.

Registered entities who make a good faith effort to self-identify and self-disclose possible violations stemming from their event analyses will be afforded consideration in any enforcement action in accordance with the NERC *Sanction Guidelines*, **Appendix B** to the Rules of Procedure. If further analysis by the Regional Entity or NERC reveals other possible violations, the registered entity's participation and cooperation will be noted and considered.

For this reason, it is recommended that registered entities establish a liaison between their internal event analysis and compliance functions. This will provide a clearer understanding and a more efficient transfer of information from both an operational and a compliance standpoint, and it will facilitate a thorough standards review by the registered entity.

Any possible violations of reliability standards that were identified in the registered entity's compliance self-assessment should be self-reported by the registered entity through the existing Compliance Monitoring and Enforcement Program procedures, with a notification that they were discovered as a result of participating in the ERO event analysis program and completing a compliance self-assessment of the event.

As provided in **Appendix 4B**, *Sanction Guidelines*, of the NERC Rules of Procedure, if the registered entity is fully cooperative in the event analysis process, conducts a self-analysis of the event and submits a timely compliance self-assessment report, and submits self-reports of any possible violations of reliability standards and implements corrective and mitigating actions, then in any subsequent enforcement actions pursuant to the Compliance Monitoring and Enforcement Program, the registered entity's actions will be considered as mitigating factors in the determination of any penalties or sanctions for violations of reliability standards in connection with the event.

Attachment A

NERC Major Event Analysis Objectives, Analysis Approach, Schedule, and Status

Analysis Objective	Analysis Approach	Schedule	Status
Pre-Major Event Conditions			
1. What was the precursor sequence of events leading to the major event?	• Assemble data/alarm logs and time-stamped sequence information. • Develop and maintain an expanding database of log and time-stamped sequence information. • Develop a precursor sequence of high-level, events relevant to, and leading to initiation of the major event. • Reconcile the precursor sequence of events with those emerging from Regional Entities, RTOs, and operating entities.		
2. What time frames are relevant for assessment of bulk power system conditions prior to the major event? What points in time should be used to establish a baseline set of study conditions when the bulk power system was last known to be stable and within normal operating criteria?	• Referencing precursor sequence of events, determine relevant times to develop base case conditions (stable and within normal operating criteria). • Verify relevant time horizons and availability of bulk power system data at those times with Regional Entities, RTOs, and operating entities.		
3. What models and data can best simulate bulk power system conditions prior to and during the major event? What is the relevant scope of the bulk power system for detailed study (what is considered the boundary of the bulk power system to be studied and what is considered neighboring or external bulk power systems?)	• Identify up-to-date bulk power system model(s) appropriate for powerflow and transient and dynamic simulations (determine if detailed eastern interconnection model is needed or multi-regional model(s) are needed. • Identify what models are available in Regional Entities, RTOs, and operating entities. • Identify who will actually perform power flow, transient and dynamic simulations; hire contractor(s) as needed. • Identify and assemble data required for these models. • Develop and maintain a bulk power system data repository.		

Analysis Objective	Analysis Approach	Schedule	Status
4. What bulk power system conditions existed in the precursor time horizon leading up to the major event (at the times identified in 1)?	• Obtain and manage data for powerflow: bulk power system configuration, planned and unplanned outages, unit commitment and dispatch, interchange schedules, congestion conditions, reserves, loads, state estimator snapshots, deratings and limitations, frequency, etc. Identify who will maintain and run powerflow simulations. • Work with Regional Entities, RTOs, and operating entities to develop powerflow cases defining the base conditions for each relevant time, ensuring the powerflows model each critical juncture leading up to the major event. • Identify and review results of additional studies completed by reliability coordinators, RTOs and operating entities. • Assess the powerflow results with respect to steady state operating criteria (was the bulk power system within all known limits at each precursor time)?		
5. Were there any prior-existing abnormalities, instabilities, reliability criteria violations, or reliability issues in the precursor sequence time horizon? Prior to initiation of the major event were there any latent instability conditions that would suggest the bulk power system was at risk? Were the precursor conditions ones that had been previously studied by the entities involved? Were there adequate reserves with effective distribution? Were planned outages effectively coordinated?	• Work with Regional Entities, RTOs, and operating entities to obtain and manage transient and dynamic models for simulations. • Identify who will conduct transient and dynamic simulations and if external contractor(s) are required. • Conduct transient and dynamic simulations at each of the precursor study times. • Assess the stability of the bulk power system at each of these times and identify any latent reliability issues prior to initiation of the major event. • Consider creating a visual map of bulk power system conditions. • Document the limitations and assumptions of simulations affecting the certainty of the simulation results.		
Sequence of Events			
6. What was the sequence of events leading to and directly triggering the major event?	• Evaluate data logs, fault recorder data disturbance recorder data, and synchro-phasor measurement to establish a detailed sequence of events that initiated the major event. • Identify the sequence of events that directly led to the major event. • Review and reconcile these trigger events with Regional Entities, RTO, and operating entity analyses.		

Analysis Objective	Analysis Approach	Schedule	Status
7. What was the sequence of events during the major event?	• Evaluate logs and disturbance recorder data to establish sequence during the major event . (The sequence of events may follow multiple tracks.) • Review and reconcile this sequence with those constructed by Regional Entities, RTOs, and operating entities. • Consider developing 3-D, time-lapse visualization of the major event (U. of Minnesota and/or U. of Wisconsin).		
8. What was the cause of the major event in terms of electrical conditions and other related occurrences? Generally describe any bulk power system breakups, islanding, etc. Were there conditions of voltage or frequency collapse, or unstable oscillations? Was the sequence strictly a sequential "domino" effect of facility trips? What were the bulk power system conditions (snapshots) at key points during the major event?	• Assess triggering sequence and major event sequence to establish the causes for the major event in terms of electrical conditions and occurrences. • Select key points in sequence for simulation that are relevant for study and that can be accurately modeled. (It may not be possible to reconcile data sufficiently to recreate bulk power system conditions during the major event.) • To the extent possible, conduct simulations and assess results at each point during the major event. • Review and reconcile results with Regional Entities, and operating entities.		
9. Why did the major event extend as far as it did? What arrested the major event from extending further into other areas of the bulk power system?	• Using advanced analysis techniques, assess where and why the major event was arrested.		
10. How did affected non-nuclear generators respond during the major event? Were trips as expected and required by procedures and standards? Did non-nuclear generators remain connected and support the bulk power system in the manner they should have? Did any generator action, generator control functions, or generator protection systems contribute to the major event?	• Prepare a table of affected generators and actions they made leading up to and during the major event, including time-stamped unit trips, relays initiating unit trips, MW and MVar outputs, voltages, and frequency, etc. • Analyze the automatic (including relay trips) and operator-initiated actions of non-nuclear generators to determine whether actions were correct under the conditions or not. • Reconcile non-nuclear generator data and analysis with that of the Regional Entities, RTOs, and operating entities.		
11. How did nuclear generators respond leading up to and during the major event? Were trips as expected and required by procedures and standards? Were there any nuclear safety issues identified?	• Work with NRC to develop a table of sequence of actions and issues regarding affected nuclear generators (both ones that tripped and those that did not). • Refer nuclear issues to NRC for analysis, assisting in their analyses where appropriate.		

Analysis Objective	Analysis Approach	Schedule	Status
12. What was the sequence and amount of load lost? What directly caused load loss (e.g. under-frequency load shed, loss of transmission source, voltage collapse, relay actions, under/over frequency protection or stalls, etc.)	• Work with Regional Entities, RTOs, and operating entities to develop a description of load lost/impacted, by area. • Analyze and report the cause for load loss in each area.		
13. How did system protection and automated controls operate during the major event? Did they operate correctly or not?	• Assess each automatic trip of a transmission or generator facility for proper or improper relay actions. • Assemble and review Regional Entity and operating entity reviews of logs, disturbance reports, and relay targets/logs and reconcile with NERC data.		
14. Was any equipment damaged during the major event?	• Request information from Regional Entities, and operating entities on equipment damage, as appropriate. • Assess any transmission or generation facilities sustaining damage during the major event, and extent of damage.		
15. Did SCADA/EMS and data communications systems operate correctly during the major event? What problems were noted?	• Request information from Regional Entities and operating entities. • Identify and analyze any problems with SCADA/EMS and data communications at regional and operating entity levels.		
Reliability Standards/Procedures			
16. What NERC reliability standards were applicable to the major event? What violations occurred? Were NERC standards and policies sufficient?	• Compliance staff review NERC standards relevant to the major event and perform a compliance review.		
17. What Regional Entity reliability standards were applicable to the major event? What violations occurred? Were Regional Entity standards and policies sufficient?	• Request Regional Entities to review applicable standards and report compliance with those standards during the major event.		
18. Were any special operating procedures or other operating guidelines in effect and being observed leading up to the major event? Were these procedures sufficient?	• Review and analyze loop flow procedures with Regional Entities and operating entities, and report analysis results.		
19. What other RTO, Transmission Owner, Balancing Authority procedures were applicable? What violations occurred? Were the procedures sufficient?	• Request RTOs, Transmission Owners, Balancing Authorities to review applicable standards and compliance with existing reliability procedures and standards during the major event, and report results.		
Maintenance			

Analysis Objective	Analysis Approach	Schedule	Status
20. Are there any indications that maintenance of transmission or generation facilities may have contributed to the major event?	• Assess whether equipment or maintenance issues (e.g. tree trimming) contributed to the major event and investigate specifics in areas of concern. • Review Regional Entity assessments of maintenance issues that may have contributed to the major event.		
Personnel, Procedures, and Communications			
21. What conditions were operators and reliability coordinators aware of leading up to and during the major event? What information did they have to warn them of unsafe bulk power system conditions? What problems or concerns did they have? What did they observe during the major event? Were human errors made that contributed to the major event? If there were, what were the causes of the errors?	• Develop an interview guide to address procedural and operational issues. • Conduct onsite interviews with operating personnel and reliability coordinators involved. • Analyze interview data to corroborate with technical data and report conclusions.		
22. Were lines of authority clearly understood and respected in the time leading up to and during the major event, as well as during the restoration period?	• Identify critical instructions given and evaluate results. • Review documentation and effectiveness of assignments of operating and reliability authorities.		
23. What communications occurred among operating entities?	• Review voice communications logs. • Evaluate logs relevant to the major event and identify key interactions. Report conclusions.		
24. What were the qualifications (including certification status) and training of all operating personnel involved in the major event and their supervisors?	• Request certification status of all operating personnel from involved operating entities. • Conduct onsite review of training materials and records. • Conduct onsite review of operating procedures and tools		
25. Was the role and performance of the reliability coordinators as expected?	• Review the adequacy of reliability plans for the affected Regional Entities. • Review the actions of the affected reliability coordinators to determine if they performed according to plans. • Assess whether inter-area communications were effective, both at the control area and reliability coordinator levels.		
System Restoration			
26. Were black start and restoration procedures available and adequate in each area? Were they followed and were they adequate to the restoration task? Were pre-defined authorities respected during the restoration?	• Onsite audit of blackstart and restoration procedures and plans. • Analyze whether the plans and procedures were used and whether they were sufficient for this major event.		

Analysis Objective	Analysis Approach	Schedule	Status
27. What issues were encountered in the restoration that created unexpected challenges or delays? What lessons were learned in the restoration (both things that went well and things that did not).	• Solicit information from operating entities and Regional Entities regarding unexpected challenges and delays in restoration, and lessons learned. • Analyze what worked well and what did not in the restoration.		
System Planning and Design			
28. Were the conditions leading up to the major event within the design and planning criteria for the transmission systems involved?	• Request transmission owners and Regional Entities involved to report any violations of design or planning criteria prior to or leading up to the major event.		
Conclusions and Recommendations			
29. From a technical perspective, what are the root causes of this major event? What additional technical factors contributed to making the major event possible?	• Conduct a root cause analysis on the findings and data. Categorize results as "root cause" or "contributing factor". Focus on technical aspects.		
30. What are the significant findings and lessons learned resulting from the analysis regarding technical failures leading to the major event? What actions are recommended to avoid similar future major events and improve bulk power system reliability? What issues may be inconclusive and require future analysis?	• Draft report of significant findings, lessons learned, and recommendations.		
31. Final Report	• Prepare and coordinate publication of final report.		

Appendix 8

Proposed Revisions 11-7-2011

NERC ~~Blackout and Disturbance~~Event Response Procedures

Effective ~~October 18, 2007~~ _____, 2012

North American Electric Reliability Corporation

NERC ~~Blackout and Disturbance~~Event Response Procedures

Introduction

~~NERC, through its professional staff and the regional entities and their members, provide the best source of technical and managerial expertise for responding to major events that affect the bulk power system.~~

This Appendix provides a structured and detailed framework which defines the roles and responsibilities of NERC, the Regional Entities, and registered entities in conducting analyses of events that occur on the bulk power system (BPS).

The Electric Reliability Organization (ERO) enterprise-wide event analysis program is based on the recognition that BPS system events that occur, or have the potential to occur, have varying levels of significance. The manner in which registered entities, Regional Entities and NERC evaluate, respond and process these events is intended to reflect either the significance of the event or specific system conditions germane to the reliability of the BPS and the circumstances involved, or both.

When a BPS event occurs, the entities involved must first recognize it, then respond to it, and ultimately stabilize the system. Once the system has been stabilized, event analysis can begin.

Event analysis is the aggressive critical self analysis of BPS events that have occurred or have the potential to cascade. This analysis produces findings, lessons learned and best practices that provide experience-based insight in order to prevent repeat occurrences, provide informational material for entity training and industry learning, and institutionalize knowledge.

Event analysis begins with the registered entities that experienced the event, or circumstances surrounding a potential event, and depends upon collaboration between the registered entities, the Regional Entities, and NERC. The delineation between event categories is based on event significance and potential impact to the BPS. The significance and potential impact will drive the level of analysis for a particular event.

Critical components of an effective event analysis effort include the following:

- Prioritization of events affecting reliability of the BPS – detailed analysis for significant events and concise reviews for minor events
- Establishment of a clear timeline illustrating the sequence of events
- Specific identification of the causal factors of the event
- Identification and timely implementation of corrective actions
- Development and dissemination of alerts, quality lessons learned and best practices to the industry
- Emphasis on an aggressive critical self analysis by registered entities
- Emphasis on being a learning organization, including proactive improvement of BPS reliability
- Process transparency and predictability

- Proper confidentiality of data and information
- Identification of emerging trends discovered through event analysis
- Clarity and certainty about event analysis roles, responsibilities, and expectations for respective entities, including target timeframes for completing certain actions
- Appropriate Regional Entity and NERC review and oversight of registered entity event analysis results

Categorization of Events

Events are classified into one of five categories referred to as Category 1 (least significant) to Category 5 (most significant) based on the criteria specified in the "Event Category and Level of Analysis" Appendix to the NERC *ERO Event Analysis Process*. The categories of events and the criteria for determining the category into which an event should be classified may be revised by NERC based on experience and technical input. Any such revisions will be implemented in the *ERO Event Analysis Process*. However, an event may be assigned to a higher or lower Category based on the significance of the event. For these purposes, the following levels of significance will be considered: Significant, Conditionally Significant, Consequential and Noteworthy, Non-Consequential but Noteworthy, or Not Consequential:

Significant – The event caused or had the potential to cause an appreciable reduction in bulk power system reliability, excessive risk to generation and/or transmission facilities and serious harm to individuals. A Significant event results from the breakdown of multiple defenses and barriers and/or a non-adherence to one or more reliability standards. A Significant event will normally correspond to a Category 4 or 5 event. However, even if an event does not meet the criteria to be classified as a Category 4 or Category 5 event, it may be determined to be Significant based on the above-described cause(s) and impact(s) and one or more or the following considerations:

Significant by Act of Sabotage – The event involves a coordinated effort of sabotage or terrorism to the bulk power system.

Significant by Recurring – The event is similar to a previously-reported Significant event and should have been avoided by implementation of NERC Alerts or recommendations or lessons learned from previous event analysis.

Significant by Alert – The event is of a type that has been described in a previously-issued NERC Alert, usually in the format of a Recommendation or a Essential Action.

The NERC Director of Reliability Risk Management, with input from applicable Regional Entity management and applicable governmental authority staff and subject to approval by the NERC President and CEO, will determine if an event should be classified as Significant.

Conditionally Significant – An event is classified as Conditionally Significant based on the uniqueness of the event and other factors outside of common occurrences or reliability concerns. Among other factors, an event may be classified as Conditionally Significant (i) based on the event drawing substantial attention from federal or state

governmental authorities and from the media, or (ii) due to the presence of unusual external conditions such as tornados, hurricanes, earthquakes, fires, floods or explosions that create lengthy unplanned outages of generation or transmission elements or result in operation of the bulk power system at a significantly reduced capability.

The NERC Director of Event Analysis and Investigations, with input from applicable Regional Entity management and Applicable Governmental Authority staff and subject to approval by the NERC President and CEO, will determine if an event should be classified as Conditionally Significant.

Consequential and Noteworthy– The event caused an unexpected change in generation or other bulk power system conditions. The event should produce lessons learned and the possibility of a NERC Alert for dissemination. A Consequential and Noteworthy event will normally correspond to a Category 1, 2 or 3 Event.

Non-Consequential but Noteworthy – The event did not result in notable consequences but had the potential to be an event that would have more severe consequences under slightly different circumstances (e.g., a "near miss"). The event may produce lessons learned for bulk power system users, owners and operators.

Not Consequential – The event resulted in minimal or no consequences and there would be no value to analyzing it.

In this Appendix, the term "major event" is intended to refer to a Category 4 or 5, or a Significant or Conditionally Significant, event; and the term "other event" is intended to refer to a Category 1, 2 or 3, or a Consequential and Noteworthy, Non-Consequential but Noteworthy, or Not Consequential event. However, for purposes of determining and assigning responsibilities for the analysis of an event, an event may be determined to be "major" even though it does not meet the criteria or have the characteristics of a Category 1 or 2, or a Significant or Conditionally Significant event.

Responsibility for Event Analysis Based on Category or Significance of Event

NERC's role following an event affecting the bulk power system, including a ~~blackout or other major bulk electric~~major event such as a significant loss of load or generation, significant bulk power system disturbance, or other emergency on the bulk power system, is to provide leadership, coordination, technical expertise, and assistance to the industry in responding to the ~~event. Working closely with the regional entities and reliability coordinators, NERC~~major event. Generally, NERC will take the lead role in the analysis of a major event, while the applicable Regional Entity or the registered entity will be responsible for the event analysis in the case of another event.

Response to and Analysis of Major Events

In the case of a major event, NERC, working closely with the Regional Entities and Reliability Coordinators, will coordinate efforts among industry participants, and with state, federal, and provincial governments in the United States and Canada to support the industry's response.

When responding to any major event where physical or cyber security is suspected as a cause or contributing factor to ~~an~~the major event, NERC will immediately notify appropriate government agencies and coordinate its analysis with them.

Following the occurrence of a major event, a planning meeting involving the affected registered entities, applicable Regional Entities, NERC, and other applicable governmental authorities (AGA) is held to discuss the event and to determine how the event analysis should proceed. The analysis of major events will be conducted by an event analysis team led by the applicable Regional Entities or NERC.

As specified in the ERO Rules of Procedure, Section 807.f, the NERC President and CEO has the authority to determine whether any event warrants analysis at the NERC level. A Regional Entity may request that NERC elevate an analysis of a major event to the NERC level.

If the analysis is led by a Regional Entity, then NERC staff and other appropriate technical experts from the NERC community will participate, as needed, as members of the Regional Entity analysis team.

During the conduct of ~~some~~ NERC-level analyses, assistance may be needed from government agencies. Collaborative analysis with certain government agencies may be appropriate in some cases; e.g., collaborating with the Nuclear Regulatory Commission technical staff when a ~~system~~major event involves a nuclear unit. This assistance could include: authority to require data reporting from affected or involved parties; communications with other agencies of government; analyses related to possible criminal or terrorist involvement in the major event; resources for initial data gathering immediately after the major event; authority to call meetings of affected or involved parties; and technical and analytical resources for studies. If a federal or multi-national government analysis is called for, government agencies should work in primarily an oversight and support role, in close coordination with the NERC analysis.

~~It is critical to establish, up front, a clear delineation of roles, responsibilities, and coordination requirements among industry and government for the analysis and reporting of findings, conclusions, and recommendations related to major blackouts, disturbances, or other emergencies affecting the bulk power system.~~

~~Depending on the severity and of the event and the area impacted, the event analysis may be conducted either by NERC or by the impacted RE. If the analysis is conducted by the regional entity, NERC staff, at least one member of the NERC Event Analysis Working Group (in addition to the Event Analysis Working Group member from the impacted regional entity), and other appropriate technical experts from the NERC community will participate as members of the regional entity analysis team.~~
If any Applicable Governmental Authority initiates a formal review process in conjunction with NERC, the decision on the composition of the event analysis team, the team lead, the information needed from affected registered entities, and the required scope of the analysis will be discussed and agreed upon by the Applicable Governmental Authority and NERC executive staff.

~~A regional entity~~NERC may lead analyses of occurrences other than major events as needed based on specific facts and circumstances such as insufficient Regional Entity resources. In

addition, a Regional Entity may request NERC to elevate an analysis ~~to a NERC~~ of an occurrence other than a major event to the NERC level. In such cases, ~~all team responsibilities~~the leadership of the analysis team will shift to NERC, and the ~~regional entity~~Regional Entity may continue to participate ~~in the analysis on appropriate teams~~.

~~These procedures do not represent a "cookbook" to be followed blindly. They provide a framework to guide NERC's response to events that may have multiregional, national, or international implications. Experienced industry leadership would still be required to tailor the response to the specific circumstances of the event.~~

Responding to major ~~blackouts and other system disturbances can be divided into~~events involves four phases:

1. situation assessment and communications;
2. situation tracking and communications;
3. data collection, investigation, analysis and reporting (event analysis); and
4. ~~follow-up on~~Publishing of recommendations (lessons learned, best practices, and Alerts, if applicable).

Phase 1 — Situation Assessment and Communications

When leading an event analysis, NERC's primary roles in Phase 1 are to:

- ~~conduct~~Lead or coordinate an initial situation assessment;
- issue a data retention hold notice;
- call for the collection of and analyze necessary initial data and information for the major event;
- assist the ~~regional entity-lead~~Regional Entity-led analysis with determining the need for supplemental technical expertise from the NERC community;
- issue initial findings, conclusions, and recommendations;
- maintain detailed data records (not subject to Freedom of Information Act);
- assist government agencies in criminal analyses when relevant;
- provide technical expertise for modeling and analyzing the major event; and
- follow up on recommendations (responsibility of both NERC and the Regional Entity).

While conducting its initial situation assessment, NERC will make an early determination as to whether the cause of the major event may be related to physical or cyber security, and communicate as appropriate with government agencies.

Notice of a major event is typically received by the NERC ~~Electricity Sector Information Sharing and Analysis Center (ESISAC)~~Bulk Power System Awareness person on duty and relayed to other appropriate NERC personnel.[1] NERC performs an initial situation assessment by contacting the appropriate ~~reliability coordinator(s)~~party or parties, and makes a decision ~~on~~as to whether to activate its crisis communications plan. At the initial stage in gathering information about an incident, it is critical to minimize interference with bulk ~~electric~~power system operators who are in the process of restoring the system. To minimize interference with their work,

[1] NERC maintains 24x7 contact information for its key personnel to facilitate such contacts.

NERC, in its capacity as the ~~ESISAC~~Electricity Sector Information Sharing and Analysis Center (ES-ISAC), should serve as the primary communications link with government agencies.

The ~~ESISAC~~ES-ISAC Concept of Operations (ConOps) specifies the operations plan, communications procedures, and logistics NERC will follow during normal conditions, emergencies, and National Security Special Events. The ConOps includes the primary points of contact (24x7) for the Federal Energy Regulatory Commission, U.S. Department of Energy, U.S. Department of Homeland Security, U.S. Nuclear Regulatory Commission, and Public Safety and Emergency Preparedness Canada.

It is important that during these early hours ~~the ESISAC~~that NERC Bulk Power System Awareness, in coordination with government agencies, ~~determine~~determines whether ~~this~~the major event was caused by the actions of criminal or terrorist parties. The results of this criminal assessment are essential to operators because if there is a possibility that the "attack" is still ongoing, restoration and response actions would need to be tailored to these circumstances. If NERC and government agencies deem it necessary for further criminal analyses, NERC will issue a formal notice to affected systems to retain all relevant information gathered during this phase and subsequent phases of ~~an~~ analysis.

~~The~~NERC Reliability Standards set forth specific criteria and procedures for reporting the bulk power system disturbances and ~~other events are described in NERC Reliability Standard EOP-004-1.~~events. These criteria and procedures are intended to provide a common basis for consistent reporting of abnormal system conditions and events that occur in North America. All registered entities ~~responsible for the reliability of bulk power systems in North America must ensure that sufficient information is submitted to NERC~~that are subject to the requirements of NERC Reliability Standard EOP-004 must report the information required by that Reliability Standard within the time ~~frame required~~periods specified. Reliability coordinators will use the Reliability Coordinator Information System (RCIS) as ~~the~~their primary method of communications to NERC. The ~~ESISAC duty person~~NERC Bulk Power Situational Awareness Group is responsible for monitoring the RCIS for such notifications.

Depending on the scope and magnitude of the major event, NERC will issue media advisories ~~through its crisis communications plan.~~in accordance with its NERC Crisis Action Plan and the NERC Communications Protocol Document.

Phase 2 ~~—~~ Situation Tracking and Communications

Based on the nature and severity of the major event, in Phase 2 NERC will continue to track progress in restoring the bulk power system and service to customers, and keep industry, government agencies, and the public informed. The most important thing to recognize in this phase is that the primary focus of ~~reliability coordinators and transmission operators~~Reliability Coordinators and Transmission Operators is the prompt restoration of the bulk ~~electric~~power system. NERC will coordinate requests by government agencies for information from ~~reliability coordinators and transmission operators~~Reliability Coordinators and Transmission Operators, and serve as a conduit and coordinator between industry and government for regular status reports on the restoration.

As ~~events continue~~the major event continues, NERC will determine whether a detailed analysis of the major event should be conducted, and start to identify manpower requirements, data collection and retention requirements, and at what level the analysis should be conducted. If the major event is localized within a region, NERC will participate in the ~~event~~ analysis of the ~~regional entity~~major event led by the Regional Entity.

Phase 3 ~~—~~ Data Collection, Investigation, Analysis, and Reporting

Based on the scope, magnitude, and impact of ~~an~~a major event, during Phase 3 NERC may:

1. perform an overview analysis of bulk power system and generator response;
2. rely on one of its ~~regional entities~~Regional Entities to ~~conduct~~lead the analysis and monitor the analysis results;
3. work with a ~~regional entity~~Regional Entity in its analysis; or
4. conduct a NERC-level analysis.

The NERC President and CEO will decide, based on the initial situation assessment and consultation with others, including the NERC technical committee officers[2], if the situation constitutes a major event and whether a NERC-level analysis is warranted. If a NERC-level analysis is to be conducted, the NERC President and CEO will appoint the ~~Director of Events Analysis and Information Exchange to lead the analysis and assemble a high-level technical steering group to provide guidance and support throughout the analysis~~analysis team leader.

NERC reserves the right to elevate or augment an analysis performed by a ~~regional entity~~Regional Entity pending the results of the ~~regional entity~~Regional Entity analysis. Additional requests for analyses or supporting data may be made by NERC at any time in the ~~investigation~~analysis process.

~~A regional entity may request NERC to elevate an analysis to a NERC-level. In such cases, all team responsibilities will shift to NERC, and the regional entity may continue to participate in the analysis on appropriate teams.~~

~~If the analysis is to be lead by one of the regional entities, a member of the NERC staff, at least one member of the NERC Event Analysis Working Group (in addition to an Event Analysis Working Group member from the impacted regional entity), and other appropriate technical experts from the NERC community will participate as a triage team. The triage team will participate as members of the regional entity analysis team. The triage team will also will assist the regional entity with determining if additional technical expertise from the NERC community are needed for the analysis.~~

~~For NERC-level analyses, the first task of the Director of Events Analysis and Information Exchange would be to identify what technical and other resources and data would be needed from staff, the industry, and government, and to issue those requests immediately. This task will include identification of any special managerial, forensic, or engineering skills needed for the analysis. Secondly, the Director of Events Analysis and Information Exchange must issue~~

[2] NERC will maintain a list of 24x7 contact information for its technical committee officers.

~~requests for those resources and information. Third, the Director of Events Analysis and Information Exchange must organize the teams that will conduct and report on the analysis.~~

~~The teams needed for a particular analysis will vary with the nature and scope of the event. Attachment A describes the typical teams that would be required for a NERC-level analysis, and Attachment B provides suggested guidelines for the NERC-level analysis team scopes. Individuals that participate on these teams will be expected to sign an appropriate confidentiality agreement. NERC uses a standard (pro forma) confidentiality agreement (Attachment C) for participants in event analyses, which it will adapt for specific analyses.~~

~~The Blackout and Disturbance Analysis Objectives, Approach, Schedule, and Status (Attachment D) and Guidelines for NERC Reports on Blackouts and Disturbances (Attachment E) are used to guide and manage analysis and reporting on major blackouts and disturbances.A~~ NERC-level analysis will comprise (a) collecting pertinent ~~event~~ data on the major event; (b) constructing a detailed sequence of events leading to and triggering the ~~disturbance~~major event; (c) assembling bulk power system models and data and conducting detailed bulk power system analysis to simulate ~~pre- and post-event~~ conditions before and after the major event; ~~and~~ (d) conducting a root cause analysis to determine causal factors, necessary corrective actions and any needed reliability mitigation; and (e) issuing findings, conclusions, and recommendations. The details of these ~~four~~five phases of the analysis are:

a. Collecting Pertinent Data on the Major Event ~~Data~~

- Collect all pertinent ~~event~~ logs, disturbance recorders, operator transcripts, and other bulk power system data pertaining to the major event.

b. Detailed Sequence of Events Leading to and Triggering the Major Event

- Construct a detailed sequence of events leading to and triggering the major event. Reconcile ~~event~~ logs, disturbance recorders, operator transcripts, and other bulk power system data to create an accurate sequence of events.
- Enter and preserve all data in a secure data warehouse.

c. Detailed Bulk Power System Analysis

- Assess the sequence of events to determine critical times for study.
- Assemble the necessary bulk power system models and data from ~~regional entity~~Regional Entity and ~~operating~~registered entities to accurately model (with power flow and dynamic simulations) the ~~pre-event~~ conditions prior to the major event.[3] Determine ~~pre-event~~ conditions at critical times prior to ~~event~~ initiation of the major event, including an assessment of reliability margins in the ~~pre-event~~ time ~~frame~~period preceding the major event.
- Analyze data from phasor measurement units, high-speed data recorders, digital fault recorders, digital relays, and system relay targets.[4]

---

[3] ~~NERC is developing standards for data and model validation that will facilitate modeling activities in future blackout analyses.~~

[4] ~~NERC is developing standards for dynamic monitoring equipment and the deployment of such equipment at critical locations in the bulk electric system.~~

- Analyze generator and load performance, including underfrequency and undervoltage relay actions.
- Use the model information and sequence of events to dynamically model the trigger ~~events~~occurrences and the outage sequence. Identify the bulk power system phenomena that propagated the failure. Provide graphical results showing the nature of the cascade. Conduct additional analyses as initial findings identify the need for further study.

d. Cause Analysis

Cause analysis methodology and the tools used guides the overall analysis process by providing a systematic approach to evaluating root causes, causal factors and contributing factors leading to the event. Cause analysis enables the analysis process to develop a factual record leading to logical and defensible conclusions in the final events analysis (EA) report regarding the causes of the event.

e. Findings, Conclusions, and Recommendations

- Identify and assess ~~failures~~causal factors contributing to the major event, including possible instability conditions, system protection mis-operations, generator actions, etc.
- Either identify or rule out man-made/criminal cyber or physical attacks on the ~~electric~~bulk power system.
- Determine if the bulk power system ~~was~~components were being operated within equipment and system design criteria at the time of the ~~outage~~major event.
- Assess the qualifications, training, SCADA/EMS tools, and communications available to bulk power system operators and ~~reliability coordinators~~Reliability Coordinators, and how effective these were leading up to and during the major event.
- Assess the adequacy of communications system and communications among bulk power system operators.
- Identify any issues regarding maintenance or equipment conditions that may have contributed to the outage.
- Determine whether bulk power system restoration procedures were available and adequate. Identify any issues that caused unexpected delays in the restoration of generators and loads.
- Identify the root causes[~~5~~3] and contributing factors of the ~~cascading outage~~major event.
- Recommend actions to prevent ~~cascading outages~~major events in the future and to improve bulk power system reliability.
- Determine whether the ~~system is adequately designed~~design of bulk power system components was a contributing factor to the event.
- All compliance issues will be referred to the NERC Director of ~~Compliance~~Enforcement.

[~~5~~] ~~NERC will rely on root cause analysis experts, both from within the industry and outside consultants, to conduct these analyses.~~

Phase 4 — Follow-up on Recommendations

For Phase 4 NERC and the ~~regional entities~~Regional Entities will follow up on specific recommendations coming from all analyses, whether done at the ~~regional entity~~Regional Entity or NERC level. In certain cases, where government agencies have taken a direct role in the analysis, reports will be made to those agencies on progress in addressing the recommendations.

Event Analysis of Other Events

For events (category 1 – 3) the registered entity should follow the methodology and steps outlined in the current version of the ERO event analysis process. The basic steps are outlined below.

1. The registered entity makes an initial assessment of an event, which includes determining the initial event category.
2. If the event is a "qualifying event" (*i.e.* Category 1-5), a planning meeting is held with all involved parties.
3. The registered entity submits a brief report.
4. If the qualifying event is a Category 3 or higher, the registered entity must also submit an event analysis report (EAR).
5. Lessons learned and best practices (if any) are developed and shared with industry.
6. The event is closed.

For lower tiered events, registered entities perform the event analysis. Coordination of the analysis becomes more complicated for events that involve a broader geographic area, involve multiple registered entities, or include a complex set of facts and circumstances.

A planning meeting should be held by the registered entity and the applicable Regional Entity as soon as possible following the occurrence of a qualifying event. During the meeting, agreement should be reached on the event category, the level of analysis, a timeline for completion of the report, and the need for a data retention hold and draft or preliminary reports. The event analysis should have a level of detail and target timeframe commensurate with the nature and scope of the event. Although the category of the event provides general guidance on the level of analysis needed, these guidelines may be adjusted based on the overall significance of the event and the potential for valuable lessons learned.

Registered entities that reside in two Regional Entity footprints should notify both Regional Entities of an event that spans both Regions. Following the notification, the two Regional Entities will determine which one will coordinate the remaining steps of the event analysis process. When multiple registered entities are involved in or affected by an event, they should collaborate with the Regional Entity to determine if it is appropriate for each entity to prepare a report or for the entities to work together to prepare a single report.

Weather-Related Occurrences - If a weather-related occurrence falls within any of the categories it should be reported. The affected registered entities should focus on restoration efforts. After restoration is complete, the affected entities, in coordination with Regional Entities, will determine if any additional information or event analysis steps are needed.

Development of Lessons Learned from Events

Lessons learned as a result of an event analysis should be shared with the industry as soon as practical. Proposed lessons learned should be drafted by a registered entity and should be submitted to the applicable Regional Entity. The lessons learned should be detailed enough to be of value to others and should not contain data or information that is deemed confidential. When possible, one-line diagrams, other diagrams and representations should be included to enhance the information provided in the lessons learned. Vendor-specific information should not be included unless it is discussed and coordinated with the vendor. If dissemination of vendor-specific information is beneficial, it may be pursued outside the event analysis process.

Lessons learned will be reviewed by selected technical groups and NERC staff for completeness and appropriateness prior to posting.

In normal operations, events may occur on the bulk power system that do not meet the reporting thresholds of the defined event categories but may yield lessons of value to the industry. These lessons learned can include the adoption of unique operating procedures, the identification of generic equipment problems, or the need for enhanced personnel training. In such cases, an event analysis report would not be required; however, registered entities are encouraged to share with their Regional Entities any potential lessons learned that could be useful to others in the industry, and to work with the Regional Entity and NERC to develop the lessons learned for dissemination.

Reporting and Analysis Requirements for Registered Entities in Connection with Events

Registered entities are required to report the occurrence of defined BPS disturbances and unusual occurrences to the applicable Regional Entity and NERC in accordance with various NERC and Regional reliability standards and other requirements. **It should be noted that following the event analysis process does not relieve the registered entity from mandatory reporting requirements dictated by regulatory authorities or NERC standards.**

In addition, a registered entity involved in an event will be required to submit one or more of the following reports, depending on the category of the event: a Brief Report; an Event Analysis Report; and proposed lessons learned. The following table shows the reports and timing requirements, by category of event:

Event Category	Brief Report	Event Analysis Report	Lessons Learned	Close Event Analysis
1	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Not required	Within 30 business days (if applicable)	10 business days following receipt of Brief Report
2	Draft within five business days, sent to applicable Regional	(If requested) Within 30 business days of	Within 30 business days	30 business days following receipt of

	Entity for review. Final report within 10 days.	the event		EAR
3	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 60 business days of the event	Within 60 business days	30 business days following receipt of EAR
4	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 180 business days of the event	Within 180 business days	60 business days following receipt of EAR
5	Draft within five business days, sent to applicable Regional Entity for review. Final report within 10 days.	Within 180 business days of the event	Within 180 business days	60 business days following receipt of EAR

The final Event Analysis Report should address corrective actions and recommendations related to the event's causal factors and any identified lessons learned. Positive outcomes identified during an event should be documented as a best practice. These are key parts of a continuous learning and improvement program.

Event Analysis Interface with Compliance

To support a strong culture of compliance, registered entities are expected to perform a compliance analysis and to develop a compliance self-assessment report proportional to the significance of the event/risk to the BPS for categorized events in which there could be a gap between actual system or human performance and the requirements of NERC or regional reliability standards. Registered entities are encouraged to submit a compliance self-assessment report to the Regional Entity compliance liaison proportional to the significance of the event/risk to the BPS for categorized events. This report should encompass a sufficiency review, proportional to the event's significance, of applicable standards associated with the event.

Registered entities who make a good faith effort to self-identify and self-disclose possible violations stemming from their event analyses will be afforded consideration in any enforcement action in accordance with the NERC *Sanction Guidelines*, **Appendix B** to the Rules of Procedure. If further analysis by the Regional Entity or NERC reveals other possible violations, the registered entity's participation and cooperation will be noted and considered.

For this reason, it is recommended that registered entities establish a liaison between their internal event analysis and compliance functions. This will provide a clearer understanding and a more efficient transfer of information from both an operational and a compliance standpoint, and it will facilitate a thorough standards review by the registered entity.

Any possible violations of reliability standards that were identified in the registered entity's compliance self-assessment should be self-reported by the registered entity through the existing Compliance Monitoring and Enforcement Program procedures, with a notification that they were discovered as a result of participating in the ERO event analysis program and completing a compliance self-assessment of the event.

As provided in **Appendix 4B**, *Sanction Guidelines*, of the NERC Rules of Procedure, if the registered entity is fully cooperative in the event analysis process, conducts a self-analysis of the event and submits a timely compliance self-assessment report, and submits self-reports of any possible violations of reliability standards and implements corrective and mitigating actions, then in any subsequent enforcement actions pursuant to the Compliance Monitoring and Enforcement Program, the registered entity's actions will be considered as mitigating factors in the determination of any penalties or sanctions for violations of reliability standards in connection with the event.

Attachment A

Typical Team Assignments for Analysis of Blackouts or Disturbances[6]

Fact-Finding Teams

- Physical and/or cyber security (if needed)
- On-site interviews
- System data collection (frequency, voltages, generation and loads)[7]
- System protection and control information
- System restoration
- Coordination with regional entity teams

Assessment and Analysis Teams

- Performance of generation and transmission protection systems
- Frequency analysis
- Equipment maintenance
- SCADA/EMS/Tools
- Operator training
- Standards compliance
- System planning
- System operation
- System restoration
- Root cause analysis
- System simulation
- Interregional coordination
- Vegetation management
- Recommendations for future actions
- Security and law enforcement liaison

Data Management Teams

- Data requests
- Data collection
- Data warehouse – entry, logging, retention, and maintenance[8]
- Data release[9]

Report Writing Teams

- Text
- Graphics
- Presentations

---

[6] The analysis team leader will specify the tasks required of each team.

[7] Standard forms and procedures for the collection of data and information will be adapted for particular circumstances.

[8] Experience with data warehousing and access procedures gained during the investigation of the August 2003 blackout will be used in future investigations.

[9] Data release procedures will prevent inappropriate disclosure of information.

~~**Communications Teams**~~

- ~~Press releases~~
- ~~Interface with government agencies~~
- ~~Interviews~~

Attachment B

NERC Blackout and Disturbance Response Procedures
Guidelines for Analysis Team Scopes

Each blackout or disturbance is unique and will therefore demand a customized approach to its analysis. The following guidelines for analysis team scopes are suggestive rather than definitive. Not all the teams listed may be needed for a particular analysis.

Data Requests and Management — This team organizes large volumes of raw data and value-added information produced by analysts in support of the blackout analysis into a data warehouse. The team issues data requests from affected entities, catalogs and stores all data received, and provides secure and confidential access to teams and personnel supporting the analysis. The team serves as the single point for issuing data requests, receiving and storing data, and managing data queries by the analysts, and is responsible for assuring consistency, security, and confidentiality of the data and minimizing redundant data requests.

Sequence of Events — A precise, accurate sequence of events is a building block for all other aspects of the analysis, and is a starting point for the root cause analysis. It is the basis for developing computer models to simulate system conditions and evaluate steady state and stability conditions in the period leading to blackout. The sequence of events is the foundation of facts upon which all other aspects of the analysis can proceed.

System Modeling and Simulation Analysis — System modeling and simulation allows the investigators to replicate system conditions leading up to the blackout. While the sequence of events provides a precise description of discrete events, it does not describe the overall state of the electric system and how close it was to various steady state, voltage stability, and power angle stability limits. An accurate computer model of the system, benchmarked to actual conditions at selected critical times, allows analysts to conduct a series of sensitivity studies to determine if the system was stable and within limits at each point in time leading up to the blackout, and at what point the system became unstable. It also allows analysts to test different solutions to prevent cascading. Although it is not possible recreate the entire blackout sequence, simulation methods will reveal the mode(s) of failure initiating the blackout and propagating through the system.

Root Cause Analysis — Root cause analysis guides the overall analysis process by providing a systematic approach to evaluating root causes and contributing factors leading to the blackout or disturbance. This team works closely with the technical analysis teams and draws on other data sources as needed to record verified facts regarding conditions and actions (or inactions) that contributed to the blackout or disturbance. The root cause analysis guides the overall analysis by indicating areas requiring further inquiry and other areas that may be of interest regarding lessons learned, but are not causal to the blackout. Root cause analysis enables the analysis process develop a factual record leading to logical and defensible conclusions in the final report regarding the causes of the blackout.

Operations Tools, SCADA/EMS, Communications, and Operations Planning — This team will assess the observability of the electric system to operators and reliability coordinators, and the availability and effectiveness of operational (real-time and day-ahead)

reliability assessment tools, including redundancy of views and the ability to observe the "big picture" regarding bulk electric system conditions. The team also investigates the operating practices and effectiveness of those practices of operating entities and reliability coordinators in the affected area. This team investigates all aspects of the blackout related to operator and reliability coordinator knowledge of system conditions, action or inactions, and communications.

Frequency/ACE — This team will analyze potential frequency anomalies that may have occurred, as compared to typical interconnection operations, to determine if there were any unusual issues with control performance and frequency and any effects they may have had related to the blackout.

System Planning, Design, and Studies — This team will analyze the responsibilities, procedures, and design criteria used in setting system operating limits, and compare them to good utility practice. The team will review the actual limits in effect on day of the blackout and whether these limits were being observed. The team will review voltage schedules and guides, and reactive management practices in the affected areas, including use of static and dynamic reactive reserves. The team will analyze the tagged and scheduled transactions to determine if inter-regional transfer limits were understood and observed. The team will analyze system planning and design studies completed in the affected areas to determine if operating conditions were consistent with the assumptions of those studies and whether the planning and design studies were sufficient and effective.

Transmission System Performance, Protection, Control, Maintenance, and Damage — This team investigates the causes of all transmission facility automatic operations (trips and reclosures) leading up to the blackout on all facilities greater than 100 kV. This review includes relay protection and remedial action schemes, identifying the cause of each operation, and any misoperations that may have occurred. The team also assesses transmission facility maintenance practices in the affected area as compared to good utility practice and identifies any transmission equipment that was damaged in any way as a result of the blackout. The team will assess transmission line rating practices and the impact that ambient temperature and wind speeds had on the transmission line performance in terms of the design temperature of the transmission conductors. The team shall report any patterns and conclusions regarding what caused transmission facilities to trip; why the blackout extended as far as it did and not further into other systems; why the transmission separated where it did; any misoperations and the effect those misoperations had on the blackout; and any transmission equipment damage. The team will also report on the transmission facility maintenance practices of entities in the affected area compared to good utility practice. Vegetation management practices are excluded here and covered in a different team.

Generator Performance, Protection, Controls, Maintenance and Damage — This team will investigate the cause of generator trips for all generators with a 10 MW or greater nameplate rating leading to and through the end of the blackout. The review shall include the cause for the generator trips, relay targets, unit power runbacks, and voltage/reactive power excursions. The team shall report any generator equipment that was damaged as a result of the blackout. The team shall report on patterns and conclusions regarding what caused generation facilities to trip. The team shall identify any unexpected performance anomalies or unexplained events. The team shall assess generator maintenance practices in the affected area as compared to good utility practice. The team will analyze the coordination of generator under-frequency

settings with transmission settings, such as under-frequency load shedding. The team will gather and analyze data on affected nuclear units and work with the Nuclear Regulatory Commission to address nuclear unit issues.

Vegetation/ROW — This team investigates the practices of transmission facility owners in the affected areas for vegetation management and ROW maintenance. These practices will be compared with accepted utility practices in general, and with NERC Reliability Standards. The team will evaluate whether the affected parties were within their defined procedures at the time of the blackout and will investigate historical patterns in the area related to outages caused by contact with vegetation.

Analysis Process and Procedures Review — This team will review the process and procedures used in the analysis of the blackout, make recommendations for improvement, and develop recommendations for appropriate processes, procedures, forms, etc. to guide and expedite future analyses including coordination and cooperation between NERC, its regional entities, and government agencies.

Restoration Review — All entities operating portions of the bulk electric system in North America are required by NERC Reliability Standards to maintain System Restoration Plans and Black Start Plans, and Reliability Coordinators are required to coordinate the implementation of those plans. This team will review the appropriateness and effectiveness of the restoration plans implemented and the effectiveness of the coordination of these plans.

NERC and RE Standards/Procedures and Compliance — This team reviews the adequacy of NERC Reliability Standards, regional entity standards and procedures, and the compliance monitoring program to address issues leading to the blackout. The team also reviews the compliance of the affected operating entities with Reliability Standards. For less significant event analyses, this tea may not be needed. However, all compliance issues will be referred to the NERC Director of Compliance.

Attachment C

NERC CONFIDENTIALITY AGREEMENT
FOR
ANALYSIS OF BLACKOUTS AND DISTURBANCES

This Confidentiality Agreement ("Agreement"), dated _____, is between the North American Electric Reliability Corporation ("NERC"), and

_____, a member of the NERC Event Analysis Team ("Team Member")(collectively referred to as "Parties").

WHEREAS, NERC is conducting an analysis of the power event that occurred in _____ on _____ and related matters ("Event"); and

WHEREAS, NERC has established a team to carry out that analysis ("Event Analysis Team"); and

WHEREAS, in order for the Event Analysis Team to fulfill its objectives, it is necessary for the Event Analysis Team have access to confidential or business sensitive information from operating entities within the _____ and to be able to conduct open and unconstrained discussions among team members,

The Parties therefore agree as follows:

1. The term "Event Analysis Information" means all information related in any way to the Event that operating entities within the _____ or their representatives have furnished or are furnishing to NERC in connection with NERC's analysis of the Event, whether furnished before or after the date of this Agreement, whether tangible or intangible, and in whatever form or medium provided (including, without limitation, oral communications), as well as all information generated by the Event Analysis Team or its representatives that contains, reflects or is derived from the furnished Event Analysis Information; provided, however, the term "Event Analysis Information" shall not include information that (i) is or becomes generally available to the public other than as a result of acts by the undersigned Parties or anyone to whom the undersigned Parties supply the Information, or (ii) is known to or acquired by the Team Member separate from receiving the information from the Event Analysis Team.

2. The Team Member understands and agrees that the Event Analysis Information is being made available solely for purposes of the Event Analysis and that the Event Analysis Information shall not be used in any manner to further the commercial interests of any person or entity. The Team Member further understands and agrees that he or she will not disclose Event Analysis Information to any person who has not signed this Agreement except as such disclosure may be required by law or judicial or regulatory order.

3. If Team Member's employing organization has signed the NERC Confidentiality Agreement for Electric System Security Data ("NERC Security Data Agreement"), paragraph 2 shall not be deemed to prohibit Team Member from disclosing Event Analysis Information to

other employees of that organization, but only to the extent that "security data" as defined in the NERC Security Data Agreement is shared within the organization.

4. The Parties expressly agree that Event Analysis Information shall otherwise only be disclosed through official releases and reports as authorized by NERC.

5. It shall not be a violation of the NERC Confidentiality Agreement for Electric System Security Data for a Reliability Coordinator to furnish Event Analysis Information to an Event Analysis Team Member who has signed this Agreement.

6. This Agreement shall be for sole benefit of the parties hereto. This Agreement may be modified or waived only by a separate writing signed by the Parties. If any clause or provision of this Agreement is illegal, or unenforceable, then it is the intention of the Parties hereto that the remainder of this Agreement shall not be affected thereby, and it is also the intention of the Parties that in lieu of each clause or provision that is illegal, invalid or unenforceable, there be added as part of this Agreement a clause or provision as similar in terms to such illegal, invalid or unenforceable clause or provision as may be possible and be legal, valid and enforceable. This Agreement will be governed and construed in accordance with the laws of the State of New Jersey, except for any choice of law requirement that otherwise may apply the law from another jurisdiction.

7. This Agreement shall have a term of two (2) years from the date hereof, except that the obligations of paragraphs 2, 3, and 4 shall continue for five (5) years from the date hereof.

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

By: _____

Printed: _____

Title: _____

NERC EVENT ANALYSIS TEAM MEMBER

Signed: _____

Printed: _____

Attachment ~~D~~A

NERC ~~Blackout and Disturbance~~Major Event Analysis Objectives, Analysis Approach, Schedule, and Status

Analysis Objective	Analysis Approach	Schedule	Status
Pre-Major Event Conditions			
1. What was the precursor sequence of events leading to the major event?	• Assemble data/alarm logs and time-stamped sequence information. • Develop and maintain an expanding database of log and time-stamped sequence information. • Develop a precursor sequence of high-level, events relevant to, and leading to ~~event~~ initiation of the major event. • Reconcile the precursor sequence of events with those emerging from ~~REs~~Regional Entities, RTOs, and operating entities.		
2. What time frames are relevant for ~~pre-event~~ assessment of bulk power system conditions prior to the major event? What points in time should be used to establish a baseline set of study conditions when the bulk power system was last known to be stable and within normal operating criteria?	• Referencing precursor sequence of events, determine relevant times to develop base case conditions (stable and within normal operating criteria). • Verify relevant time horizons and availability of bulk power system data at those times with ~~REs organizations, RTOS~~Regional Entities, RTOs, and operating entities.		
3. What models and data can best simulate bulk power system conditions prior to and during the major event? What is the relevant scope of the bulk power system for detailed study (what is considered the boundary of the ~~study~~bulk power system to be studied and what is considered neighboring or external bulk power systems?)	• Identify up-to-date bulk power system model(s) appropriate for powerflow and transient and dynamic simulations (determine if detailed eastern interconnection model is needed or multi-regional model(s) are needed. • Identify what models are available in ~~REs~~Regional Entities, RTOs, and operating entities. • Identify who will actually perform power flow, transient and dynamic simulations; hire contractor(s) as needed. • Identify and assemble data required for these models. • Develop and maintain a bulk power system data repository.		
4. What bulk power system conditions existed in the precursor time horizon leading up to the major event (at the times identified in ~~1.~~1)?	• Obtain and manage data for powerflow: bulk power system configuration, planned and unplanned outages, unit commitment and dispatch, interchange schedules, congestion conditions, reserves, loads, state estimator snapshots, deratings and limitations, frequency, etc. Identify who will maintain and run powerflow simulations. • Work with ~~REs~~Regional Entities, RTOs, and operating entities to develop powerflow cases defining the base conditions for each relevant		

Analysis Objective	Analysis Approach	Schedule	Status
	time, ensuring the powerflows model each critical juncture leading up to the major event. • Identify and review results of additional studies completed by reliability coordinators, RTOs and operating entities. • Assess the powerflow results with respect to steady state operating criteria (was the bulk power system within all known limits at each precursor time)?		
5. Were there any prior-existing abnormalities, instabilities, reliability criteria violations, or reliability issues in the precursor sequence time horizon? Prior to ~~event~~ initiation of the major event were there any latent instability conditions that would suggest the bulk power system was at risk? Were the precursor conditions ones that had been previously studied by the entities involved? Were there adequate reserves with effective distribution? Were planned outages effectively coordinated?	• Work with ~~REs~~Regional Entities, RTOs, and operating entities to obtain and manage transient and dynamic models for simulations. • Identify who will conduct transient and dynamic simulations and if external contractor(s) are required. • Conduct transient and dynamic simulations at each of the precursor study times. • Assess the stability of the bulk power system at each of these times and identify any latent reliability issues prior to ~~blackout~~ initiation of the major event. • Consider creating a visual map of bulk power system conditions. • Document the limitations and assumptions of simulations affecting the certainty of the simulation results.		
~~Blackout~~ Sequence of Events			
6. What was the sequence of ~~system~~ events leading to and directly triggering the ~~blackout~~major event?	• Evaluate data logs, fault recorder data disturbance recorder data, and synchro-phasor measurement to establish a detailed sequence of events that initiated the major event. • Identify the sequence of events that directly led to the major event. • Review and reconcile these trigger events with ~~REs~~Regional Entities, RTO, and operating entity analyses.		
7. What was the sequence of events during the major event?	• Evaluate logs and disturbance recorder data to establish sequence during the ~~blackout~~major event. (The ~~event~~ sequence of events may follow multiple tracks.) • Review and reconcile this sequence with those constructed by ~~REs~~Regional Entities, RTOs, and operating entities. • Consider developing 3-D, time-lapse visualization of the ~~blackout~~major event (U. of Minnesota and/or U. of Wisconsin).		
8. What was the cause of the major event in terms of electrical conditions and other related ~~events~~occurrences? Generally describe any bulk power system breakups, islanding, etc. Were there conditions of voltage or	• Assess triggering sequence and ~~blackout~~major event sequence to establish the causes for the ~~blackout~~major event in terms of electrical conditions and ~~events~~occurrences. • Select key points in sequence for simulation that are relevant for study and that can be accurately modeled. (It may not be possible		

	Analysis Objective	Analysis Approach	Schedule	Status
	frequency collapse, or unstable oscillations? Was the sequence strictly a sequential "domino" effect of facility trips? What were the bulk power system conditions (snapshots) at key points during the major event?	to reconcile data sufficiently to recreate bulk power system conditions during the ~~blackout~~major event.) • To the extent possible, conduct simulations and assess results at each point during the ~~blackout~~major event. • Review and reconcile results with ~~REs~~Regional Entities, and operating entities.		
9.	Why did the major event extend as far as it did? What arrested the major event from extending further into other ~~systems~~areas of the bulk power system?	• Using advanced analysis techniques, assess where and why the major event was arrested.		
10.	How did affected non-nuclear generators respond during the major event? Were trips as expected and required by procedures and standards? Did non-nuclear generators remain connected and support the bulk power system in the manner they should have? Did any generator action, generator control functions, or generator protection systems contribute to the major event?	• Prepare a table of affected generators and actions they made leading up to and during the major event, including time-stamped unit trips, relays initiating unit trips, MW and MVar outputs, voltages, and frequency, etc. • Analyze the automatic (including relay trips) and operator-initiated actions of non-nuclear generators to determine whether actions were correct under the conditions or not. • Reconcile non-nuclear generator data and analysis with that of the ~~REs~~Regional Entities, RTOs, and operating entities.		
11.	How did nuclear generators respond leading up to and during the ~~blackout~~major event? Were trips as expected and required by procedures and standards? Were there any nuclear safety issues identified?	• Work with NRC to develop a table of sequence of actions and issues regarding affected nuclear generators (both ones that tripped and those that did not). • Refer nuclear issues to NRC for analysis, assisting in their analyses where appropriate.		
12.	What was the sequence and amount of load lost? What directly caused load loss (e.g. under-frequency load shed, loss of transmission source, voltage collapse, relay actions, under/over frequency protection or stalls, etc.)	• Work ~~REs~~with Regional Entities, RTOs, and operating entities to develop a description of load lost/impacted, by area. • Analyze and report the cause for load loss in each area.		
13.	How did system protection and automated controls operate during the major event? Did they operate correctly or not?	• Assess each automatic trip of a transmission or generator facility for proper or improper relay actions. • Assemble and review ~~RE~~Regional Entity and operating entity reviews of logs, disturbance reports, and relay targets/logs and reconcile with NERC data.		
14.	Was any equipment damaged during the major event?	• Request information from ~~REs~~Regional Entities, and ~~companies~~operating entities on equipment damage, as appropriate. • Assess any transmission or generation facilities sustaining damage during the major		

Analysis Objective	Analysis Approach	Schedule	Status
	event, and extent of damage.		
15. Did SCADA/EMS and data communications systems operate correctly during the major event? What problems were noted?	• Request information from ~~REs,~~Regional Entities and ~~companies~~operating entities. • Identify and analyze any problems with SCADA/EMS and data communications at regional and ~~company~~operating entity levels.		
Reliability Standards/Procedures			
16. What NERC reliability standards were applicable to the major event? What violations occurred? Were NERC standards and policies sufficient?	• Compliance staff review NERC standards relevant to the major event and perform a compliance review.		
17. What ~~RE~~Regional Entity reliability standards were applicable to the major event? What violations occurred? Were ~~RE~~Regional Entity standards and policies sufficient?	• Request ~~REs~~Regional Entities to review applicable standards and report compliance with those standards during the major event.		
18. Were any special operating procedures or other operating guidelines in effect and being observed leading up to the major event? Were these procedures sufficient?	• Review and analyze loop flow procedures with ~~involved REs and companies~~Regional Entities and operating entities, and report analysis results.		
19. What other RTO, ~~TO, CA~~Transmission Owner, Balancing Authority procedures were applicable? What violations occurred? Were the procedures sufficient?	• Request RTOs, ~~TOs, CAs~~Transmission Owners, Balancing Authorities to review applicable standards and compliance with existing reliability procedures and standards during the major event, and report results.		
Maintenance			
20. Are there any indications that maintenance of transmission or generation facilities may have contributed to the major event?	• Assess whether equipment or maintenance issues (e.g. tree trimming) contributed to the ~~blackout~~major event and investigate specifics in areas of concern. • Review ~~RE~~Regional Entity assessments of maintenance issues that may have contributed to the major event.		
Personnel, Procedures, and Communications			
21. What conditions were operators and reliability coordinators aware of leading up to and during the major event? What information did they have to warn them of unsafe bulk power system conditions? What problems or concerns did they have? What did they observe during the major event? Were human errors made that contributed to the major	• Develop an interview guide to address procedural and operational issues. • Conduct onsite interviews with operating personnel and reliability coordinators involved. • Analyze interview data to corroborate with technical data and report conclusions.		

Analysis Objective	Analysis Approach	Schedule	Status
event? If there were, what were the causes of the errors?			
22. Were lines of authority clearly understood and respected in the time leading up to and during the major event, as well as during the restoration period?	• Identify critical instructions given and evaluate results. • Review documentation and effectiveness of assignments of operating and reliability authorities.		
23. What communications occurred among operating entities?	• Review voice communications logs. • Evaluate logs relevant to the major event and identify key interactions. Report conclusions.		
24. What were the qualifications (including certification status) and training of all operating personnel involved in the major event and their supervisors?	• Request certification status of all operating personnel from involved operating entities. • Conduct onsite review of training materials and records. • Conduct onsite review of operating procedures and tools		
25. Was the role and performance of the reliability coordinators as expected?	• Review the adequacy of reliability plans for the affected Regional Entities. • Review the actions of the affected reliability coordinators to determine if they performed according to plans. • Assess whether inter-area communications were effective, both at the control area and reliability coordinator levels.		
System Restoration			
26. Were black start and restoration procedures available and adequate in each area? Were they followed and were they adequate to the restoration task? Were pre-defined authorities respected during the restoration?	• Onsite audit of blackstart and restoration procedures and plans. • Analyze whether the plans and procedures were used and whether they were sufficient for this major event.		
27. What issues were encountered in the restoration that created unexpected challenges or delays? What lessons were learned in the restoration (both things that went well and things that did not).	• Solicit information from operating entities and Regional Entities regarding unexpected challenges and delays in restoration, and lessons learned. • Analyze what worked well and what did not in the restoration.		
System Planning and Design			
28. Were the conditions leading up to the major event within the design and planning criteria for the transmission systems involved?	• Request transmission owners and Regional Entities involved to report any violations of design or planning criteria prior to or leading up to the major event.		
Conclusions and Recommendations			
29. From a technical perspective, what are the root causes of this major event? What additional technical factors contributed to making the	• Conduct a root cause analysis on the findings and data. Categorize results as “root cause” or “contributing factor”. Focus on technical aspects.		

Analysis Objective	Analysis Approach	Schedule	Status
major event possible?			
30. What are the significant findings and lessons learned resulting from the analysis regarding technical failures leading to the major event? What actions are recommended to avoid similar future major events and improve bulk power system reliability? What issues may be inconclusive and require future analysis?	• Draft report of significant findings, lessons learned, and recommendations.		
31. Final Report	• Prepare and coordinate publication of final report.		

Personnel, Procedures, and Communications			
21. What conditions were operators and reliability coordinators aware of leading up to and during the event? What information did they have to warn them of unsafe system conditions? What problems or concerns did they have? What did they observe during the event? Were human errors made that contributed to the event? If there were, what were the causes of the errors?	• Develop an interview guide to address procedural and operational issues. • Conduct onsite interviews with operating personnel and reliability coordinators involved. • Analyze interview data to corroborate with technical data and report conclusions.		
22. Were lines of authority clearly understood and respected in the time leading up to and during the event, as well as during the restoration period?	• Identify critical instructions given and evaluate results. • Review documentation and effectiveness of assignments of operating and reliability authorities.		
23. What communications occurred among operating entities?	• Review voice communications logs. • Evaluate logs relevant to the blackout and identify key interactions. Report conclusions.		
24. What were the qualifications (including certification status) and training of all operating personnel involved in the event and their supervisors?	• Request certification status of all operating personnel from involved operating entities. • Conduct onsite review of training materials and records. • Conduct onsite review of operating procedures and tools		
25. Was the role and performance of the reliability coordinators as expected?	• Review the adequacy of reliability plans for the affected REs. • Review the actions of the affected reliability coordinators to determine if they performed according to plans. • Assess whether inter-area communications were effective, both at the control area and reliability coordinator levels.		
System Restoration			
26. Were black start and restoration procedures available and adequate in each area? Were they followed and were they adequate to the restoration task? Were pre-defined authorities respected during the restoration?	• Onsite audit of blackstart and restoration procedures and plans. • Analyze whether the plans and procedures were used and whether they were sufficient for this outage.		
27. What issues were encountered in the restoration that created unexpected challenges or delays? What lessons were learned in the restoration (both things that went well	• Solicit information from operating entities and REs regarding unexpected challenges and delays in restoration, and lessons learned. • Analyze what worked well and what did not in the restoration.		

~~and things that did not).~~			

System Planning and Design			
28. Were the conditions leading up to the event within the design and planning criteria for the transmission systems involved?	• Request transmission owners and REs involved to report any violations of design or planning criteria prior to or leading up to the blackout.		
Conclusions and Recommendations			
29. From a technical perspective, what are the root causes of this event? What additional technical factors contributed to making the event possible?	• Conduct a root cause analysis on the findings and data. Categorize results as "root cause" or "contributing factor". Focus on technical aspects.		
30. What are the significant findings and lessons learned resulting from the analysis regarding technical failures leading to the event? What actions are recommended to avoid similar future events and improve bulk electric system reliability? What issues may be inconclusive and require future analysis?	• Draft report of significant findings, lessons learned, and recommendations.		
31. Final Report	• Prepare and coordinate publication of final report.		

Attachment E

Guidelines for NERC Reports on Blackouts and Disturbances[10]

Introduction and Purpose

Executive Summary of Blackout or Disturbance

Conclusions & Recommendations

Actions to Minimize the Possibility of Future Blackouts and Disturbances

Detailed Analysis of Event

1. **Sequence of Events**
   - 1.1. Sequence of transmission and generation events
     - 1.1.1. Reasons for each trip
     - 1.1.2. Sequence of loss of load
     - 1.1.3. Description of cascading and islanding

[10] Each blackout or disturbance is unique and will therefore demand a customized approach to its investigation and reporting. These guidelines for NERC reports are suggestive rather than definitive. Not all investigations and reports will require covering all of these topics.

2. **System Modeling**
   2.1. Model and assumptions
      2.1.1. Equipment ratings and limits
      2.1.2. Steady state, system dynamics, and other analyses
      2.1.3. Degree of simulation success
      2.1.4. Simulation results
      2.1.5. Conclusions and lessons learned

   2.2. Pre-event Conditions
      2.2.1. Load levels
         2.2.1.1. Forecast vs. Actual
         2.2.1.2. Comparison with planning and operational models
      2.2.2. Generation dispatch
         2.2.2.1. Forecast vs. actual
         2.2.2.2. Comparison with day ahead studies
         2.2.2.3. Reporting of scheduled and forced outages
      2.2.3. Reserve capacity
         2.2.3.1. Location of MW reserves
         2.2.3.2. Planned vs. actual
      2.2.4. Transmission configurations
         2.2.4.1. Planned vs. actual
         2.2.4.2. Comparison with day ahead studies
         2.2.4.3. Reporting of scheduled and forced outages
      2.2.5. Interregional transactions
         2.2.5.1. Calculated transfer limits
         2.2.5.2. Basis for limits – thermal, voltage, and stability
         2.2.5.3. Seasonal assessments – Assumptions vs. actual
         2.2.5.4. Actual schedules vs. Tagged schedules
            2.2.5.4.1. AIE Survey
            2.2.5.4.2. Tag Survey
      2.2.6. System voltages (profile) and reactive supplies
         2.2.6.1. Coordination of reactive supplies and voltage schedules
         2.2.6.2. Reactive supply with power transfers

   2.3. Event Key Parameters
      2.3.1. System voltages (profile) and reactive supplies
      2.3.2. Power flows and equipment loadings
      2.3.3. System dynamic effects

3. **Transmission system performance**
   3.1. Equipment ratings
   3.2. Protective relay actions
   3.3. Equipment maintenance
   3.4. Equipment damage

4. **Generator performance**
   4.1. Generator control actions
   4.2. Generator protection

4.2.1. Underfrequency
4.2.2. Overspeed
4.2.3. Excitation systems
4.2.4. Other systems
4.3. Equipment maintenance
4.4. Equipment protection
4.5. Dynamic effects of generators

5. **System frequency**
5.1. Frequency excursions – pre event
5.1.1. Analysis of frequency anomalies
5.1.2. Effect of time error correction
5.2. Frequency analysis of the event
5.2.1. Remaining interconnection
5.2.2. Islands remaining

6. **Operations**
6.1. Operational visibility and actions
6.1.1. Reliability Coordinators
6.1.1.1. Delegation and authority
6.1.1.2. Monitoring capabilities
6.1.1.2.1. Scope of coverage and system visibility
6.1.1.2.2. Monitoring tools
6.1.1.2.3. Data availability and use
6.1.1.3. Operations planning capability
6.1.1.3.1. Operational planning tools
6.1.1.3.2. Coordination
6.1.1.4. Operating procedures
6.1.1.4.1. Emergency operations
6.1.1.4.2. Loss of monitoring system or components
6.1.1.4.3. Communication procedures
6.1.1.5. Operating qualifications and training
6.1.1.5.1. Qualification of operators
6.1.1.5.2. Training provided
6.1.1.5.3. Simulation of emergencies
6.1.2. Transmission Operators
6.1.2.1. Authority to take action
6.1.2.2. Monitoring capabilities
6.1.2.2.1. Scope of coverage and system visibility
6.1.2.2.2. Monitoring tools
6.1.2.2.3. Data availability and use
6.1.2.3. Operations planning capability
6.1.2.3.1. Operational planning tools
6.1.2.3.2. Coordination
6.1.2.4. Operating procedures
6.1.2.4.1. Emergency operations
6.1.2.4.2. Loss of monitoring system or components
6.1.2.4.3. Communication procedures

6.1.2.5. Operating qualifications and training
6.1.2.5.1. Qualification of operators
6.1.2.5.2. Training provided
6.1.2.5.3. Simulation of emergencies

7. **System Planning and Design**
7.1. Establishing operating limits
7.1.1. Responsibility for setting limits
7.1.2. ATC and TTC calculations
7.1.3. Planning studies
7.1.3.1. ·Wide-area simultaneous transfer limits
7.1.3.1.1. Determination of limits
7.1.3.1.2. Monitoring of limits
7.1.3.1.3. Basis for limits – thermal, voltage, and stability
7.1.3.1.4. RE assessments
7.1.3.1.5. Other system studies in affected areas
7.1.3.2. Reactive planning
7.1.3.2.1. Reactive reserve planning
7.1.3.2.2. Active vs. static resources
7.1.3.2.3. Voltage stability analysis
7.1.3.3. RE criteria and/or NERC standards used for planning
7.1.3.3.1. Compliance to these planning criteria and/or standards

8. **Reliability Standards and Compliance**
8.1. Audits
8.1.1. Reliability Coordinators
8.1.1.1. Previous audits and results
8.1.1.1.1. Compliance with NERC standards
8.1.1.2. Updated findings based on analysis
8.1.1.3. Post blackout audit results and findings
8.1.1.4. Recommendations for future audits
8.1.2. Balancing Authorities
8.1.2.1. RE audits
8.1.2.1.1. Compliance with NERC and RE standards
8.1.2.2. Updated findings based on analysis
8.1.2.3. Post blackout audit results and findings
8.1.2.4. Recommendations for future audits
8.2. RE criteria and/or NERC Reliability Standards used for operations
8.2.1. Compliance to these operating criteria and/or standards
8.3. Reliability Standards
8.3.1. Improvements needed
8.3.2. Potential new standards

9. **Actions to Minimize the Possibility of Future Widespread Events**
9.1. Reliability Standards and Compliance to Standards
9.2. Availability of Planned Facilities as Scheduled
9.3. Automatic Load Shedding Programs
9.4. Controlled Separation and Islanding

9.5. Improved Data Collection and System Monitoring
9.6. Studies of Impacts of Severe Events

10. **Restoration of Service**
10.1. Restoration Procedures
10.1.1. RTOs and ISOs
10.1.2. Transmission operators
10.1.3. Generator operators
10.1.4. Distribution providers

10.2. Restoring service
10.2.1. Transmission Line Restoration
10.2.1.1. Within control area/ISO/RTO
10.2.1.2. Interarea tie lines
10.2.1.3. Impediments and other issues
10.2.2. Generation Restoration
10.2.2.1. Utility-owned generation
10.2.2.2. Independent generation
10.2.2.3. Fuel supply adequacy
10.2.2.4. Fossil units
10.2.2.5. Nuclear units
10.2.2.6. Capacity reserves
10.2.2.7. Coordination with transmission
10.2.2.8. Coordination with load and other generation
10.2.2.9. Impediments and other issues
10.2.3. Coordination and Communications
10.2.3.1. Within control area/ISO/RTO
10.2.3.2. With outside control areas/ISOs/RTOs
10.2.3.3. Wide-area coverage
10.2.3.4. Impediments and other issues

10.3. Review of Restoration Procedures
10.3.1. Time to restore customers
10.3.2. Need for modifications
10.3.3. Availability of procedures to necessary participants
10.3.4. Need for training and practice drills
10.3.5. Comparison with other control areas/ISOs/RTOs

11. **Analysis Process**
11.1. Description of process
11.1.1. Organization
11.1.2. Coordination with US-Canada Task force
11.1.3. Coordination with RE and RTOs
11.1.4. Recommended process improvements
11.1.4.1. Use for other events – near misses, etc.
11.2. Data Management
11.2.1. Data collection processes
11.2.1.1. Data request process

~~11.2.1.2. Data forms used~~
~~11.2.2. Data received~~
~~11.2.2.1. Quality and usefulness of data~~
~~11.2.3. Data warehousing~~
~~11.2.3.1. Data warehouse structure~~
~~11.2.3.2. Accessibility of data~~
~~11.2.4. Data forms and process for future analyses~~

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Revised Version – 11-7-2011

Rules of Procedure

Effective: ~~October 7, 2011~~ _____, 2012

TABLE OF CONTENTS

SECTION 100 — APPLICABILITY OF RULES OF PROCEDURE 1

SECTION 200 — DEFINITIONS OF TERMS 2

201. General 2
202. Specific Definitions 2

SECTION 300 — RELIABILITY STANDARDS DEVELOPMENT 5

301. General 5
302. Essential Attributes for Technically Excellent Reliability Standards 5
303. Relationship between Reliability Standards and Competition 7
304. Essential Principles for the Development of Reliability Standards 8
305. Registered Ballot Body 8
306. Standards Committee 10
307. Standards Process Management 11
308. Steps in the Development of Reliability Standards 11
309. Filing of Reliability Standards for Approval by ERO Governmental Authorities 12
310. Reliability Standards Annual Work Plan 13
311. Regional Entity Standards Development Procedures 13
312. Regional Reliability Standards 15
313. Other Regional Criteria, Guides, Procedures, Agreements, Etc. 18
314. Conflicts with Statutes, Regulations, and Orders 18
315. Revisions to NERC Reliability Standards Processes Manual Development Procedure 19
316. Accreditation 19
317. Five-Year Review of Standards 19
318. Coordination with the North American Energy Standards Board 20
319. Archived Standards Information 20
320. Alternate Method Procedure for Developing and Approving Adopting Violation Risk Factors and Violation Severity Levels 20
321. Special Rule to Address Certain Regulatory Directives 21

SECTION 400 — COMPLIANCE ENFORCEMENT 25

401. Scope of the NERC Compliance Enforcement Program 25
402. NERC Oversight of the Regional Entity Compliance Enforcement Programs 28
403. Required Attributes of Regional Entity Compliance Enforcement Programs 31
404. NERC Monitoring of Compliance for Regional Entities or Bulk Power Owners, Operator, or Users 38
405. Monitoring of Standards and Other Requirements Applicable to NERC 38
406. Independent Audits of the NERC Compliance Monitoring and Enforcement Program 39
407. Penalties, Sanctions, and Remedial Actions 39
408. Review of NERC Decisions 40
409. Appeals from Final Decisions of Regional Entities 41
410. Hold Harmless 42
411. Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards 43
412. Certification of Questions from Regional Entity Hearing Bodies for Decision by the NERC Board of Trustees Compliance Committee 43
413. Review and Processing of Regional Entity Hearing Body Final Decisions that Are Not Appealed 4X
414. Appeals of Decisions of Regional Entity Hearing Bodies Granting or Denying

Motions to Intervene in Regional Entity Hearing Body Proceedings....4Y

SECTION 500 — ORGANIZATION REGISTRATION AND CERTIFICATION 47

501. Scope of the Organization Registration and Organization Certification Programs....47
502. Organization Registration and Organization Certification Program Requirements....51
503. Regional Entity Implementation of Organization Registration and Organization Certification Program Requirements....52
504. Appeals....54
505. Program Maintenance....54
506. Independent Audit of NERC Organization Registration and Organization Certification Program....54
507. Provisions Relating to Joint Registration Organizations (JRO)....55
508. Provisions Relating to Coordinated Functional Registration (CFR) Entities....56

SECTION 600 — PERSONNEL CERTIFICATION....58

601. Scope of Personnel Certification....58
602. Structure of ERO Personnel Certification Program....58
603 Examinations and Maintenance of NERC System Operator Certification Credentials....
604 Dispute Resolution Process....
605 Disciplinary Action....
6036. Candidate Testing Mechanisms....64
6047. Public Information About the Personnel Certification Program....64
6058. Responsibilities to Applicants for Certification or Recertification....64
6069. Responsibilities to the Public and to Employers of Certified Practitioners....65

SECTION 700 — RELIABILITY READINESS EVALUATION AND IMPROVEMENT AND FORMATION OF SECTOR FORUMS....67

701 Confidentiality Requirements for Readiness Evaluations and Evaluation Team Members....67
702. Formation of Sector Forum....67

SECTION 800 — RELIABILITY ASSESSMENT AND PERFORMANCE ANALYSIS....68

801. Objectives of the Reliability Assessment and Performance Analysis Program....68
802. Scope of the Reliability Assessment Program....68
803. Reliability Assessment Reports....69
804. Reliability Assessment Data and Information Requirements....70
805. Reliability Assessment Process....71
806. Scope of the Reliability Performance and Analysis Program....73
807. Analysis of Major Events....73
808. Analysis of Off-Normal OccurrencesEvents, Bulk Power Potential System PerformanceVulnerabilities, and Bulk Power System PerformanceVulnerabilities....74
809. Reliability Benchmarking....75
810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions....75
811. Equipment Performance Data....76

SECTION 900 — TRAINING AND EDUCATION....77

901. Scope of the Training and Education Program....77
902. Continuing Education Program....77

SECTION 1000 — SITUATION AWARENESS AND INFRASTRUCTURE SECURITY....79

1001. Situation Awareness 79
1002. Reliability Support Services 79
1003. Infrastructure Security Program 80

SECTION 1100 — ANNUAL NERC BUSINESS PLANS AND BUDGETS 83

1101. Scope of Business Plans and Budgets 83
1102. NERC Funding and Cost Allocation 83
1103. NERC Budget Development 83
1104. Submittal of Regional Entity Budgets to NERC 84
1105. Submittal of NERC and Regional Entity Budgets to Governmental Authorities for Approval 84
1106. NERC and Regional Entity Billing and Collections 85
1107. Penalty Applications 86
1108. Special Assessments 87

SECTION 1200 — REGIONAL DELEGATION AGREEMENTS 88

1201. Pro Forma Regional Delegation Agreement 88
1202. Regional Entity Essential Requirements 88
1203. Negotiation of Regional Delegation Agreements 88
1204. Conformance to Rules and Terms of Regional Delegation Agreements 88
1205. Sub-delegation 88
1206. Nonconformance to Rules or Terms of Regional Delegation Agreement 88
1207. Regional Entity Audits 89
1208. Process for Considering Registered Entity Requests to Transfer to Another Regional Entity Audits 89

SECTION 1300 — COMMITTEES 92

1301. Establishing Standing Committees 92
1302. Committee Membership 92
1303. Procedures for Appointing Committee Members 92
1304. Procedures for Conduct of Committee Business 92
1305. Committee Subgroups 93

SECTION 1400 — AMENDMENTS TO THE NERC RULES OF PROCEDURE 94

1401. Proposals for Amendment or Repeal of Rules of Procedure 94
1402. Approval of Amendment or Repeal of Rules of Procedure 94
~~1403. Alternative Procedure for Violation Risk Factors ..... 94~~

SECTION 1500 — CONFIDENTIAL INFORMATION 95

1501. Definitions 95
1502. Protection of Confidential Information 95
1503. Requests for Information 96
1504. Employees, Contractors and Agents 98
1505. Provision of Information to FERC and Other Governmental Authorities 98
1506. Permitted Disclosures 98
1507. Remedies for Improper Disclosure 98

SECTION 1600 — REQUESTS FOR DATA OR INFORMATION 100

1601. Scope of a NERC or Regional Entity Request for Data or Information 100
1602. Procedure for Authorizing a NERC Request for Data or Information 100
1603. Owners, Operators, and Users to Comply 101
1604. Requests by Regional Entity for Data or Information 101

1605. Confidentiality 102
1606 Expedited Procedure for Requesting Time-Sensitive Data or Information..... 102

SECTION 100 — APPLICABILITY OF RULES OF PROCEDURE

NERC and NERC members shall comply with these rules of procedure. Each regional entity shall comply with these rules of procedure as applicable to functions delegated to the regional entity by NERC or as required by an appropriate governmental authority or as otherwise provided.

Each bulk power system owner, operator, and user shall comply with all rules of procedure of NERC that are made applicable to such entities by approval pursuant to applicable legislation or regulation, or pursuant to agreement.

Any entity that is unable to comply or that is not in compliance with a NERC rule of procedure shall immediately notify NERC in writing, stating the rule of concern and the reason for not being able to comply with the rule.

NERC shall evaluate each case and inform the entity of the results of the evaluation. If NERC determines that a rule has been violated, or cannot practically be complied with, NERC shall notify the applicable governmental authorities and take such other actions as NERC deems appropriate to address the situation.

NERC shall comply with each approved reliability standard that identifies NERC or the electric reliability organization as a responsible entity. Regional Entities shall comply with each approved reliability standard that identifies Regional Entities as responsible entities. A violation by NERC or a Regional Entity of such a reliability standard shall constitute a violation of these Rules of Procedure.

SECTION 200 — DEFINITIONS OF TERMS

201. General

For purposes of NERC rules of procedure, the terms defined in Section 202 shall have the meaning set forth therein. Other terms are defined within particular sections of the rules of procedure. Other terms used but not defined in the rules of procedure shall be defined in NERC's Bylaws, the NERC Glossary of Terms Used in Reliability Standards adopted in conjunction with NERC's Reliability Standards, or in accordance with their commonly understood and used technical meanings in the electric power industry, including applicable codes and standards.

202. Specific Definitions

"Board" means the Board of Trustees of NERC.

"Bulk power system" means facilities and control systems necessary for operating an interconnected electric energy supply and transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.

"Canadian" means one of the following: (a) a company or association incorporated or organized under the laws of Canada, or its designated representative(s) irrespective of nationality; (b) an agency of a federal, provincial, or local government in Canada, or its designated representative irrespective(s) of nationality; or (c) a self-representing individual who is a Canadian citizen residing in Canada.

"Certification" means an official recognition that indicates the recipient has passed a NERC exam or completed a specified number of continuing education hours.

"Compliance enforcement authority" means NERC or the regional entity in their respective roles of monitoring and enforcing compliance with the NERC reliability standards

"Confirmed violation" is an alleged violation~~one~~ for which (1) the registered~~an~~ entity has~~: 1)~~ accepted the notice of alleged violation and proposed penalty or sanction or other notification~~the finding~~ of the alleged violation ~~by a regional entity or NERC and will not seek an appeal~~, or (2) there has been the issuance of a final order finding a violation, penalty or sanction, ~~completed the hearing and appeals process within NERC~~, or (3) the period for requesting a hearing or~~allowed the time for submitting an~~ appeal has ~~to~~ expired and the registered entity has not contested the notice of alleged violation or penalty in any filing with the compliance enforcement authority, or (4) the registered entity has entered into~~admitted to the violation in~~ a settlement agreement, regardless of whether or not the registered entity has admitted or contested the alleged violation.

"Continuing education hour" or "CE hour" means based on sixty clock minutes, and includes at least fifty minutes of participation in a group, or self-study learning activity that meets the criteria of the NERC Continuing Education Program.

"Electric reliability organization" or "ERO" means the organization that is certified by the Commission under Section 39.3 of its regulations, the purpose of which is to establish and enforce Reliability Standards for the bulk power system in the United States. The organization may also have received recognition by applicable governmental authorities in Canada and Mexico to establish and enforce reliability standards for the bulk power systems of the respective countries.

~~"Entity variance" means an aspect of a reliability standard that applies only within a particular entity or a subset of entities within a limited portion of a regional entity, such as a variance that would apply to a regional transmission organization or particular market or to a subset of bulk power system owners, operators or users. An entity variance may not be inconsistent with or less stringent than the reliability standards as it would otherwise exist without the entity variance. An entity variance shall be approved only through the NERC standards development procedure and shall be made part of the NERC reliability standards.~~

"ERO governmental authority" is a government agency that has subject matter jurisdiction over the reliability of the bulk power system within its jurisdictional territory. In the United States, the ERO governmental authority is the Federal Energy Regulatory Commission. In Canada, the ERO governmental authority resides with applicable federal and provincial governments who may delegate duties and responsibilities to other entities. Use of the term is intended to be inclusive of all applicable authorities in the United States, Canada, and Mexico, and is not restricted to those listed here.

"Net Energy for Load" or "NEL" means net generation of an electric system plus energy received from others less energy delivered to others through interchange. It includes system losses but excludes energy required for the storage of energy at energy storage facilities.

"Reliable operation" means operating the elements of the bulk power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.

"Regional criteria" means reliability requirements developed by a regional entity that are necessary to implement, to augment, or to comply with reliability standards, but which are not reliability standards. Such regional criteria may be necessary to account for physical differences in the bulk power system but are not inconsistent with reliability standards nor do they result in lesser reliability. Such regional criteria are not enforceable pursuant to NERC-delegated authorities, but may be enforced through other available mechanisms. Regional criteria may include specific acceptable operating or planning parameters, guides, agreements, protocols or other documents.

"Regional reliability standard" means a type of reliability standards that is applicable only within a particular regional entity or group of regional entities. A regional reliability standard may augment, add detail to, or implement another reliability standard or cover matters not addressed by other reliability standards. Regional reliability standards, upon adoption by NERC and approval by the applicable ERO governmental authority(ies), shall be reliability standards and shall be enforced within the applicable regional entity or regional entities pursuant to delegated authorities.

"Reliability standard" means a requirement to provide for reliable operation of the bulk power system, including without limiting the foregoing, requirements for the operation of existing bulk power system facilities, including cyber security protection, and including the design of planned additions or modifications to such facilities to the extent necessary for reliable operation of the bulk power system, but the term does not include any requirement to enlarge bulk power system facilities or to construct new transmission capacity or generation capacity. A reliability standard shall not be effective in the United States until approved by the Federal Energy Regulatory Commission and shall not be effective in other jurisdictions until made or allowed to become effective by the applicable governmental authority.

"Remedial action directive" means an action (other than a penalty or sanction) required by a compliance enforcement authority that (1) is to bring a registered entity into compliance with a reliability standard or to avoid a reliability standard violation, and (2) is immediately necessary to protect the reliability of the bulk power system from an imminent or actual threat.

"Required date" means the date given a registered entity in a notice from NERC or a regional entity by which some action by the registered entity is required.

"Variance" means an approved alternative method of achieving the reliability intent of one or more requirements in~~aspect or element of~~ a reliability standard ~~that applies only within a particular regional entity or group of regional entities, or to a particular entity or class of entities. A variance allows an alternative approach to meeting the same reliability objective as the reliability standard, and is typically necessitated by a physical difference. A variance is embodied within a reliability standard and as such, if adopted by NERC and approved by the ERO governmental authority, shall be enforced within the applicable regional entity or regional entities pursuant to delegated authority~~. No regional entity or bulk power system owner, operator, or user shall claim a variance from a NERC reliability standard without approval of such a variance through the relevant standard approval procedure for the variance. Each variance from a NERC reliability standard that is approved by NERC and applicable governmental authorities shall be made an enforceable part of the associated NERC reliability standard.

SECTION 300 — RELIABILITY STANDARDS DEVELOPMENT

301. General

NERC shall develop and maintain reliability standards that apply to bulk power system owners, operators, and users and that enable NERC and regional entities to measure the reliability performance of bulk power system owners, operators, and users; and to hold them accountable for reliable operation of the bulk power systems. The reliability standards shall be technically excellent, timely, just, reasonable, not unduly discriminatory or preferential, in the public interest, and consistent with other applicable standards of governmental authorities.

302. Essential Attributes for Technically Excellent Reliability Standards

1. **Applicability** — Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted. Such functional classes[1] include: reliability coordinators, balancing authorities, transmission operators, transmission owners, generator operators, generator owners, interchange authorities, transmission service providers, market operators, planning authorities, transmission planners, resource planners, load-serving entities, purchasing-selling entities, and distribution providers. Each reliability standard shall also identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area. A standard may also identify any limitations on the applicability of the standard based on electric facility characteristics.

2. **Reliability Objectives** — Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system. The following general objectives for the bulk power system provide a foundation for determining the specific objective(s) of each reliability standard:

    2.1 **Reliability Planning and Operating Performance**— Bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions.

    2.2 **Frequency and Voltage Performance**— The frequency and voltage of bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

[1] These functional classes of entities are derived from NERC's Reliability Functional Model. When a standard identifies a class of entities to which it applies, that class must be defined in the Glossary of Terms Used in Reliability Standards.

2.3 **Reliability Information** — Information necessary for the planning and operation of reliable bulk power systems shall be made available to those entities responsible for planning and operating bulk power systems.

2.4 **Emergency Preparation** — Plans for emergency operation and system restoration of bulk power systems shall be developed, coordinated, maintained, and implemented.

2.5 **Communications and Control** — Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of bulk power systems.

2.6 **Personnel** — Personnel responsible for planning and operating bulk power systems shall be trained and qualified, and shall have the responsibility and authority to implement actions.

2.7 **Wide-area View** — The reliability of the bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

2.8 **Security** —Bulk power systems shall be protected from malicious physical or cyber attacks.

3. **Performance Requirement or Outcome**— Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest. Each requirement is not a "lowest common denominator" compromise, but instead achieves an objective that is the best approach for bulk power system reliability, taking account of the costs and benefits of implementing the proposal.

4. **Measurability** — Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement. Each performance requirement shall have one or more associated measures used to objectively evaluate compliance with the requirement. If performance can be practically measured quantitatively, metrics shall be provided to determine satisfactory performance.

5. **Technical Basis in Engineering and Operations**— Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.

6. **Completeness** — Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.

7. **Consequences for Noncompliance** — In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.

8. **Clear Language** — Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.

9. **Practicality** — Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.

10. **Consistent Terminology** — To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.

303. Relationship between Reliability Standards and Competition

To ensure reliability standards are developed with due consideration of impacts on competition, to ensure standards are not unduly discriminatory or preferential, and recognizing that reliability is an essential requirement of a robust North American economy, each reliability standard shall meet all of these market-related objectives:

1. **Competition** — A reliability standard shall not give any market participant an unfair competitive advantage.

2. **Market Structures** — A reliability standard shall neither mandate nor prohibit any specific market structure.

3. **Market Solutions** — A reliability standard shall not preclude market solutions to achieving compliance with that standard.

4. **Commercially Sensitive Information** — A reliability standard shall not require the public disclosure of commercially sensitive information or other confidential information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.

5. **Adequacy** — NERC shall not set standards defining an adequate amount of, or requiring expansion of, bulk power system resources or delivery capability.

304. Essential Principles for the Development of Reliability Standards

NERC shall develop reliability standards in accordance with the NERC *Standard Processes Manual*, which is incorporated into these rules as **Appendix 3A**. Appeals in connection with the development of a reliability standard shall also be conducted in accordance with the NERC *Standard Processes Manual*. Any amendments or revisions to the *Standard Processes Manual* shall be consistent with the following essential principles:

1. **Openness** — Participation shall be open to all persons and entities who are directly and materially affected by the reliability of the North American bulk power system. There shall be no undue financial barriers to participation. Participation shall not be conditional upon membership in NERC or any other organization, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements.

2. **Transparency** — The process shall be transparent to the public.

3. **Consensus-building** —The process shall build and document consensus for each standard, both with regard to the need and justification for the standard and the content of the standard.

4. **Fair Balance of Interests** — The process shall fairly balance interests of all stakeholders and shall not be dominated by any two industry segments as defined in **Appendix** 3D, *Development of the Registered Ballot Body*, of these rules of procedure, and no single ~~interest category~~industry segment, individual or organization shall be able to defeat a matter.

5. **Due Process** — Development of standards shall provide reasonable notice and opportunity for any person with a direct and material interest to express views on a proposed standard and the basis for those views, and to have that position considered in the development of the standards.

6. **Timeliness** — Development of standards shall be timely and responsive to new and changing priorities for reliability of the bulk power system.

305. Registered Ballot Body

NERC reliability standards shall be approved by a registered ballot body prior to submittal to the board and then to ERO governmental authorities for their approval, where authorized by applicable legislation or agreement. This Section 305 sets forth the rules pertaining to the composition of, and eligibility to participate in, the registered ballot body.

1. **Eligibility to Vote on Standards** — Any person or entity may join the registered ballot body to vote on standards, whether or not such person or entity is a member of NERC.

2. **Inclusive Participation** — The segment qualification guidelines are inclusive; i.e., any entity with a legitimate interest in the reliability of the bulk power system that can meet any one of the eligibility criteria for a segment is entitled to belong to and vote in each segment for which it qualifies, subject to limitations defined in Sections 305.3 and 305.5.

3. **General Criteria for Registered Ballot Body Membership** — The general criteria for membership in the segments are:

   3.1 **Multiple Segments** — A corporation or other organization with integrated operations or with affiliates that qualifies to belong to more than one segment (e.g., transmission owners and load serving entities) may join once in each segment for which it qualifies, provided that each segment constitutes a separate membership and the organization is represented in each segment by a different representative. Affiliated entities are collectively limited to one membership in each segment for which they are qualified.

   3.2 **Withdrawing from a Segment or Changing Segments** — After its initial registration in a segment, each registered participant may elect to withdraw from a segment or apply to change segments at any time.

   3.3 **Review of Segment Criteria** — The board shall review the qualification guidelines and rules for joining segments at least every three years to ensure that the process continues to be fair, open, balanced, and inclusive. Public input will be solicited in the review of these guidelines.

4. **Proxies for Voting on Standards** — Any registered participant may designate an agent or proxy to vote on its behalf. There are no limits on how many proxies an agent may hold. However, for the proxy to be valid, NERC must have in its possession written documentation signed by the representative of the registered participant that the voting right by proxy has been transferred from the registered participant to the agent.

5. **Stakeholder Segments** — The specific criteria for membership in each registered ballot body segment are defined in the ~~*Standard Processes Manual*~~*Development of the Registered Ballot Body* in **Appendix ~~3A~~3D.**

6. **Review of Stakeholder Segment Entries** — NERC shall review all applications for joining the registered ballot body, and shall make a determination of whether the applicant's self-selection of a segment satisfies at least one of the guidelines to belong to that segment. The entity shall then become eligible to participate as a

voting member of that segment. The Standards Committee shall resolve disputes regarding eligibility for membership in a segment, with the applicant having the right of appeal to the board.

306. Standards Committee

The Standards Committee shall provide oversight of the reliability standards development process to ensure stakeholder interests are fairly represented. The Standards Committee shall not under any circumstance change the substance of a draft or approved standard.

1. **Membership** — The Standards Committee is a representative committee comprising representatives of two members of each of the segments in the registered ballot body and two officers elected to represent the interests of the industry as a whole.

2. **Elections** — Standards Committee members are elected for staggered (one per segment per year) two-year terms by the respective stakeholder segments in accordance with the *Procedure for the Election of Members of the NERC Standards Committee*, which is incorporated into these rules as **Appendix ~~2~~3B**. Segments may use their own election procedure if such a procedure is ratified by two-thirds of the members of a segment and approved by the board.

3. **Canadian Representation**

   The Standards Committee will include Canadian representation as provided in **Appendix 3B**, *Procedure for the Election of Members of the NERC Standards Committee*.

   ~~3.1 **Provision for Sufficient Canadian Representation** — If any regular election of Standards Committee members does not result in at least two Canadian members on the Standards Committee, the Canadian nominees who were not elected but who received the next highest percentage of votes within their respective segment(s) will be designated as additional members of the Standards Committee, as needed to achieve a total of two Canadian members.~~

   ~~3.2 **Terms of Specially Designated Canadian Members** — Each specially designated Canadian member of the Standards Committee shall have a term ending with the next annual election.~~

   ~~3.3 **Segment Preference** — If any segment has an unfilled representative position on the Standards Committee following the annual election, the first preference is to assign each specially designated Canadian representative to a segment with an unfilled representative position for which his or her organization qualifies.~~

~~3.4~~3.1 **~~Rights of Specially Designated Canadian Members~~** — ~~Any specially designated Canadian members of the Standards Committee shall have the same rights and obligations as all other members of the Standards Committee.~~

4. **Open Meetings** — All meetings of the Standards Committee shall be open and publicly noticed on the NERC Web site.

307. Standards Process Management~~Manager~~

NERC shall assign a standards process manager to administer the development of continent-wide reliability standards and a regional standards manager to administer the development of regional reliability standards. The standards process manager shall be responsible for ensuring that the development and revision of standards are in accordance with the NERC *Standard Processes Manual*. The standards process manager and the regional standards manager shall work to achieve the highest degree of integrity and consistency of quality and completeness of the reliability standards. The regional standards ~~process~~ manager shall coordinate with any regional entities that develop regional reliability standards to ensure those standards are effectively integrated with the NERC reliability standards.

308. Steps in the Development of Reliability Standards

1. **Procedure** — NERC shall develop reliability standards through the process set forth in the NERC *Standard Processes Manual* (**Appendix 3A**). The ~~procedure~~*Standard Processes Manual* includes ~~a~~ provisions for developing~~approval of urgent action~~ reliability standards that can be completed using expedited processes, including a process to develop reliability standards to address national security situations that involve confidential isues~~within 60 days and emergency actions that may be further expedited~~.

2. **Board Adoption~~Approval~~** — Reliability standards or revisions to reliability standards approved by the ballot pool in accordance with the *Standard Processes Manual* shall be submitted for ~~approval~~adoption by the board. No reliability standard or revision to a reliability standard shall be effective unless ~~approved~~adopted by the board.

3. **Governmental Approval** — After ~~receiving~~ board adoption~~approval~~, a reliability standard or revision to a reliability standard shall be submitted to all applicable ERO governmental authorities in accordance with Section 309. No reliability standard or revision to a reliability standard shall be effective within a geographic area over which an ERO governmental authority has jurisdiction unless it is approved by such ERO governmental authority or is otherwise made effective pursuant to the laws applicable to such ERO governmental authority.

309. Filing of Reliability Standards for Approval by ERO Governmental Authorities

1. **Filing of Reliability Standards for Approval** — Where authorized by applicable legislation or agreement, NERC shall file with the applicable ERO governmental authorities each reliability standard, modification to a reliability standard, or withdrawal of a standard that is ~~approved~~adopted by the board. Each filing shall be in the format required by the ERO governmental authority and shall include: a concise statement of the basis and purpose of the standard; the text of the standard; the implementation plan for the reliability standard; a demonstration that the standard meets the essential attributes of reliability standards as stated in Section 302; the drafting team roster; the ballot pool and final ballot results; and a discussion of public comments received during the development of the reliability standard and the consideration of those comments.

2. **Remanded Reliability Standards and Directives to Develop Standards** — If an ERO governmental authority remands a reliability standard to NERC or directs NERC to develop a reliability standard, NERC shall within five (5) business days notify all other applicable ERO governmental authorities, and shall within thirty (30) calendar days report to all ERO governmental authorities a plan and timetable for modification or development of the reliability standard. Standards that are remanded or directed by an ERO governmental authority shall be modified or developed using the *Standard Processes Manual*. NERC shall, during the development of a modification for the remanded standard or directed standard, consult with other ERO governmental authorities to coordinate any impacts of the proposed standards in those other jurisdictions. The expedited standards development process~~action procedure~~ may be applied if necessary to meet a timetable for action required by the ERO governmental authorities, respecting to the extent possible the provisions in the standards development process for reasonable notice and opportunity for public comment, due process, openness, and a balance of interest in developing reliability standards. If the Board of Trustees determines that the standards process did not result in a standard that addresses a specific matter that is identified in a directive issued by an applicable ERO governmental authority, then Rule 321 of these Rules of Procedure shall apply.

3. **Directives to Develop Standards under Extraordinary Circumstances** — An ERO governmental authority may, on its own initiative, determine that extraordinary circumstances exist requiring expedited development of a reliability standard. In such a case, the applicable agency may direct the development of a standard within a certain deadline. NERC staff shall prepare the standard~~s~~ authorization request ~~and seek a stakeholder sponsor for the request. If NERC is unable to find a sponsor for the proposed standard, NERC will be designated as the requestor~~. The proposed standard will then proceed through the standards development process, using the expedited action process~~procedures~~ described in the *Standard Processes Manual* as necessary to meet the specified deadline. The timeline will be developed to respect, to the extent possible, the provisions in the

standards development process for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing reliability standards. If the Board of Trustees determines that the standards process did not result in a standard that addresses a specific matter that is identified in a directive issued by an applicable ERO governmental authority, then Rule 321 of these Rules of Procedure shall apply, with appropriate modification of the timeline.

~~3.1Consistent with all reliability standards developed under the expedited action process, each of the three possible follow-up actions as documented in the *Standard Processes Manual* are to be completed through the standards development process and are subject to approval by the ERO governmental authorities in the U.S. and Canada.~~

310. Reliability Standards Annual Work Plan

NERC shall develop and provide an annual work plan for development of reliability standards to the applicable ERO governmental authorities. NERC shall consider the comments and priorities of the ERO governmental authorities in developing and updating the work plan. Each annual work plan shall include a progress report comparing results achieved to the prior year's plan.

311. Regional Entity Standards Development Procedures

1. **NERC Approval of Regional Entity Reliability Standards Development Procedure** — To enable a regional entity to develop regional reliability standards that are to be recognized and made part of NERC reliability standards, a regional entity may request NERC to approve a regional entity reliability standards development procedure.

2. **Public Notice and Comment on Regional Reliability Standards Development Procedure** — Upon receipt of such a request, NERC shall publicly notice and request comment on the proposed regional standards development procedure, allowing a minimum of 45 days for comment. The regional entity shall have an opportunity to resolve any objections identified in the comments and may choose to withdraw the request, revise the procedure and request another posting for comment, or submit the procedure, along with its consideration of any objections received, for approval by NERC.

3. **Evaluation of Regional Reliability Standards Development Procedure** — NERC shall evaluate whether a regional reliability standards development procedure meets the criteria listed below and shall consider stakeholder comments, any unresolved stakeholder objections, and the consideration of comments provided by the regional entity, in making that determination. If NERC determines the regional reliability standards development procedure meets these requirements, the procedure shall be submitted to the board for approval. The

board shall consider the recommended action, stakeholder comments, any unresolved stakeholder comments, and the regional entity consideration of comments in determining whether to approve the regional reliability standards development procedure.

3.1 **Evaluation Criteria** — The regional reliability standards development procedure shall be:

3.1.1 **Open** — The regional reliability standards development procedure shall provide that any person or entity who is directly and materially affected by the reliability of the bulk power systems within the regional entity shall be able to participate in the development and approval of reliability standards. There shall be no undue financial barriers to participation. Participation shall not be conditional upon membership in the regional entity, a regional entity or any organization, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements.

3.1.2 **Inclusive** — The regional reliability standards development procedure shall provide that any person with a direct and material interest has a right to participate by expressing an opinion and its basis, having that position considered, and appealing through an established appeals process if adversely affected.

3.1.3 **Balanced** — The regional reliability standards development procedure shall have a balance of interests and shall not permit any two interest categories to ~~control the vote on~~dominate a matter or any single interest category to defeat a matter.

3.1.4 **Due Process** — The regional reliability standards development procedure shall provide for reasonable notice and opportunity for public comment. At a minimum, the procedure shall include public notice of the intent to develop a standard, a public comment period on the proposed standard, due consideration of those public comments, and a ballot of interested stakeholders.

3.1.5 **Transparent** — All actions material to the development of regional reliability standards shall be transparent. All standards development meetings shall be open and publicly noticed on the regional entity's Web site.

3.1.6 **Accreditation of Regional Standards Development Procedure** — A regional entity's reliability standards development procedure that is accredited by the American National Standards Institute ~~or the Standards Council of Canada~~ shall be deemed to meet the

criteria listed in this Section 311.3.1, although such accreditation is not a prerequisite for approval by NERC.

3.1.7 **Use of NERC Procedure** — A regional entity may adopt the NERC *Standard Processes Manual* as the regional reliability standards development procedure, in which case the regional entity's procedure shall be deemed to meet the criteria listed in this Section 311.3.1.

4. **Revisions of Regional Reliability Standards Development Procedures** — Any revision to a regional reliability standards development procedure shall be subject to the same approval requirements set forth in Sections 311.1 through 311.3.

5. **Duration of Regional Reliability Standards Development Procedures** — The regional reliability standards development procedure shall remain in effect until such time as it is replaced with a new version approved by NERC or it is withdrawn by the regional entity. The regional entity may, at its discretion, withdraw its regional reliability standards development procedure at any time.

312. Regional Reliability Standards

1. **Basis for Regional Reliability Standards** — Regional entities may propose regional reliability standards that set more stringent reliability requirements than the NERC reliability standard or cover matters not covered by an existing NERC reliability standard. Such regional reliability standards shall in all cases be submitted to~~approved by~~ NERC for adoption and, if adopted, made part of the NERC reliability standards and shall be enforceable in accordance with the delegation agreement between NERC and the regional entity or other instrument granting authority over enforcement to the regional entity. No entities other than NERC and the regional entity shall be permitted to develop regional reliability standards that are enforceable under statutory authority delegated to NERC and the regional entity.

2. **Regional Reliability Standards That are Directed by a NERC Reliability Standard** — Although it is the intent of NERC to promote uniform reliability standards across North America, in some cases it may not be feasible to achieve a reliability objective with a reliability standard that is uniformly applicable across North America. In such cases, NERC may direct regional entities to develop regional reliability standards necessary to implement a NERC reliability standard. Such regional reliability standards that are developed pursuant to a direction by NERC shall be made part of the NERC reliability standards.

3. **Procedure for Developing an Interconnection-wide Regional Standard** — A regional entity organized on an interconnection-wide basis may propose a regional reliability standard for approval as a NERC reliability standard to be

made mandatory for all applicable bulk power system owners, operators, and users within that interconnection.

3.1 **Presumption of Validity** — An interconnection-wide regional reliability standard that is determined by NERC to be just, reasonable, and not unduly discriminatory or preferential, and in the public interest, and consistent with such other applicable standards of governmental authorities, shall be adopted as a NERC reliability standard. NERC shall rebuttably presume that a regional reliability standard developed, in accordance with a regional reliability standards development process approved by NERC, by a regional entity organized on an interconnection-wide basis, is just, reasonable, and not unduly discriminatory or preferential, and in the public interest, and consistent with such other applicable standards of governmental authorities.

3.2 **Notice and Comment Procedure for Interconnection-wide Regional Reliability Standard** — NERC shall publicly notice and request comment on the proposed interconnection-wide regional reliability standard, allowing a minimum of 45 days for comment. NERC may publicly notice and post for comment the proposed regional reliability standard concurrent with similar steps in the regional entity's reliability standards development process. The regional entity shall have an opportunity to resolve any objections identified in the comments and may choose to comment on or withdraw the request, revise the proposed regional reliability standard and request another posting for comment, or submit the proposed regional reliability standard along with its consideration of any objections received, for approval by NERC.

3.3 **Approval of Interconnection-wide Regional Reliability Standard by NERC** — NERC shall evaluate and recommend whether a proposed interconnection-wide regional reliability standard has been developed in accordance with all applicable procedural requirements and whether the regional entity has considered and resolved stakeholder objections that could serve as a basis for rebutting the presumption of validity of the regional reliability standard. The regional entity, having been notified of the results of the evaluation and recommendation concerning NERC proposed regional reliability standard, shall have the option of presenting the proposed regional reliability standard to the board for approval as a NERC reliability standard. The board shall consider the regional entity's request, NERC's recommendation for action on the regional reliability standard, any unresolved stakeholder comments, and the regional entity's consideration of comments, in determining whether to approve the regional reliability standard as a NERC reliability standard.

3.4 **ERO Governmental Authority Approval** — An interconnection-wide regional reliability standard that has been approved by the board shall be

filed with the applicable ERO governmental authorities for approval, where authorized by applicable legislation or agreement, and shall become effective when approved by such ERO governmental authorities or on a date set by the ERO governmental authorities.

3.5 **Enforcement of Interconnection-wide Regional Reliability Standard** — An interconnection-wide regional reliability standard that has been approved by the board and by the applicable ERO governmental authorities or is otherwise made effective within Canada as mandatory within a particular region shall be applicable and enforced as a NERC reliability standard within the region.

4. **Procedure for Developing Non-Interconnection-Wide Regional Reliability Standards** — Regional entities that are not organized on an interconnection-wide basis may propose regional reliability standards to apply within their respective regions. Such standards may be developed through the NERC reliability standards development procedure, or alternatively, through a regional reliability standards development procedure that has been approved by NERC.

4.1 **No Presumption of Validity** — Regional reliability standards that are not proposed to be applied on an interconnection-wide basis are not presumed to be valid but may be demonstrated by the proponent to be valid.

4.2 **Notice and Comment Procedure for Non-Interconnection-wide Regional Reliability Standards** — NERC shall publicly notice and request comment on the proposed regional reliability standard, allowing a minimum of 45 days for comment. NERC may publicly notice and post for comment the proposed regional reliability standard concurrent with similar steps in the regional entity's reliability standards development process. The regional entity shall have an opportunity to comment on or resolve any objections identified in the comments and may choose to withdraw the request, revise the proposed regional reliability standard and request another posting for comment, or submit the proposed regional reliability standard along with its consideration of any objections received, for approval by NERC.

4.3 **NERC Approval of Non-Interconnection-wide Regional Reliability Standards** — NERC shall evaluate and recommend whether a proposed non-Interconnection-wide regional reliability standard has been developed in accordance with all applicable procedural requirements and whether the regional entity has considered and resolved stakeholder objections. The regional entity, having been notified of the results of the evaluation and recommendation concerning proposed regional reliability standard, shall have the option of presenting the proposed regional reliability standard to the board for approval as a NERC reliability standard. The board shall consider the regional entity's request, the recommendation for action on

the regional reliability standard, any unresolved stakeholder comments, and the regional entity's consideration of comments, in determining whether to approve the regional reliability standard as a NERC reliability standard.

4.4 **NERC Governmental Authority Approval** — A non-Interconnection-wide regional reliability standard that has been approved by the board shall be filed with the applicable ERO governmental authorities for approval, where authorized by applicable legislation or agreement, and shall become effective when approved by such ERO governmental authorities or on a date set by the ERO governmental authorities.

4.5 **Enforcement of Non-Interconnection-wide Regional Reliability Standards** — A non-Interconnection-wide regional reliability standard that has been approved by the board and by the applicable ERO governmental authorities or is otherwise made effective within Canada as mandatory within a particular region shall be applicable and enforced as a NERC reliability standard within the region.

5. **Appeals** — A Regional Entity shall have the right to appeal NERC's decision not to approve a proposed regional reliability standard or variance to the Commission or other applicable governmental authority.

313. Other Regional Criteria, Guides, Procedures, Agreements, Etc.

1. **Regional Criteria** — Regional entities may develop regional criteria that are necessary to implement, to augment, or to comply with NERC reliability standards, but which are not reliability standards. Regional criteria may also address issues not within the scope of reliability standards, such as resource adequacy. Regional criteria may include specific acceptable operating or planning parameters, guides, agreements, protocols or other documents used to enhance the reliability of the regional bulk power system. These documents typically provide benefits by promoting more consistent implementation of the NERC reliability standards within the region. These documents are not NERC reliability standards, regional reliability standards, or regional variances, and therefore are not enforceable under authority delegated by NERC pursuant to delegation agreements and do not require NERC approval.

2. **Catalog of Regional Reliability Criteria** — NERC shall maintain a current catalog of regional reliability criteria. Regional entities shall provide a catalog listing of regional reliability criteria to NERC and shall notify NERC of changes to the listing. Regional entities shall provide any listed document to NERC upon written request.

314. Conflicts with Statutes, Regulations, and Orders

Notice of Potential Conflict — If a bulk power system owner, operator, or user determines that a NERC or regional reliability standard may conflict with a function, rule, order, tariff, rate schedule, legislative requirement or agreement that has been accepted, approved, or ordered by a governmental authority affecting that entity, the entity shall expeditiously notify the governmental authority, NERC, and the relevant regional entity of the conflict.

1. **Determination of Conflict —** NERC, upon request of the governmental authority, may advise the governmental authority regarding the conflict and propose a resolution of the conflict, including revision of the reliability standard if appropriate.

2. **Regulatory Precedence** — Unless otherwise ordered by a governmental authority, the affected bulk power system owner, operator, or user shall continue to follow the function, rule, order, tariff, rate schedule, legislative requirement, or agreement accepted, approved, or ordered by the governmental authority until the governmental authority finds that a conflict exists and orders a remedy and such remedy is affected.

315. Revisions to NERC ~~Reliability~~ Standard~~s~~ Processes Manual~~Development Procedure~~

Any person or entity may submit a written request to modify NERC *Standard Processes Manual*. Consideration of the request and development of the revision shall follow the process defined in the NERC *Standard Processes Manual*. Upon approval by the board, the revision shall be submitted to the ERO governmental authorities for approval. Changes shall become effective only upon approval by the ERO governmental authorities or on a date designated by the ERO governmental authorities or as otherwise applicable in a particular jurisdiction.

316. Accreditation

NERC shall seek and maintain~~continuing~~ accreditation of the NERC reliability standards development process by the American National Standards Institute ~~and the Standards Council of Canada~~.

317. Five-Year Review of Standards

NERC shall complete a review of each NERC reliability standard at least once every five years, or such longer period as is permitted by the American National Standards Institute, from the effective date of the standard or the latest revision to the standard, whichever is later. The review process shall be conducted in accordance with the NERC *Standard Processes Manual*. The standards process manager shall be responsible for administration of the five-year review of reliability standards. As a result of this review, the NERC

reliability standard shall be reaffirmed, revised, or withdrawn. If the review indicates a need to revise or withdraw the standard, a request for revision or withdrawal shall be prepared, submitted and addressed in accordance with the NERC *Standard Processes Manual*.

318. Coordination with the North American Energy Standards Board

NERC shall, through a memorandum of understanding, maintain a close working relationship with the North American Energy Standards Board ~~and ISO/RTO Council~~ to ensure effective coordination of wholesale electric business practice standards and market protocols with the NERC reliability standards.

319. Archived Standards Information

NERC shall maintain a historical record of reliability standards information that is no longer maintained on-line. For example, standards that have been retired~~expired or were replaced~~ may be removed from the on-line system. Archived information shall be retained indefinitely as practical, but in no case less than five years or one complete standards review cycle from the date on which the standard was no longer in effect. Archived records of reliability standards information shall be available electronically within 30 days following the receipt by the NERC standards information~~process~~ manager of a written request.

320. ~~Alternate Method~~Procedure for Developing and Approving~~Adopting~~ Violation Risk Factors and Violation Severity Levels

1. **Development of Violation Risk Factors and Violation Severity Levels** — NERC shall follow the process for developing violation risk factors (VRFs) and violation severity levels (VSLs) as set forth in the *Standard Processes Manual*, **Appendix 3A** to these rules of procedure.

2. **Remands or Directed Revision of VRFs and VSLs by ERO Governmental Authorities** — If an ERO governmental authority remands or directs a revision to a board-approved VRF or VSL assignment, the NERC director of standards, after consulting with the standard drafting team, Standards Committee, and the NERC director of compliance operations, will recommend to the board one of the following actions: (1) filing a request for clarification; (2) filing for rehearing or for review of the ERO governmental authority decision; or (3) approval of the directed revisions to the VRF or VSL. If and to the extent time is available prior to the deadline for the board's decision, an opportunity for interested parties to comment on the action to be taken will be provided.

3. **Alternative Procedure for Developing and Approving Violation Risk Factors and Violation Severity Levels** — In the event the standards development process fails to produce violation risk factors or violation severity levels for a particular

standard in a timely manner, the Board of Trustees may approve~~adopt~~ violation risk factors or violation severity levels for that standard after notice and opportunity for comment. In approving VRFs or VSLs, the board shall consider the inputs of the Member Representatives Committee and affected stakeholders ~~using the procedures set out in Section 1400 of these Rules of Procedure~~.

321. Special Rule to Address Certain Regulatory Directives

In circumstances where this Rule 321 applies, the Board of Trustees shall have the authority to take one or more of the actions set out below. The Board of Trustees shall have the authority to choose which one or more of the actions are appropriate to the circumstances and need not take these actions in sequential steps.

1. The Standards Committee shall have the responsibility to ensure that standards drafting teams address specific matters that are identified in directives issued by applicable ERO governmental authorities. If the Board of Trustees is presented with a proposed standard that fails to address such directives, the Board of Trustees has the authority to remand, with instructions (including establishing a timetable for action), the proposed reliability standard to the Standards Committee.

2. Upon a written finding by the Board of Trustees that a ballot pool has failed to approve a proposed reliability standard that contains a provision to address a specific matter identified in a directive issued by an ERO governmental authority, the Board of Trustees has the authority to remand the proposed reliability standard to the Standards Committee, with instructions to (i) convene a public technical conference to discuss the issues surrounding the regulatory directive, including whether or not the proposed standard is just, reasonable, not unduly discriminatory or preferential, in the public interest, helpful to reliability, practical, technically sound, technically feasible, and cost-justified; (ii) working with NERC staff, prepare a memorandum discussing the issues, an analysis of the alternatives considered and other appropriate matters; and (iii) re-ballot the proposed reliability standard one additional time, with such adjustments in the schedule as are necessary to meet the deadline contained in paragraph 2.1 of this Rule.

   2.1 Such a re-ballot shall be completed within forty-five (45) days of the remand. The Standards Committee memorandum shall be included in the materials made available to the ballot pool in connection with the re-ballot.

   2.2 In any such re-ballot, negative votes without comments related to the proposal shall be counted for purposes of establishing a quorum, but only affirmative votes and negative votes with comments related to the proposal shall be counted for purposes of determining the number of votes cast and whether the proposed standard has been approved.

3. If the re-balloted proposed reliability standard achieves at least an affirmative two-thirds majority vote of the weighted segment votes cast, with a quorum established, then the proposed reliability standard shall be deemed approved by the ballot pool and shall be considered by the Board of Trustees for approval.

4. If the re-balloted proposed reliability standard fails to achieve at least an affirmative two-thirds majority vote of the weighted segment votes cast, but does achieve at least a sixty percent affirmative majority of the weighted segment votes cast, with a quorum established, then the Board of Trustees has the authority to consider the proposed reliability standard for approval under the following procedures:

   4.1 The Board of Trustees shall issue notice of its intent to consider the proposed reliability standard and shall solicit written public comment particularly focused on the technical aspects of the provisions of the proposed reliability standard that address the specific matter identified in the regulatory directive, including whether or not the proposed standard is just, reasonable, not unduly discriminatory or preferential, in the public interest, helpful to reliability, practical, technically sound, technically feasible, and cost-justified.

   4.2 The Board of Trustees may, in its discretion, convene a public technical conference to receive additional input on the matter.

   4.3 After considering the developmental record, the comments received during balloting and the additional input received under paragraphs 4.1 and 4.2 of this Rule, the Board of Trustees has authority to act on the proposed reliability standard.

      4.3.1 If the Board of Trustees finds that the proposed reliability standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest, considering (among other things) whether it is helpful to reliability, practical, technically sound, technically feasible, and cost-justified, then it has authority to approve the proposed reliability standard and direct that it be filed with applicable ERO governmental authorities with a request that it be made effective.

      4.3.2 If the Board of Trustees is unable to find that the proposed reliability standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest, considering (among other things) whether it is helpful to reliability, practical, technically sound, technically feasible, and cost-justified, then it has authority to treat the proposed reliability standard as a draft reliability standard and direct that the draft reliability standard and complete developmental record, including the additional input received under paragraphs 4.1 and 4.2 of this Rule, be filed with the applicable ERO governmental authorities as a compliance filing in

response to the order giving rise to the regulatory directive, along with a recommendation that the standard not be made effective and an explanation of the basis for the recommendation.

5. Upon a written finding by the Board of Trustees that standard drafting team has failed to develop, or a ballot pool has failed to approve, a proposed reliability standard that contains a provision to address a specific matter identified in a directive issued by an ERO governmental authority, the Board of Trustees has the authority to direct the Standards Committee (with the assistance of stakeholders and NERC staff) to prepare a draft reliability standard that addresses the regulatory directive, taking account of the entire developmental record pertaining to the matter. If the Standards Committee fails to prepare such draft reliability standard, the Board of Trustees may direct NERC management to prepare such draft reliability standard.

   5.1 The Board of Trustees may, in its discretion, convene a public technical conference to receive input on the matter. The draft reliability standard shall be posted for a 45-day public comment period.

   5.2 If, after considering the entire developmental record (including the comments received under paragraph 5.1 of this Rule), the Board of Trustees finds that the draft reliability standard, with such modifications as the Board of Trustees determines are appropriate in light of the comments received, is just, reasonable, not unduly discriminatory or preferential, and in the public interest, considering (among other things) whether it is practical, technically sound, technically feasible, cost-justified and serves the best interests of reliability of the bulk power system, then the Board of Trustees has the authority to approve the draft standard and direct that the proposed standard be filed with ERO governmental authorities with a request that the proposed standard be made effective.

   5.3 If, after considering the entire developmental record (including the comments received under paragraph 5.1 of this Rule), the Board of Trustees is unable to find that the draft reliability standard, even with modifications, is just, reasonable, not unduly discriminatory or preferential, and in the public interest, considering (among other things) whether it is practical, technically sound, technically feasible, cost-justified and serves the best interests of reliability of the bulk power system, then the Board of Trustees has the authority to direct that the draft standard and complete developmental record be filed as a compliance filing in response to the regulatory directive with the ERO governmental authority issuing the regulatory directive, with a recommendation that the draft standard not be made effective.

5.4 The filing of the reliability standard under either paragraph 5.2 or paragraph 5.3 of this Rule shall include an explanation of the basis for the decision by the Board of Trustees.

5.5 A reliability standard approved under paragraph 5 of this Rule shall not be eligible for submission as an American National Standard.

6. NERC shall on or before March 31st of each year file a report with applicable ERO governmental authorities on the status and timetable for addressing each outstanding directive to address a specific matter received from an applicable ERO governmental authority.

SECTION 400 — COMPLIANCE ENFORCEMENT

401. Scope of the NERC Compliance Enforcement Program

1. **Components of the NERC Compliance Enforcement Program** — NERC shall develop and implement a NERC Compliance Monitoring and Enforcement Program to promote the reliability of the bulk power system by enforcing compliance with approved reliability standards in those regions of North American in which NERC and/or a regional entity (pursuant to a delegation agreement with NERC that has been approved by the applicable ERO governmental authority) has been given enforcement authority. There are four distinct parts of the NERC Monitoring and Compliance Enforcement Program: (1) NERC's oversight of the regional entity compliance programs (Section 402), (2) the definition of the required regional entity compliance enforcement program attributes (Section 403), (3) NERC's monitoring of regional entity compliance with reliability standards (Section 404), and (4) the monitoring of compliance with reliability standards that are applicable to NERC (Sections 405–406).

2. **Who Must Comply** — Where required by applicable legislation, regulation, rule or agreement, all bulk power system owners, operators, and users, regional entities, and NERC, are required to comply with all approved NERC reliability standards at all times. Regional reliability standards and regional variances approved by NERC and the applicable ERO governmental authority shall be considered NERC reliability standards and shall apply to all bulk power system owners, operators, or users responsible for meeting those standards within the regional entity boundaries, whether or not the bulk power system owner, operator, or user is a member of the regional entity.

3. **Data Access** — All bulk power system owners, operators, and users shall provide to NERC and the applicable regional entity such information as is necessary to monitor compliance with the reliability standards. NERC and the applicable regional entity will define the data retention and reporting requirements in the reliability standards and compliance reporting procedures.

4. **Role of Regional Entities in the Compliance Enforcement Program** — Each regional entity that has been delegated authority through a delegation agreement or other legal instrument approved by the applicable ERO governmental authority shall, in accordance with the terms of the approved delegation agreement, administer a regional entity compliance enforcement program to meet the NERC Compliance Monitoring and Enforcement Program goals and the requirements in this Section 400.

5. **Program Continuity** — NERC will ensure continuity of compliance monitoring and enforcement within the geographic boundaries of a regional entity in the event that NERC does not have a delegation agreement, or the regional entity withdraws from the agreement or does not operate its compliance enforcement program in accordance with the delegation agreement or other applicable requirements.

5.1 Should NERC not have a delegation agreement with a regional entity covering a geographic area, or a regional entity withdraws from an existing delegation agreement or the delegation agreement is otherwise terminated, NERC will directly administer the Compliance Monitoring and Enforcement Program applicable to owners, operators and users of the bulk-power system within that geographic area.

1. This monitoring and enforcement will be accomplished by NERC and compliance staff from another approved regional entity.

2. If an existing delegation agreement with a regional entity is terminating, the regional entity shall promptly provide to NERC all relevant compliance information regarding registered entities, contacts, prior compliance information and actions, mitigation plans, and remedial actions for the period in which the regional entity was responsible for administering the Compliance Monitoring and Enforcement Program.

3. NERC will levy and collect all penalties directly and will utilize any penalty monies collected to offset the expenses of administering the compliance monitoring and enforcement program for the geographic area.

5.2 Should a regional entity seek to withdraw from its delegation agreement, NERC will seek agreement from another regional entity to amend its delegation agreement with NERC to extend that regional entity's boundaries for compliance monitoring and enforcement. In the event no regional entity is willing to accept this responsibility, NERC will administer the Compliance Monitoring and Enforcement Program within the geographical boundaries of the regional entity seeking to withdraw from the delegation agreement, in accordance with Section 401.5.1.

6. **Actively Monitored Requirements** — NERC, with input from the regional entities, stakeholders, and regulators, shall annually select a subset of the NERC reliability standards and requirements to be actively monitored and audited in the NERC annual compliance program. Compliance is required, and NERC and the regional entities have authority to monitor compliance, with all NERC reliability standards whether or not they are included in the subset of reliability standards and requirements designated to be actively monitored and audited in the NERC annual compliance program.

7. **Penalties, Sanctions, and Remedial Action Directives** — NERC and regional entities will apply penalties, sanctions, and remedial action directives that bear a reasonable relation to the seriousness of a violation and take into consideration timely remedial efforts as defined in the NERC *Sanction Guidelines*, which is incorporated into these rules as **Appendix 4B**.

8. **Multiple Enforcement Actions** – A registered entity shall not be subject to an enforcement action by NERC and a regional entity, or by more than one regional entity, for the same violation.

9. **Records** — NERC shall maintain a record of each compliance submission, including self-reported, possible, alleged, and confirmed violations of approved reliability standards; associated penalties, sanctions, remedial action directives and settlements; and the status of mitigation actions.

10. **Confidential Information** — NERC will treat all possible and alleged violations of reliability standards and matters related to a compliance monitoring and enforcement program process, including the status of any compliance investigation or other compliance monitoring and enforcement process, as confidential in accordance with Section 1500.

    The types of information that will be considered confidential and will not (subject to statutory and regulatory requirements) be disclosed in any public information reported by NERC are identified in Section 1500. Information that would jeopardize bulk power system reliability, including information relating to a Cyber Security Incident, will be identified and protected from public disclosure as critical energy infrastructure information in accordance with Section 1500.

    The regional entity and NERC shall give bulk power system owners, operators, and users a reasonable opportunity to demonstrate that information concerning a violation is confidential before such report is disclosed to the public.

11. **Public Posting** — When the affected bulk power system owner, operator, or user either agrees with a possible or alleged violation(s) of a reliability standard(s) or a report of a compliance audit or compliance investigation, or enters into a settlement agreement concerning a possible or alleged violation(s), or the time for submitting an appeal is passed, or all appeals processes are complete, NERC shall, subject to the confidentiality requirements of these rules, publicly post each confirmed violation, penalty or sanction, settlement agreement, and final compliance audit or compliance investigation report, on its Web site.

    11.1 Each bulk power system owner, operator, or user may provide NERC with a statement to accompany the violation or report to be posted publicly. The statement must be on company letterhead and include a signature, as well as the name and title of the person submitting the information.

    11.2 In accordance with Section 1500, information deemed by a bulk power system owner, operator, or user, regional entity, or NERC as critical energy infrastructure information (*NERC Security Guidelines for the Electricity Sector — Protecting Potentially Sensitive Information* may be used as a guide) or other confidential information shall be redacted in accordance with Section 1500 and not be released publicly.

    11.3 Subject to redaction of critical energy infrastructure information or other confidential information, for each confirmed violation or settlement relating to a possible violation or an alleged violation, the public posting shall include the name of any relevant entity, the nature, time period, and circumstances of such possible, alleged or confirmed violation, any

mitigation plan or other mitigating activities to be implemented by the entity in connection with the violation or settlement, and sufficient facts to assist owners, operators and users of the bulk power system to evaluate whether they have engaged in or are engaging in similar activities.

12. **Violation Information Review** — NERC compliance monitoring and enforcement program staff shall periodically review and analyze all reports of possible, alleged and confirmed violations to identify trends and other pertinent reliability issues.

402. NERC Oversight of the Regional Entity Compliance Enforcement Programs

1. **NERC Monitoring Program** — NERC shall have a program to monitor the compliance enforcement program of each regional entity that has been delegated authority. The objective of this monitoring program shall be to ensure that the regional entity carries out its compliance enforcement program in accordance with these rules and the terms of the delegation agreement, and to ensure consistency and fairness of the regional entity's compliance enforcement program. Oversight and monitoring by NERC shall be accomplished through an annual compliance enforcement program review, program audits, and regular evaluations of regional entity compliance enforcement program performance as described below.

   1.1 **NERC Review of Regional Compliance Enforcement Program Annual Plans** — NERC shall require each regional entity to submit for review and approval an annual compliance enforcement program implementation plan. NERC shall review each regional entity's compliance enforcement program annual implementation plan and shall accept the plan if it meets NERC requirements and the requirements of the delegation agreement.

   1.2 **Regional Entity Program Evaluation** — NERC shall annually evaluate the goals, tools, and procedures of each regional entity compliance enforcement program to determine the effectiveness of each regional entity program, using criteria developed by the NERC Compliance and Certification Committee.

   1.3 **Regional Entity Program Audit** — At least once every five years, NERC shall conduct an audit to evaluate how each regional entity compliance enforcement program implements the NERC Compliance Monitoring and Enforcement Program. The evaluation shall be based on these rules of procedures, including Appendix 4C, the delegation agreement, directives in effect pursuant to the delegation agreement, approved regional entity annual compliance enforcement program annual implementation plans, required program attributes, and the NERC compliance program procedures. These evaluations shall be provided to the appropriate ERO governmental authorities to demonstrate the effectiveness of each regional entity. In addition, audits of cross-border regional entities shall cover applicable requirements imposed on the regional entity by statute, regulation, or order of, or agreement with, provincial governmental and/or regulatory authorities for which NERC has auditing responsibilities over

the regional entity's compliance with such requirements within Canada or Mexico. Participation of a representative of an applicable ERO governmental authority shall be subject to the limitations of sections 3.1.6 and 8.0 of Appendix 4C of these rules of procedure regarding disclosures of non-public compliance information related to other jurisdictions. NERC shall maintain an audit procedure containing the requirements, steps, and timelines to conduct an audit of each regional entity compliance enforcement program. The current procedure is contained in the NERC Audit of Regional Entity Compliance Programs, which is incorporated into these rules as **Appendix 4A**.

1.4 ERO governmental authorities will be allowed to participate as an observer in any audit conducted by NERC of a regional entity's compliance monitoring and enforcement program. A representative of the regional entity being audited will be allowed to participate in the audit as an observer.

2. **Consistency Among Regional Compliance Enforcement Programs** — To provide for a consistent compliance enforcement program for all bulk power system owners, operators, and users required to comply with approved reliability standards, NERC shall maintain a single, uniform Compliance Monitoring and Enforcement Program, which is incorporated into these rules of procedure as **Appendix 4C**. Any differences in regional entity program methods, including determination of violations and penalty assessment, shall be justified on a case-by-case basis and fully documented in each regional entity delegation agreement.

2.1 NERC shall ensure that each of the regional entity compliance enforcement programs meets these Rules of Procedure, including **Appendix 4C**, and follows the terms of the delegation agreement and the approved regional entity compliance enforcement program annual plan.

2.2 NERC shall maintain a single, uniform compliance monitoring and enforcement program in **Appendix 4C** containing the procedures to ensure the consistency and fairness of the processes used to determine regional entity compliance enforcement program findings of compliance and noncompliance, and the application of penalties and sanctions.

2.3 NERC shall periodically conduct regional entity compliance manager forums. These forums shall use the results of regional entity compliance program audits and findings of NERC compliance staff to identify and refine regional entity compliance program differences into a set of best practices over time.

3. **Information Collection and Reporting** — NERC and the regional entities shall implement data management procedures that address data reporting requirements, data integrity, data retention, data security, and data confidentiality.

4. **Violation Disclosure** — NERC shall disclose all confirmed violations and maintain as confidential possible violations and alleged violations, according to the reporting and disclosure process in **Appendix 4C**.

5. **Authority to Determine Noncompliance, Levy Penalties and Sanctions, and Issue Remedial Action Directives** — NERC and regional entity compliance staff shall have the authority and responsibility to make initial determinations of compliance or noncompliance, and where authorized by the appropriate governmental authorities or where otherwise authorized, to determine penalties and sanctions for noncompliance with a reliability standard, and issue remedial action directives. Regional entity boards or a compliance panel reporting directly to the regional entity board will be vested with the authority for the overall regional entity compliance program and have the authority to impose penalties and sanctions on behalf of NERC, where authorized by applicable legislation or agreement. Remedial action directives may be issued by NERC or a regional entity that is aware of a bulk power system owner, operator, or user that is, or is about to engage in an act or practice that would result, in noncompliance with a reliability standard, where such directive is immediately necessary to protect the reliability of the bulk power system from an imminent or actual threat. If, after receiving such a directive, the bulk power system owner, operator, or user does not take appropriate action to avert a violation of a reliability standard, NERC may petition the applicable ERO governmental authority to issue a compliance order.

6. **Due Process** — NERC shall establish and maintain a fair, independent, and nondiscriminatory appeals process. The appeals process is set forth in Sections 408-410. The process shall allow bulk power system owners, operators, and users to appeal the regional entity's findings of noncompliance and to appeal penalties, sanctions, and remedial action directives that are levied by the regional entity. Appeals beyond the NERC process will be heard by the applicable ERO governmental authority.

   The appeals process will also allow for appeals to NERC of any findings of noncompliance issued by NERC to a regional entity for standards and requirements where the regional entity is monitored for compliance to a reliability standard. No monetary penalties will be levied in these matters; however sanctions, remedial actions, and directives to comply may be applied by NERC.

7. **Conflict Disclosure** — NERC shall disclose to the appropriate governmental authorities any potential conflicts between a market rule and the enforcement of a regional reliability standard.

8. **Confidentiality** — To maintain the integrity of the NERC Compliance Monitoring and Enforcement Program, NERC and regional entity staff, audit team members, and committee members shall maintain the confidentiality of information obtained and shared during compliance monitoring and enforcement

processes including investigations, audits, spot checks, drafting of reports, appeals, and closed meetings.

8.1 NERC and the regional entity shall have in place appropriate codes of conduct and confidentiality agreements for staff and other compliance enforcement program participants.

8.2 Individuals not bound by NERC or regional entity codes of conduct who serve on compliance-related committees or audit teams shall sign a NERC confidentiality agreement prior to participating on the committee or team.

8.3 Information deemed by a bulk power system owner, operator, or user, regional entity, or NERC as critical energy infrastructure information shall not be distributed outside of a committee or team, nor released publicly. Other information subject to confidentiality is identified in Section 1500.

8.4 In the event that a staff, committee, or audit team member violates any of the confidentiality rules set forth above, the staff, committee, or audit team member and any member organization with which the individual is associated may be subject to appropriate action by the regional entity or NERC, including prohibiting participation in future compliance enforcement activities.

9. **Auditor Training** — NERC shall develop and provide training in auditing skills to all people who participate in NERC and regional entity compliance enforcement audits. Training for NERC and regional entity personnel and others who serve as compliance audit team leaders shall be more comprehensive than training given to industry subject matter experts and regional entity members. Training for regional entity members may be delegated to the regional entity.

403. Required Attributes of Regional Entity Compliance Enforcement Programs

Each regional entity compliance enforcement program shall promote excellence in the enforcement of reliability standards. To accomplish this goal, each regional entity compliance enforcement program shall (i) conform to and comply with the NERC uniform Compliance Monitoring and Enforcement Program, **Appendix 4C** to these rules of procedure, except to the extent of any deviations that are stated in the regional entity's delegation agreement, and (ii) meet all of the attributes set forth in this Section 403.

Program Structure

1. **Independence** — Each regional entity's governance of its compliance enforcement program shall exhibit independence, meaning the compliance enforcement program shall be organized so that its compliance monitoring and enforcement activities are carried out separately from other activities of the regional entity. The program shall not be unduly influenced by the bulk power system owners, operators, and users being monitored or other regional entity activities that are required to meet the reliability standards. Regional entities must

include rules providing that no two industry sectors may control any decision and no single segment may veto any matter related to compliance.

2. **Exercising Authority** — Each regional entity compliance enforcement program shall exercise the responsibility and authority in carrying out the delegated functions of the NERC Compliance Monitoring and Enforcement Program in accordance with delegation agreements and **Appendix 4C**. These functions include but are not limited to: data gathering, data reporting, compliance investigations, compliance auditing activities, evaluating compliance and noncompliance, imposing penalties and sanctions, and approving and tracking mitigation actions.

3. **Delegation of Authority** — To maintain independence, fairness, and consistency in the NERC Compliance Monitoring and Enforcement Program, a regional entity shall not sub-delegate its compliance enforcement program duties to entities or persons other than the regional entity compliance enforcement program staff, unless (i) required by statute or regulation in the applicable jurisdiction, or (ii) by agreement with express approval of NERC and of FERC or other appropriate ERO governmental authority, to another regional entity.

4. **Hearings of Contested Findings or Sanctions —** The regional entity board or compliance panel reporting directly to the regional entity board (with appropriate recusal procedures) will be vested with the authority for conducting compliance hearings in which any bulk power system owner, operator, or user provided notice of an alleged violation may present facts and other information to contest a notice of alleged violation or any proposed penalty, sanction, any remedial action directive, or any mitigation plan component. Compliance hearings shall be conducted in accordance with the Hearing ~~Process~~Procedures set forth in Attachment 2 to **Appendix 4C**. If a stakeholder body serves as the hearing body, no two industry sectors may control any decision and no single segment may veto any matter related to compliance after recusals.

Program Resources

5. **Regional Entity Compliance Staff** — Each regional entity shall have sufficient resources to meet delegated compliance monitoring and enforcement responsibilities, including the necessary professional staff to manage and implement the regional entity compliance monitoring and enforcement program.

6. **Regional Entity Compliance Staff Independence** — The regional entity compliance monitoring and enforcement program staff shall be capable of and required to make all determinations of compliance and noncompliance and determine penalties, sanctions, mitigating activities and remedial action directives.

   6.1 Regional entity compliance enforcement program staff shall not have a conflict of interest, real or perceived, in the outcome of compliance monitoring and enforcement processes, reports, or sanctions. The regional entity shall have in effect a conflict of interest policy.

6.2 Regional entity compliance monitoring and enforcement program staff shall have the authority and responsibility to carry out compliance monitoring and enforcement processes (with the input of industry subject matter experts), make determinations of compliance or noncompliance, and levy penalties and sanctions without interference or undue influence from regional entity members and their representative or other industry entities.

6.3 Regional entity compliance monitoring and enforcement program staff may call upon independent technical subject matter experts who have no conflict of interest in the outcome of the compliance monitoring and enforcement process to provide technical advice or recommendations in the determination of compliance or noncompliance.

6.4 Regional entity compliance monitoring and enforcement program staff shall abide by the confidentiality requirements contained in Section 1500 and **Appendix 4C** of these Rules of Procedure, the NERC delegation agreement and other confidentiality agreements required by the NERC Compliance Monitoring and Enforcement Program.

6.5 Contracting with independent consultants or others working for the regional entity compliance enforcement program shall be permitted provided the individual has not received compensation from a bulk power system owner, operator, or user being monitored for a period of at least the preceding six months and owns no financial interest in any bulk power system owner, operator, or user being monitored for compliance to the reliability standard, regardless of where the bulk power system owner, operator, or user operates. Any such individuals for the purpose of these rules shall be considered as augmenting regional entity compliance staff.

7. Use of Industry Subject Matter Experts and Regional Entity Members — Industry experts and regional entity members may be called upon to provide their technical expertise in compliance monitoring and enforcement program activities.

7.1 The regional entity shall have procedures defining the allowable involvement of industry subject matter experts and regional entity members. The procedures shall address applicable antitrust laws and conflicts of interest.

7.2 Industry subject matter experts and regional entity members shall have no conflict of interest or financial interests in the outcome of their activities.

7.3 Regional entity members and industry subject matter experts, as part of teams or regional entity committees, may provide input to the regional entity compliance staff so long as the authority and responsibility for (i) evaluating and determining compliance or noncompliance and (ii) levying penalties, sanctions, or remedial action directives shall not be delegated to any person or entity other than the compliance staff of the regional entity. Industry subject matter experts, regional entity members, or regional entity

committees shall not make determinations of noncompliance or levy penalties, sanctions, or remedial action directives. Any committee involved shall be organized so that no two industry sectors may control any decision and no single segment may veto any matter related to compliance.

7.4 Industry subject matter experts and regional entity members shall sign a confidentiality agreement appropriate for the activity being performed.

7.5 All industry subject matter experts and regional entity members participating in compliance audits and compliance investigations shall successfully complete auditor training provided by NERC or the regional entity prior to performing these activities

Program Design

8. **Regional Entity Compliance Enforcement Program Content** — All approved reliability standards shall be included in the regional entity compliance monitoring and enforcement program for all bulk power system owners, operators, and users within the defined boundaries of the regional entity. Compliance to approved regional entity reliability standards is applicable only within the footprint of the regional entity that submitted those particular regional entity reliability standards for approval. NERC will identify the minimum set of reliability standards and requirements to be actively monitored by the regional entity in a given year.

9. **Antitrust Provisions** — Each regional entity's compliance monitoring and enforcement program shall be structured and administered to abide by U.S. antitrust law and Canadian competition law.

10. **Information Submittal** — All bulk power system owners, operators, and users within the regional entity responsible for complying with reliability standards shall submit timely and accurate information when requested by the regional entity or NERC. NERC and the regional entities shall preserve any mark of confidentiality on information submitted pursuant to Section 1502.1.

10.1 Each regional entity has the authority to collect the necessary information to determine compliance and shall develop processes for gathering data from the bulk power system owners, operators, and users the regional entity monitors.

10.2 The regional entity or NERC has the authority to request information from bulk power system owners, operators, and users pursuant to section 401.3 or this section 403.10 without invoking a specific compliance monitoring and enforcement process in **Appendix 4C**, for purposes of determining whether to pursue one such process in a particular case and/or validating in the enforcement phase of a matter the conclusions reached through the compliance monitoring and enforcement process(es).

10.3 When required or requested, the regional entities shall report information to NERC promptly and in accordance with **Appendix 4C** and other NERC procedures.

10.4 Regional entities shall notify NERC of all possible, alleged and confirmed violations of NERC reliability standards by entities over which the regional entity has compliance monitoring and enforcement authority , in accordance with **Appendix 4C**.

10.5 A bulk power system owner, operator, or user found in noncompliance with a reliability standard shall submit a mitigation plan with a timeline addressing how the noncompliance will be corrected. The regional entity compliance staff shall review and approve the mitigation plan in accordance with **Appendix 4C**.

10.6 An officer of a bulk power system owner, operator, or user shall certify as accurate all compliance data self-reported to the regional entity compliance monitoring and enforcement program.

10.7 Regional entities shall develop and implement procedures to verify the compliance information submitted by bulk power system owners, operators, and users.

11. **Compliance Audits of Bulk Power System Owners, Operators, and Users** — Each regional entity will maintain and implement a program of proactive compliance audits of bulk power system owners, operators, and users responsible for complying with reliability standards, in accordance with **Appendix 4C**. A compliance audit is a process in which a detailed review of the activities of a bulk power system owner, operator, or user is performed to determine if that bulk power system owner, operator, or user is complying with approved reliability standards.

11.1 For an entity registered as a balancing authority, reliability coordinator, or transmission operator, the compliance audit will be performed at least once every three years. For other bulk power system owners, operators, and users on the NERC Compliance Registry, compliance audits shall be performed on a schedule established by NERC.

11.2 Audits of balancing authorities, reliability coordinators, and transmission operators will include a component at the audited entity's site. For other bulk power system owners, operators, and users on the NERC Compliance Registry, the audit may be either an on-site audit or based on review of documents, as determined to be necessary and appropriate by NERC or regional entity compliance monitoring and enforcement program, staff.

11.3 Compliance audits must include a detailed review of the activities of the bulk power system owner, operator, or user to determine if the bulk power system owner, operator, or user is complying with all approved reliability

standards identified for audit by NERC. The compliance audit shall include a review of supporting documentation and evidence used by the bulk power system owner, operator or user to demonstrate compliance for an appropriate period prior to the compliance audit.

12. **Confidentiality of Compliance Monitoring and Enforcement Processes** — All compliance monitoring and enforcement processes, and information obtained from such processes, are to be non-public and treated as confidential in accordance with Section 1500 and **Appendix 4C** of these rules of procedure, unless NERC, the regional entity or FERC or another applicable governmental authority with jurisdiction determines a need to conduct a compliance monitoring and enforcement program process on a public basis, provided, that NERC and the regional entities shall publish (i) schedules of compliance audits scheduled in each year, (ii) a public report of each compliance audit, and (iii) notices of penalty and settlement agreements. Advance authorization from the applicable ERO governmental authority is required to make public any compliance monitoring and enforcement process or any information relating to a compliance monitoring and enforcement process, or to permit interventions when determining whether to impose a penalty. This prohibition on making public any compliance monitoring and enforcement process does not prohibit NERC or a regional entity from publicly disclosing (i) the initiation of or results from an analysis of a significant system event under Section 807 or of off-normal events or system performance under Section 808, or (ii) information of general applicability and usefulness to owners, operators, and users of the bulk power system concerning reliability and compliance matters, so long as specific allegations or conclusions regarding possible or alleged violations of reliability standards are not included in such disclosures.

13. **Critical Energy Infrastructure Information** — Information that would jeopardize bulk power system reliability, including information relating to a Cyber Security Incident will be identified and protected from public disclosure as critical energy infrastructure information. In accordance with Section 1500, information deemed by a bulk power system owner, operator, or user, regional entity, or NERC as critical energy infrastructure information shall be redacted according to NERC procedures and shall not be released publicly.

14. **Penalties, Sanctions, and Remedial Action Directives** — Each regional entity will apply all penalties, sanctions, and remedial action directives in accordance with the approved *Sanction Guidelines*, **Appendix 4B** to these rules of procedure. Any changes to the *Sanction Guidelines* to be used by any regional entity must be approved by NERC and submitted to the appropriate ERO governmental body for approval. All confirmed violations, penalties, and sanctions, including confirmed violations, penalties and sanctions specified in a regional entity hearing body final decision, will be provided to NERC for review and filing with applicable ERO governmental authorities as a notice of penalty, in accordance with **Appendix 4C**.

15. **Regional Hearing Process** — Each regional entity compliance enforcement program shall establish and maintain a fair, independent, and nondiscriminatory process for hearing contested violations and any penalties or sanctions levied, in conformance with Attachment 2 to **Appendix 4C** to these rules of procedure and any deviations therefrom that are set forth in the regional entity's delegation agreement.. The hearing process shall allow bulk power system owners, operators, and users to contest findings of compliance violations, any penalties and sanctions that are proposed to be levied, proposed remedial action directives, and components of proposed mitigation plans. The regional entity hearing process shall be conducted before the regional entity board or a balanced committee established by and reporting to the regional entity board as the final adjudicator, provided, that Canadian provincial regulators may act as the final adjudicator in their respective jurisdictions. The regional entity hearing process shall (i) include provisions for recusal of any members of the hearing body with a potential conflict of interest, real or perceived, from all compliance matters considered by the hearing body for which the potential conflict of interest exists and (ii) provide that no two industry sectors may control any decision and no single segment may veto any matter brought before the hearing body after recusals.

    Each regional entity will notify NERC of all hearings and NERC may observe any of the proceedings. Each regional entity will notify NERC of the outcome of all hearings.

    If a bulk power system owner, operator, or user or a regional entity has completed the regional entity hearing process and desires to appeal the outcome of the hearing, the bulk power system owner, operator, or user or the regional entity shall appeal to NERC in accordance with Section 409 of these rules of procedure, except that a determination of violation or penalty that has been directly adjudicated by an ERO governmental authority shall be appealed with that ERO governmental authority.

16. **Annual Regional Entity Compliance Enforcement Program Implementation Plan** — Each regional entity shall annually develop and submit to NERC for approval a regional entity compliance enforcement implementation plan in accordance with **Appendix 4C** that identifies the reliability standards and requirements to be actively monitored (both those required by NERC and any additional reliability standards the regional entity proposes to monitor), and how each NERC and regional entity identified standard will be monitored, evaluated, reported, sanctioned, and appealed. These implementation plans will be submitted to NERC on the schedule established by NERC, generally on or about ~~November~~October 1 of the preceding year. In conjunction with the annual implementation plan, each regional entity must report to NERC regarding how it carried out its delegated compliance monitoring and enforcement authority in the previous year, the effectiveness of the program, and changes expected to correct any deficiencies identified. Each regional entity will provide its annual report on

the schedule established by NERC, generally on or about February 15 of the following year.

404. NERC Monitoring of Compliance for Regional Entities or Bulk Power Owners, Operator, or Users

NERC shall monitor regional entity compliance with NERC reliability standards and, if no there is no delegation agreement in effect with a regional entity for the geographic area, shall monitor bulk power system owners, operators, and users for compliance with NERC reliability standards. Industry subject matter experts may be used as appropriate in compliance investigations, compliance audits, and other compliance activities, subject to confidentiality, antitrust, and conflict of interest provisions.

1. **NERC Obligations** — NERC compliance monitoring and enforcement staff shall monitor the compliance of the regional entity with the reliability standards for which the regional entities are responsible, in accordance with **Appendix 4C**. NERC shall actively monitor in its annual Compliance Enforcement and Monitoring Program selected reliability standards that apply to the regional entities. NERC shall evaluate compliance and noncompliance with all of the reliability standards that apply to the regional entities and shall impose sanctions, penalties, or remedial action directives when there is a finding of noncompliance. NERC shall post all violations of reliability standards that apply to the regional entities as described in the reporting and disclosure process in **Appendix 4C**.

   In addition, NERC will directly monitor bulk power system owners, operators, and users for compliance with NERC Reliability Standards in any geographic area for which there is not a delegation agreement in effect with a regional entity, in accordance with **Appendix 4C**. In such cases, NERC will serve as the Compliance Enforcement Authority described in **Appendix 4C**. Compliance matters contested by bulk power system owners, operators, and users in such an event will be heard by the NERC Compliance and Certification Committee.

2. **Compliance Audit of the Regional Entity** — NERC shall perform a compliance audit of each regional entity responsible for complying with reliability standards at least once every three years. NERC shall make an evaluation of compliance based on the information obtained through the audit. After due process is complete, the final audit report shall be made public in accordance with the reporting and disclosure process in **Appendix 4C**.

3. **Appeals Process** —Any regional entity or bulk-power system owner, operator or user found by NERC, as opposed to a regional entity, to be in noncompliance with a reliability standard may appeal the findings of noncompliance with reliability standards and any sanctions or remedial action directives that are issued by, or mitigation plan components imposed by, NERC, pursuant to the processes described in Sections 408 through 410.

405. Monitoring of Standards and Other Requirements Applicable to NERC

The NERC Compliance and Certification Committee shall establish and implement a process to monitor NERC's compliance with the reliability standards that apply to NERC. The process shall use independent monitors with no conflict of interest, real or perceived, in the outcomes of the process. All violations shall be made public according to the reporting and disclosure process in **Appendix 4C**. The Compliance and Certification Committee will also establish a procedure for monitoring NERC's compliance with its Rules of Procedure for the Standards Development, Compliance Enforcement, and Organization Registration and Certification Programs. Such procedures shall not be used to circumvent the appeals processes established for those programs.

406. Independent Audits of the NERC Compliance Monitoring and Enforcement Program

NERC shall provide for an independent audit of its compliance monitoring and enforcement program at least once every three years, or more frequently as determined by the board. The audit shall be conducted by independent expert auditors as selected by the board. The independent audit shall meet the following minimum requirements and any other requirements established by the NERC board.

1. **Effectiveness** — The audit shall evaluate the success and effectiveness of the NERC Compliance Monitoring and Enforcement Program in achieving its mission.

2. **Relationship** — The audit shall evaluate the relationship between NERC and the regional entity compliance enforcement programs and the effectiveness of the programs in ensuring reliability.

3. **Final Report Posting** — The final report shall be posted by NERC for public viewing in accordance with **Appendix 4C**.

4. **Response to Recommendations** — If the audit report includes recommendations to improve the NERC Compliance Monitoring and Enforcement Program, the administrators of the NERC Compliance Monitoring and Enforcement Program shall provide a written response and plan to the board within 30 days of the release of the final audit report.

407. Penalties, Sanctions, and Remedial Action Directives

1. **NERC Review of Regional Penalties and Sanctions —** NERC shall review all penalties, sanctions, and remedial action directives imposed by each regional entity for violations of reliability standards, including penalties, sanctions and remedial action directives that are specified by a regional entity hearing body final decision, to determine if the regional entity's determination is supported by a sufficient record compiled by the regional entity, is consistent with the *Sanction Guidelines* incorporated into these rules as **Appendix 4B** and with other directives, guidance and directions issued by NERC pursuant to the delegation agreement, and is consistent with penalties, sanctions and remedial action directives imposed by the regional entity and by other regional entities for violations involving the same or similar facts and circumstances.

2. **Developing Penalties and Sanctions** — The regional entity compliance monitoring and enforcement program staff shall use the *Sanction Guidelines*, which are incorporated into these rules as **Appendix 4B**, to develop an appropriate penalty, sanction, or remedial action directive for a violation, and shall notify NERC of the penalty, ~~or~~ sanction or remedial action directive.

3. **Effective Date of Penalty** — Where authorized by applicable legislation or agreement, no penalty imposed for a violation of a reliability standard shall take effect until the thirty-first day after NERC files, with the applicable ERO governmental authority, a "notice of penalty" and the record of the proceedings in which the violation and penalty were determined, or such other date as ordered by the ERO applicable governmental authority.

408. Review of NERC Decisions

1. **Scope of Review** — A registered entity or a regional entity wishing to challenge a finding of noncompliance and the imposition of a penalty for a compliance measure directly administered by NERC, or a regional entity wishing to challenge a regional compliance program audit finding, may do so by filing a notice of the challenge with NERC's director of ~~compliance~~enforcement no later than 21 days after issuance of the notice of finding of violation or audit finding. Appeals by registered entities or regional entities of decisions of regional entity hearing bodies shall be pursuant to section 409 .

2. **Contents of Notice** — The notice of challenge shall include the full text of the decision that is being challenged, a concise statement of the error or errors contained in the decision, a clear statement of the relief being sought, and argument in sufficient detail to justify such relief.

3. **Response by NERC Compliance Monitoring and Enforcement Program** — Within 21 days after receiving a copy of the notice of challenge, the NERC ~~D~~director of ~~Compliance~~enforcement may file with the hearing body a response to the issues raised in the notice, with a copy to the regional entity.

4. **Hearing by Compliance and Certification Committee** — The NERC Compliance and Certification Committee shall provide representatives of the regional entity or registered entity, and the NERC Compliance Monitoring and Enforcement Program an opportunity to be heard and shall decide the matter based upon the filings and presentations made, with a written explanation of its decision.

5. **Appeal** — The regional entity~~,~~ or registered entity may appeal the decision of the Compliance and Certification Committee by filing a notice of appeal with NERC's director of ~~compliance~~enforcement no later than 21 days after issuance of the written decision by the Compliance and Certification Committee. The notice of appeal shall include the full text of the written decision of the Compliance and Certification Committee that is being appealed, a concise statement of the error or errors contained in the decision, a clear statement of the

relief being sought, and argument in sufficient detail to justify such relief. No factual material shall be presented in the appeal that was not presented to the Compliance and Certification Committee.

6. **Response by NERC Compliance Monitoring and Enforcement Program** — Within 21 days after receiving a copy of the notice of appeal, the NERC Compliance Monitoring and Enforcement Program staff may file its response to the issues raised in the notice of appeal, with a copy to the entity filing the notice.

7. **Reply** — The entity filing the appeal may file a reply within 7 days.

8. **Decision** — The Compliance Committee of the NERC Board of Trustees shall decide the appeal, in writing, based upon the notice of appeal, the record, the response, and any reply. At its discretion, the Compliance Committee may invite representatives of the regional entity or registered entity, and the NERC Compliance Monitoring and Enforcement Program to appear before the Committee. Decisions of the Compliance Committee shall be final, except for further appeal to the applicable ERO governmental authority.

9. **Impartiality** — No member of the Compliance and Certification Committee or the Board of Trustees Compliance Committee having an actual or perceived conflict of interest in the matter may participate in any aspect of the challenge or appeal except as a party or witness.

10. **Expenses** — Each party in the challenge and appeals processes shall pay its own expenses for each step in the process.

11. **Non-Public Proceedings —** All challenges and appeals shall be closed to the public to protect confidential information.

409. Appeals from Final Decisions of Regional Entities

1. **Time for Appeal** — A regional entity acting as the compliance enforcement authority, or an owner, operator or user of the bulk-power system, ~~wishing~~ shall be entitled to appeal ~~from~~ a final decision of a regional entity hearing body concerning ~~that finds~~ an alleged violation of a reliability standard, a proposed ~~or imposes a~~ penalty or sanction for violation of a reliability standard, a proposed mitigation plan, or a proposed remedial action directive, ~~shall file its~~by filing a notice of appeal with NERC's director of enforcement~~compliance~~, with ~~a copy~~copies to the regional entity and any other participants in the regional entity hearing body proceeding, no later than 21 days after issuance of the final decision of the regional entity hearing body. ~~The same appeal procedures will apply regardless of whether the matter first arose in a compliance investigation, compliance audit or self-report, other compliance monitoring and enforcement process, or in a reliability readiness evaluation.~~

2. **Contents** — The notice of appeal shall include the full text of the final decision of the regional entity hearing body that is being appealed, a concise statement of

the error or errors contained in the final decision, a clear statement of the relief being sought, and argument in sufficient detail to justify such relief. No factual material shall be presented in the appeal that was not first presented during the ~~compliance hearing~~proceeding before the regional entity hearing body.

3. **Response to Notice of Appeal~~by Regional Entity~~** — Within 21 days after the date~~receiving a copy of~~ the notice of appeal is filed, ~~(i)~~ the regional entity shall file the entire record of the ~~matter~~regional entity hearing body proceeding with NERC's director of ~~compliance~~enforcement, with a copy to the entity filing the notice of appeal~~,~~. ~~together with and (ii)~~Within 35 days after the date of the notice of appeal, all participants in the proceeding before the regional entity hearing body, other than the participant filing the notice of appeal, shall file their ~~its~~ responses to the issues raised in the notice of appeal.

4. **Reply** — The entity filing the appeal may file a reply to the responses~~regional entity~~ within 7 days.

5. **Decision** — The Compliance Committee of the NERC Board of Trustees shall decide the appeal, in writing, based upon the notice of appeal, the record of the ~~matter from~~ proceeding before the regional entity, the responses, and any replies~~y~~ filed with NERC. At its discretion, the Compliance Committee may invite representatives of the entity making the appeal and the other participants in the proceeding before the regional entity hearing body, to appear before the Committee. Decisions of the Compliance Committee shall be final, except for further appeal to the applicable ERO governmental authority.

6. **Expenses** — Each party in the appeals process shall pay its own expenses for each step in the process.

7. **Non-Public Proceedings** — All appeals shall be closed to the public to protect confidential information.

8. **Appeal of Hearing Body Decisions Granting or Denying Motions to Intervene** — This section is not applicable to an appeal of a decision of a regional entity hearing body granting or denying a motion to intervene in the regional entity hearing body proceeding. Appeals of decisions of regional entity hearing bodies granting or denying motions to intervene in regional entity hearing body proceedings shall be prosecuted and decided pursuant to Section 414.

410. Hold Harmless

A condition of invoking the challenge or appeals processes under Section 408 or 409 is that the entity requesting the challenge or appeal agrees that neither NERC (defined to include its members, Board of Trustees, committees, subcommittees, staff and industry subject matter experts), any person assisting in the challenge or appeals processes, nor any company employing a person assisting in the challenge or appeals processes, shall be liable, and they shall be held harmless against the consequences of or any action or inaction or of any agreement reached in resolution of the dispute or any failure to reach

agreement as a result of the challenge or appeals proceeding. This "hold harmless" clause does not extend to matters constituting gross negligence, intentional misconduct, or a breach of confidentiality.

411. Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards

A registered entity that is subject to a requirement of a NERC critical infrastructure protection reliability standard for which technical feasibility exceptions are permitted, may request a technical feasibility exception to the requirement, and the request will be reviewed, approved or disapproved, and if approved, implemented, in accordance with the NERC *Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standard*, Appendix 4D to these Rules of Procedure.

412. Certification of Questions from Regional Entity Hearing Bodies for Decision by the NERC Board of Trustees Compliance Committee

1. Certification from a Regional Entity Hearing Body

1.1 A regional entity hearing body that is conducting a hearing concerning a disputed compliance matter pursuant to Attachment 2, Hearing Procedures, of Appendix 4C, may certify to the NERC Board of Trustees, for decision, a significant question of law, policy or procedure the resolution of which may be determinative of the issues in the hearing in whole or in part, or as to which there are other extraordinary circumstances that make prompt consideration of the question by the Compliance Committee appropriate, in accordance with section 1.5.12 of the Hearing Procedures. All questions certified by a regional entity hearing body to the NERC Board of Trustees shall be considered and disposed of by the Compliance Committee of the Board of Trustees.

1.2. The Compliance Committee may accept or reject a certification of a question for decision. If the Compliance Committee rejects the certified question, it shall issue a written statement that the certification is rejected.

1.3 If the Compliance Committee accepts the certification of a question for decision, it shall establish a schedule by which the participants in the hearing before the regional entity hearing body may file memoranda and reply memoranda stating their positions as to how the question certified for decision should be decided by the Compliance Committee. The Compliance Committee may also request, or provide an opportunity for, the NERC Compliance Operations department, the NERC Compliance Enforcement department, and/or the NERC General Counsel to file memoranda stating their positions as to how the question certified for decision should be decided. After receiving such memoranda and reply memoranda as are filed in accordance with the schedule, the Compliance Committee shall issue a written decision on the certified question.

1.4. Upon receiving the Compliance Committee's written decision on the certified question, the regional entity hearing body shall proceed to complete the hearing in accordance with the Compliance Committee's decision.

2. Publication of Decisions of the Board of Trustees Compliance Committee on Certified Questions

NERC shall post on its web site the written decisions issued by the Compliance Committee on certified questions. Consistent with the non-public nature of hearings before regional entity hearing bodies, in the posted decision the names of the regional entity, registered entity or entities, and any other participants in the regional entity hearing body hearing, and such other information as is necessary to maintain the non-public nature of the hearing before the regional entity hearing body, shall be redacted. Decisions of the Compliance Committee to not accept a question proposed for certification by the regional entity hearing body shall not be posted.

413. Review and Processing of Regional Entity Hearing Body Final Decisions that Are Not Appealed

NERC shall review and process all final decisions of regional entity hearing bodies concerning an alleged violation, proposed penalty or sanction, or proposed mitigation plan that are not appealed pursuant to section 409, as though the determination had been made by the regional entity compliance program. NERC shall review and process such final decisions, and may require that they be modified by the regional entity, in accordance with, as applicable to the particular decision, sections 5.8, 5.9 and 6.5 of Appendix 4C

414. Appeals of Decisions of Regional Entity Hearing Bodies Granting or Denying Motions to Intervene in Regional Entity Hearing Body Proceedings

1. **Time to Appeal** — An entity may appeal a decision of a regional entity hearing body under section 1.4.4 of Attachment 2 of **Appendix C** denying the entity's motion to intervene in a regional entity hearing body proceeding, and the regional entity compliance staff or any other participant in the regional entity hearing body proceeding may appeal a decision of the regional entity hearing body under section 1.4.4 of Attachment 2 of **Appendix C** granting or denying a motion to intervene in the regional entity hearing body proceeding, in either case by filing a notice of appeal with the NERC director of enforcement, with copies to the regional entity clerk, the hearing body, the hearing officer, the regional entity compliance staff, and all other participants in the regional entity hearing body proceeding, no later than seven (7) days following the date of the regional entity hearing body decision granting or denying the motion to intervene.

2. **Contents of Notice of Appeal** — The notice of appeal shall set forth information and argument to demonstrate that the decision of the regional entity hearing body

granting or denying the motion to intervene was erroneous under the grounds for intervention specified in section 1.4.4 of Attachment 2 of **Appendix 4C** and that the entity requesting intervention should be granted or denied intervention, as applicable. Facts alleged in, and any offers of proof made in, the notice of appeal shall be supported by affidavit or verification. The notice of appeal shall include a copy of the original motion to intervene and a copy of the decision of the regional entity hearing body granting or denying the motion to intervene.

3. **Responses to Notice of Appeal** — Within ten (10) days following the date the notice of appeal is filed, the regional entity clerk shall transmit to the NERC director of compliance copies of all pleadings filed in the regional entity hearing body proceeding on the motion to intervene. Within fourteen (14) days following the date the notice of appeal is filed, the regional entity hearing body, the regional entity compliance staff, and any other participants in the regional entity hearing body proceeding, may each file a response to the notice of appeal with the NERC director of enforcement. Within seven (7) days following the last day for filing responses, the entity filing the notice of appeal, and any participant in the regional entity hearing body proceeding that supports the appeal, may file replies to the responses with the NERC director of compliance.

4. **Disposition of Appeal** — The appeal shall be considered and decided by the Compliance Committee of the NERC Board of Trustees. The NERC director of compliance shall provide copies of the notice of appeal and any responses and replies to the Compliance Committee. The Compliance Committee shall issue a written decision on the appeal; provided, that if the Compliance Committee does not issue a written decision on the appeal within forty-five (45) days following the date of filing the notice of appeal, the appeal shall be deemed denied and the decision of the regional entity hearing body granting or denying the motion to intervene shall stand. The NERC director of compliance shall transmit copies of the Compliance Committee's decision, or shall provide notice that the forty-five (45) day period has expired with no decision by the Compliance Committee, to the regional entity clerk, the regional entity hearing body, the entity filing the notice of appeal, the regional entity compliance staff, and any other participants in the regional entity hearing body proceeding that filed responses to the notice of appeal or replies to responses.

5. **Appeal of Compliance Committee Decision to FERC or Other ERO Governmental Authority** — Any entity aggrieved by the decision of the Compliance Committee of the NERC Board of Trustees on an appeal of a regional entity hearing body decision granting or denying a motion to intervene in a regional entity hearing body proceeding (including a denial of such appeal by the expiration of the forty-five (45) period as provided in section 414.4) may appeal or petition for review of the decision of the Compliance Committee to FERC or to another ERO governmental authority having jurisdiction over the matter, in accordance with the authorities, rules and procedures of FERC or such other ERO governmental authority. Any such appeal or petition for review shall be filed within the time period, if any, and in the form and manner, specified by

the applicable statutes, rules or regulations governing proceedings before FERC or the other ERO governmental authority.

SECTION 500 — ORGANIZATION REGISTRATION AND CERTIFICATION

501. Scope of the Organization Registration and Organization Certification Programs

The purpose of the Organization Registration Program is to clearly identify those entities that are responsible for compliance with the FERC approved reliability standards. Organizations that are registered are included on the NERC Compliance Registry (NCR) and are responsible for knowing the content of and for complying with all applicable reliability standards. Registered organizations are not and do not become members of NERC or a Regional Entity, by virtue of being listed on the NCR. Membership in NERC is governed by Article II of NERC's bylaws; membership in a Regional Entity or regional reliability organization is governed by that entity's bylaws or rules.

The purpose of the Organization Certification Program is to ensure that ~~the new entity (i.e., applicant to be an RC, BA, or TOP that is not already performing the function for which it is applying to be certified as) has~~entities performing certain functions have the tools, processes, training, and procedures to demonstrate their ability to meet the requirements/sub requirements of all of the reliability standards applicable to the function(s) they perform~~for which it is applying~~ thereby demonstrating the ability to become certified and then operational.

Organization Registration and Organization Certification may be delegated to Regional Entities in accordance with the procedures in this Section 500; the NERC *Organization Registration and Organization Certification Manual*, which is incorporated into these rules as Appendix 5A; and, approved Regional Entity delegation agreements or other applicable agreements.

1. **NERC Compliance Registry** — NERC shall establish and maintain the NCR of the bulk power system owners, operators, and users that are subject to approved reliability standards.

   1.1 (a) The NCR shall set forth the identity and functions performed for each organization responsible for meeting requirements/sub-requirements of the reliability standards. Bulk power system owners, operators, and users (i) shall provide to NERC and the applicable Regional Entity information necessary to complete the registration, and (ii) shall provide NERC and the applicable Regional Entity with timely updates to information concerning the registered entity's ownership, operations, contact information, and other information that may affect the registered entity's registration status or other information recorded in the compliance registry.

   (b) A generation or transmission cooperative, a joint-action agency or another organization may register as a Joint Registration Organization (JRO), in lieu of each of the JRO's members or related entities being registered individually for one or more functions. Refer to Section 507.

(c) Multiple entities may each register using a Coordinated Functional Registration (CFR) for one or more reliability standard(s) and/or for one or more requirements/sub-requirements within particular reliability standard(s) applicable to a specific function pursuant to a written agreement for the division of compliance responsibility. Refer to Section 508.

1.2 In the development of the NCR, NERC and the Regional Entities shall determine which organizations should be placed on the NCR based on the criteria provided in the NERC *Statement of Compliance Registry Criteria* which is incorporated into these rules as Appendix 5B.

1.3 NERC and the Regional Entities shall use the following rules for establishing and maintaining the NCR based on the registration criteria as set forth in Appendix 5B *Statement of Compliance Registry Criteria*:

1.3.1 NERC shall notify each organization that it is on the NCR. NERC's notification shall state the effective date of the organization's registration. Where the organization is being registered for the first time and its bulk power system facilities were not previously owned by another registered entity, the effective date of the registration will be the date agreed to by the entity to be registered and the regional entity. Where the organization is being registered because it has acquired bulk power system facilities from a registered entity, or based on an internal restructuring or name change where the organization has been registered under a different entity name, the effective date of the registration will be the effective date of the transaction that results in the organization performing reliability functions that require it to be registered. The organization~~entity~~ is responsible for compliance with all the reliability standards applicable to the functions for which it is registered from the effective date of~~time it receives~~ the registration ~~notification from NERC~~.

1.3.2 Any organization receiving such a notice may challenge its placement on the NCR according to the process in Appendix 5A *Organization Registration and Organization Certification Manual*, Section V.

1.3.3 The Compliance Committee of the Board of Trustees shall promptly issue a written decision on the challenge, including the reasons for the decision.

1.3.4 The decision of the Compliance Committee of the Board of Trustees shall be final unless, within 21 days of the date of the Compliance Committee of the Board of Trustees decision, the

organization appeals the decision to the applicable governmental authority.

1.3.5 Each entity identified on the NCR shall notify its corresponding Regional Entity(s) of any corrections, revisions, deletions, changes in ownership, corporate structure, or similar matters that affect the entity's responsibilities with respect to the reliability standards. Failure to notify will not relieve the entity from any responsibility to comply with the reliability standards or shield it from any penalties or sanctions associated with failing to comply with the standards applicable to its associated registration.

1.4 For all geographical or electrical areas of the bulk power system, the registration process shall ensure that (1) no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards to the fullest extent practical, and (2) there is no unnecessary duplication of such coverage or of required oversight of such coverage. In particular the process shall:

1.4.1 Ensure that all areas are under the oversight of one and only one Reliability Coordinator.

1.4.2 Ensure that all Balancing Authorities and Transmission Operator entities[2] are under the responsibility of one and only one Reliability Coordinator.

1.4.3 Ensure that all transmission facilities of the bulk power system are the responsibility and under the control of one and only one Transmission Planner, Planning Authority, and Transmission Operator.

1.4.4 Ensure that all loads and generators are under the responsibility and control of one and only one Balancing Authority.

1.5 NERC shall maintain the NCR of organizations responsible for meeting the requirements/sub-requirements of the reliability standards currently in effect on its Web site and shall update the NCR monthly.

2. **Entity Certification** — NERC shall provide for certification of all entities with primary reliability responsibilities requiring certification, including, but not limited to, Reliability Coordinators, Transmission Operators, Balancing Authorities, and those entities that perform some or all of the reliability functions

[2] Some organizations perform the listed functions (e.g., balancing authority, transmission operator) over areas that transcend the footprints of more than one reliability coordinator. Such organizations will have multiple registrations, with each such registration corresponding to that portion of the organization's overall area that is within the footprint of a particular reliability coordinator.

of Reliability Coordinators, Transmission Operators and Balancing Authorities. ~~This includes those entities that satisfy the criteria established in the NERC Provisional Certification Process. The NERC programs~~Certification of entities shall include, but is not limited to, the following:

2.1 Evaluate and certify the competency of entities performing or intending to perform the reliability functions of~~. The entities presently expected to be certified include~~ Reliability Coordinators, Transmission Operators, and Balancing Authorities.

2.2 Evaluate and certify each applicant's ability to meet the requirements for certification.

2.3 Maintain process documentation.

2.4 Maintain records of currently certified entities.

2.5 Issue a certification document to the applicant that successfully demonstrates its competency to perform the evaluated functions.

3. **Delegation and Oversight**

3.1 NERC may delegate responsibilities for Organization Registration and Organization Certification to Regional Entities in accordance with requirements established by NERC. Delegation will be via the delegation agreement between NERC and the Regional Entity or other applicable agreement. The Regional Entity shall administer Organization Registration and Organization Certification Programs in accordance with such delegations to meet NERC's programs goals and requirements subject to NERC oversight.

3.2 NERC shall develop and maintain a plan to ensure the continuity of Organization Registration and Organization Certification within the geographic or electrical boundaries of a Regional Entity in the event that no entity is functioning as a Regional Entity for that region, or the Regional Entity withdraws as a Regional Entity, or does not operate its Organization Registration and Organization Certification Programs in accordance with delegation agreements.

3.3 NERC shall develop and maintain a program to monitor and oversee the NERC Organization Registration and Organization Certification Programs activities that are delegated to each Regional Entity through a delegation agreement or other applicable agreement.

3.3.1 This program shall monitor whether the Regional Entity carries out those delegated activities in accordance with NERC requirements, and whether there is consistency, fairness of administration, and comparability.

3.3.2 Monitoring and oversight shall be accomplished through direct participation in the Organization Registration and Organization Certification Programs with periodic reviews of documents and records of both programs.

502. Organization Registration and Organization Certification Program Requirements

1. NERC shall maintain the Organization Registration and Organization Certification Programs.

   1.1 The roles and authority of Regional Entities in the programs are delegated from NERC pursuant to the Rules of Procedure through regional delegation agreements or other applicable agreements.

   1.2 Processes for the programs shall be administered by NERC and the Regional Entities. Materials that each Regional Entity uses are subject to review and approval by NERC.

   1.3 The appeals process for the Organization Registration and Organization Certification Programs are identified in Appendix 5A *Organization Registration and Organization Certification Manual*, Sections V and VI, respectively.

   1.4 The certification team membership is identified in Appendix 5A *Organization Registration and Organization Certification Manual*, Section IV.8.d.

2. To ensure consistency and fairness of the Organization Registration and Organization Certification Programs, NERC shall develop procedures to be used by all Regional Entities and NERC in accordance with the following criteria:

   2.1 NERC and the Regional Entities shall have data management processes and procedures that provide for confidentiality, integrity, and retention of data and information collected.

   2.2 Documentation used to substantiate the conclusions of the Regional Entity/ NERC related to registration and/or certification must be retained by the Regional Entity for (6) six years, unless a different retention period is otherwise identified, for the purposes of future audits of these programs.

   2.3 To maintain the integrity of the NERC Organization Registration and Organization Certification Programs, NERC, Regional Entities, certification team members, program audit team members (Section 506), and committee members shall maintain the confidentiality of information provided by an applicant or entities.

      2.2.1 NERC and the Regional Entities shall have appropriate codes of conduct and confidentiality agreements for staff, certification team,

certification related committees, and certification program audit team members.

2.2.2 NERC, Regional Entities, certification team members, program audit team members and committee members shall maintain the confidentiality of any registration or certification-related discussions or documents designated as confidential (see Section 1500 for types of confidential information).

2.2.3 NERC, Regional Entities, certification team members, program audit team members and committee members shall treat as confidential the individual comments expressed during evaluations, program audits and report-drafting sessions.

2.2.4 Copies of notes, draft reports, and other interim documents developed or used during an entity certification evaluation or program audit shall be destroyed after the public posting of a final, uncontested report.

2.2.5 Information deemed by an applicant, entity, a Regional Entity, or NERC as confidential, including critical energy infrastructure information, shall not be released publicly or distributed outside of a committee or team.

2.2.6 In the event that an individual violates any of the confidentiality rules set forth above, that individual and any member organization with which the individual is associated will be subject to immediate dismissal from the audit team and may be prohibited from future participation in compliance program activities by the Regional Entity or NERC.

2.2.7 NERC shall develop and provide training in auditing skills to all individuals prior to their participation in certification evaluations. Training for certification team leaders shall be more comprehensive than the training given to industry subject matter experts and Regional Entity members. Training for Regional Entity members may be delegated to the Regional Entity.

2.4 An applicant that is determined to be competent to perform a function after completing all certification requirements shall be deemed certified by NERC to perform that function for which it has demonstrated full competency.

2.4.1 All NERC certified entities shall be included on the NCR.

503. Regional Entity Implementation of Organization Registration and Organization Certification Program Requirements

1. **Delegation** — Recognizing the Regional Entity's knowledge of and experience with their members, NERC may delegate responsibility for Organization Registration and Organization Certification to the Regional Entity through a delegation agreement.

2. **Registration** — The following Organization Registration activities shall be managed by the Regional Entity per the NERC *Organization Registration and Organization Certification Manual*, which is incorporated into the Rules of Procedure as Appendix 5A *Organization Registration and Organization Certification Manual*:

    2.1 Regional entities shall verify that all Reliability Coordinators, Balancing Authorities, and Transmission Operators meet the registration requirements of Section 501(1.4).

3. **Certification —** The following Organization certification activities shall be managed by the Regional Entity in accordance with an approved delegation agreement or another applicable agreement:

    3.1 An entity seeking certification to perform one of the functions requiring certification shall contact the Regional Entity for the region(s) in which it plans to operate to apply for certification.

    3.2 An entity seeking certification and other affected entities shall provide all information and data requested by NERC or the Regional Entity to conduct the certification process.

    3.3 Regional Entities shall notify NERC of all certification applicants.

    3.4 NERC and/or the Regional Entity shall evaluate the competency of entities requiring certification to meet the NERC certification requirements.

    3.5 NERC or the Regional Entity shall establish certification procedures to include evaluation processes, schedules and deadlines, expectations of the applicants and all entities participating in the evaluation and certification processes, and requirements for certification team members.

        3.5.1 The NERC / Regional Entity certification procedures will include provisions for on-site visits to the applicant's facilities to review the data collected through questionnaires, interviewing the operations and management personnel, inspecting the facilities and equipment (including requesting a demonstration of all tools identified in the certification process), reviewing all necessary documents and data (including all agreements, processes, and procedures identified in the certification process), reviewing certification documents and projected system operator work schedules, and reviewing any additional documentation needed to

support the completed questionnaire or inquiries arising during the site visit.

3.5.2 The NERC/ Regional Entity certification procedures will provide for preparation of a written report by the certification team, detailing any deficiencies that must be resolved prior to granting certification, along with any other recommendations for consideration by the applicant, the Regional Entity, or NERC.

504. Appeals

1. NERC shall maintain an appeals process to resolve any disputes related to registration or certification activities per the *Organization Registration and Organization Certification Manual,* which is incorporated in these rules as Appendix 5A.

2. The Regional Entity certification appeals process shall culminate with the regional board or a committee established by and reporting to the regional board as the final adjudicator, provided that where applicable, Canadian provincial governmental authorities may act as the final adjudicator in their jurisdictions. NERC shall be notified of all appeals and may observe any proceedings **(**Appendix 5A *Organization Registration and Organization Certification Manual***)**.

505. Program Maintenance

NERC shall maintain its program materials, including such manuals or other documents as it deems necessary, of the governing policies and procedures of the Organization Registration and Organization Certification Programs.

506. Independent Audit of NERC Organization Registration and Organization Certification Program

1. NERC, through the Compliance and Certification Committee, shall provide for an independent audit of its Organization Registration and Organization Certification Programs at least once every three years, or more frequently, as determined by the Board. The audit shall be conducted by independent expert auditors as selected by the Board.

2. The audit shall evaluate the success, effectiveness and consistency of the NERC Organization Registration and Organization Certification Programs.

3. The final report shall be posted by NERC for public viewing.

4. If the audit report includes recommendations to improve the program, the administrators of the program shall provide a written response to the Board within 30 days of the final report, detailing the disposition of each and every

recommendation, including an explanation of the reasons for rejecting a recommendation and an implementation plan for the recommendations accepted.

507. Provisions Relating to Joint Registration Organizations (JRO)

1. In addition to registering as the entity responsible for all functions that it performs itself, an entity may register as a JRO on behalf of one or more of its members or related entities for one or more functions for which such members or related entities would otherwise be required to register and, thereby, accept on behalf of such members or related entities all compliance responsibility for that function or those functions including all reporting requirements. Any entity seeking to register as a JRO must submit a written agreement with its members or related entities for all requirements/sub-requirements for the function(s) for which the entity is registering for and takes responsibility for, which would otherwise be the responsibility of one or more of its members or related entities. Neither NERC nor the Regional Entity shall be parties to any such agreement, nor shall NERC or the Regional Entity have responsibility for reviewing or approving any such agreement, other than to verify that the agreement provides for an allocation or assignment of responsibilities consistent with the JRO registration.

2. The JRO registration data must include the same registration information as a normal compliance registration entry. The JRO is responsible for providing all of the information and data, including submitting reports, as needed by the Regional Entity for performing assessments of compliance.

3. The Regional Entity shall notify NERC of each JRO that the Regional Entity accepts. The notification will identify the point of contact and the functions(s) being registered for on behalf of its members or related entities.

4. For purposes of compliance audits, the Regional Entity shall keep a list of all JROs. This document shall contain a list of each JRO's members or related entities and the function(s) for which the JRO is registered for that member(s) or related entity(s). It is the responsibility of the JRO to provide the Regional Entity with this information as well as the applicable JRO agreement(s).

5. The Regional Entity may request clarification of any list submitted to it that identifies the members of the JRO and may request such additional information as the Regional Entity deems appropriate.

6. The Regional Entity's acceptance of a JRO shall be a representation by the Regional Entity to NERC that the Regional Entity has concluded the JRO will meet the registration requirements of Section 501(1.4).

7. NERC shall maintain, and post on its Web site, a JRO registry listing all JRO registrations that have been reviewed and accepted by the Regional Entity. The posting shall identify the JRO entity taking compliance responsibilities for itself and its members.

8. The JRO shall inform the Regional Entity of any changes to an existing JRO. The Regional Entity shall promptly notify NERC of each such revision.

9. Nothing in Section 507 shall preclude a member of a JRO, a related entity, or any other entity from registering on its own behalf and undertaking full compliance responsibility including reporting requirements for the reliability standards applicable to the function(s) for which the member or other entity is registering. A JRO member or related entity that registers as responsible for any reliability standard or requirement/sub-requirement of a reliability standard shall inform the JRO of its registration.

508. Provisions Relating to Coordinated Functional Registration (CFR) Entities

1. I n addition to registering as an entity responsible for all functions that it performs itself, multiple entities may each register using a CFR for one or more reliability standard(s) and/or for one or more requirements/sub-requirements within particular reliability standard(s) applicable to a specific function. The CFR submission must include a written agreement that governs itself and clearly specifies the entities' respective compliance responsibilities. The registration of the CFR is the complete registration for each entity. Additionally, each entity shall take full compliance responsibility for those standards and/or requirements/sub-requirements it has registered for in the CFR. Neither NERC nor the Regional Entity shall be parties to any such agreement, nor shall NERC or the Regional Entity have responsibility for reviewing or approving any such agreement, other than to verify that the agreement provides for an allocation or assignment of responsibilities consistent with the CFR.

2. Each CFR or each individual entity within a CFR must identify a point of contact that is responsible for providing information and data, including submitting reports as needed by the Regional Entity related to the CFR registration.

3. The Regional Entity shall notify NERC of each CFR that the Regional Entity accepts.

4. NERC or the Regional Entity may request clarification of any list submitted to it that identifies the compliance responsibilities of the CFR and may request such additional information as NERC or the Regional Entity deems appropriate.

5. The Regional Entity's acceptance of that CFR shall be a representation by the Regional Entity to NERC that the Regional Entity has concluded the CFR will meet the registration requirements of Section 501(1.4).

6. NERC shall maintain, and post on its Web site, a CFR registry listing all CFR registrations that have been accepted by NERC or by a Regional Entity. The posting shall clearly list all the reliability standards or requirements/sub-requirements thereof for which each entity of the CFR is responsible for under the CFR.

7. The point of contact shall inform the Regional Entity of any changes to an existing CFR. The Regional Entity shall promptly notify NERC of each such revision.

8. In the event of a violation of a reliability standard or of a requirement/sub requirement of a reliability standard for which an entity of a CFR is registered, that entity shall be identified in the notice of alleged violation and shall be assessed the sanction or penalty in accordance with the NERC Sanctions Guidelines. In the event a Regional Entity is not able to determine which entity(ies) is responsible for a particular reliability standard, or requirements/sub requirements thereof that has been violated, the Regional Entity shall investigate the noncompliance in accordance with the NERC Rules of Procedure Section 400, *Compliance Enforcement*, to determine the entity(ies) to which the Regional Entity shall to issue the sanction or penalty for the violation.

9. Nothing in Section 508 shall preclude an entity registered in a CFR, or any other entity from registering on its own behalf and undertaking full compliance responsibility including reporting requirements for the reliability standards applicable to the function(s) for which the entity is registering. An entity registered in a CFR that registers as responsible for any reliability standard or requirement/sub requirement of a reliability standard shall inform the point of contact of its registration.

SECTION 600 — PERSONNEL CERTIFICATION

601. Scope of Personnel Certification

Maintaining the reliability of the bulk electric system through implementation of the reliability standards requires skilled, trained and qualified system operators. The ~~System Operator~~Personnel Certification Program provides the mechanism to ensure system operators are provided the education and training necessary to obtain the essential knowledge and skills and are therefore qualified to operate the bulk electric system. The Personnel Certification Program awards system operator certification credentials to individuals who demonstrate they have attained essential knowledge relating to NERC reliability standards as well as principles of bulk power system operations. NERC, as the ERO, will ensure skilled, trained, and qualified system operators through the ~~System Operator~~Personnel Certification Program.

Except as necessary to obtain approval of the Rules of Procedure, the NERC Personnel Certification Governance Committee (PCGC) is the governing body that establishes the policies, sets fees, and monitors the performance of the Personnel Certification Program for system operators.

~~NERC shall develop and maintain a personnel certification program to evaluate individuals and to issue credentials to individuals who demonstrate the required level of competence. A current version of such a program is the *System Operator Certification Program Manual*, which is incorporated into these rules as **Appendix 6**.~~

602. Structure of ERO Personnel Certification Program

1. The NERC personnel certification program shall be international in scope.

2. The personnel certification program shall have a governing body that (1) is able to independently exercise decision-making for all matters pertaining to certification, (2) includes individuals from the discipline being certified and whose composition addresses the needs of the users of the program (e.g., employers, regulators, etc.), and (3) has representation for each specialty or level within a discipline.

3. NERC shall maintain a nominating process for membership in the governing body. Nominations shall be open to all interested parties and self-nominations shall be accepted. The NERC Board of Trustees shall appoint members to the governing body from among those nominated. The members of the governing body shall serve at the pleasure of the board.

4. The personnel certification program governing body shall have control over the matters related to the personnel certification and recertification programs listed below, without being subject to approval by any other body.

    4.1 Policies and procedures, including eligibility requirements and application processing.

4.2 Requirements for personnel certification, maintaining certification, and recertification.

4.3 Examination content, development, and administration.

4.4 Examination cut score.

4.5 Grievance and disciplinary processes.

4.6 Governing body and subgroup(s)' meeting rules including agenda, frequency, and related procedures.

4.7 Subgroup(s) appointments and work assignments.

4.8 Publications about personnel certification and recertification.

4.9 Setting fees for application, and all other services provided as a part of the personnel certification and recertification activities.

4.10 Program funding, spending, and budget authority. Financial matters related to the operation of the program shall be segregated from other NERC activities.

5. The personnel certification program shall utilize written procedures for the selection of members of the governing body that prohibit the governing body from selecting a majority of its successors.

6. The personnel certification program shall be separate from the accreditation and education functions of NERC in related disciplines.

7. No member of the personnel certification program governing body or staff member working with the personnel certification program governing body shall have or exercise any authority or responsibility for compliance matters related to reliability standards concerning personnel certification.

603. Examinations and Maintenance of NERC System Operator Certification Credentials

1. System operators seeking to obtain a credential must pass an examination to earn the credential.

2. A certificate will be issued to successful candidates which is valid for three years.

3. A system operator must earn continuing education (CE) hours in NERC approved learning activities within the three-year period preceding the expiration date of his/her certificate as determined by the PCGC and posted in the NERC System Operator Program Manual. A system operator must request a renewal and submit the appropriate fee for certification renewal evaluation.

4. The credential of a certified system operator who does not accumulate the required number and balance of CE hours within the three-year period will be suspended. A system operator with a suspended certificate cannot perform any task that requires an operator to be NERC-certified. The system operator with a suspended credential will have up to twelve months to acquire the necessary CE hours.

   4.1 During the time of suspension, the original anniversary date will be maintained. Therefore, should the system operator accumulate the required number of CE hours within the twelve month suspension period, he/she will be issued a certificate that will be valid for three years from the previous expiration date.

   4.2 At the end of the twelve-month suspension period, if the system operator has not accumulated the required number of CE hours, the credential will be revoked and all CE hours earned will be forfeited. After a credential is revoked, the system operator will be required to pass an examination to become certified.

5. Hardship: Due to unforeseen events and extenuating circumstances, a certified system operator may be unable to accumulate the necessary CE hours in the time frame required by the Personnel Certification Program to maintain the credential. In such an event, the individual must submit a written request containing a thorough explanation of the circumstances and supporting information to the NERC Personnel Certification Manager. The PCGC retains the right to invoke this Hardship Clause as it deems appropriate to address such events or circumstances.

604. Dispute Resolution Process

1. Any dispute arising under the NERC agreement establishing the *NERC Personnel Certification Program* or from the establishment of any NERC rules, policies, or procedures dealing with any segment of the certification process shall be subject to the NERC System Operator Certification Dispute Resolution Process. The Dispute Resolution Process is for the use of persons who hold an operator certification or persons wishing to be certified to dispute the validity of the examination, the content of the test, the content outlines, or the registration process.

2. Dispute Resolution Process consists of three steps.

   2.1. Notify NERC Personnel Certification Program Staff: This first step can usually resolve the issues without further actions. It is expected that most disputes will be resolved at this step. If the issue(s) is not resolved to the satisfaction of the parties involved in the first step, the issue can be brought to the Personnel Certification Governance Committee (PCGC) Dispute Resolution Task Force.

2.2. PCGC Dispute Resolution Task Force: If the NERC staff did not resolve the issue(s) to the satisfaction of the parties involved, a written request must be submitted to the chairman of the PCGC through NERC staff explaining the issue(s) and requesting further action. Upon receipt of the letter, the PCGC chairman will present the request to the PCGC Dispute Resolution Task Force for action. This task force consists of three current members of the PCGC. The PCGC Dispute Resolution Task Force will investigate and consider the issue(s) presented and make a decision. This decision will then be communicated to the submitting party, the PCGC chairman, and the NERC staff within 45 calendar days of receipt of the request.

3. Personnel Certification Governance Committee: If the PCGC Dispute Resolution Task Force's decision did not resolve the issue(s) to the satisfaction of the parties involved, the final step in the process is for the issue(s) to be brought before the PCGC. Within 45 days of the date of the Task Force's decision, the disputing party shall submit a written request to the PCGC chairman through NERC staff requesting that the issue(s) be brought before the PCGC for resolution. The chairman shall see that the necessary documents and related data are provided to the PCGC members as soon as practicable. The PCGC will then meet or conference to discuss the issue(s) and make their decision within 60 calendar days of the chairman's receipt of the request. The decision will be provided to the person bringing the issue(s) and the NERC staff. The PCGC is the governing body of the certification program and its decision is final.

4. Dispute Resolution Process Expenses: All individual expenses associated with the Dispute Resolution Process, including salaries, meetings, or consultant fees, shall be the responsibility of the individual parties incurring the expense.

5. Decision Process: Robert's Rules of Order shall be used as a standard of conduct for the Dispute Resolution Process. A majority vote of the members present will decide all issues. The vote will be taken in a closed session. No member of the PCGC may participate in the Dispute Resolution Process, other than as a party or witness, if he or she has an interest in the particular matter.

5.1 A stipulation of invoking the Dispute Resolution Process is that the entity invoking the Dispute Resolution Process agrees that neither NERC (its members, Board of Trustees, committees, subcommittees, and staff), any person assisting in the Dispute Resolution Process, nor any company employing a person assisting in the Dispute Resolution Process, shall be liable, and they shall be held harmless against the consequences of or any action or inaction or of any agreement reached in resolution of the dispute or any failure to reach agreement as a result of the Dispute Resolution Process. This "hold harmless" clause does not extend to matters constituting gross negligence, intentional misconduct, or a breach of confidentiality.

605. Disciplinary Action

1. Disciplinary action may be necessary to protect the integrity of the system operator credential. The PCGC may initiate disciplinary action should an individual act in a manner that is inconsistent with expectations, including but not limited to:

   1.1. Willful, gross, and/or repeated violation of the NERC reliability standards as determined by a NERC investigation.

   1.2. Willful, gross, and/or repeated negligence in performing the duties of a certified system operator as determined by a NERC investigation.

   1.3. Intentional misrepresentation of information provided on a NERC application for a system operator certification exam or to maintain a system operator credential using CE hours.

   1.4. Intentional misrepresentation of identification in the exam process, including a person identifying himself or herself as another person to obtain certification for the other person.

   1.5. Any form of cheating during a certification exam, including, but not limited to, bringing unauthorized reference material in the form of notes, crib sheets, or other methods of cheating into the testing center.

   1.6. A certified system operator's admission to or conviction of any felony or misdemeanor directly related to his/her duties as a system operator.

2. Hearing Process: Upon report to NERC of a candidate's or certified system operator's alleged misconduct, the NERC PCGC Credential Review Task Force will convene for the determination of facts. An individual, government agency, or other investigating authority can file a report. Unless the task force initially determines that the report of alleged misconduct is without merit, the candidate or certified system operator will be given the right to notice of the allegation. A hearing will be held and the charged candidate or certified system operator will be given an opportunity to be heard and present further relevant information. The task force may seek out information from other involved parties. The hearing will not be open to the public, but it will be open to the charged candidate or certified system operator and his or her representative. The task force will deliberate in a closed session, but the task force cannot receive any evidence during the closed session that was not developed during the course of the hearing.

3. Task force's decision: The task force's decision will be unanimous and will be in writing with inclusion of the facts and reasons for the decision. The task force's written decision will be delivered to the PCGC and by certified post to the charged candidate or certified system operator. In the event that the task force is

unable to reach a unanimous decision, the matter shall be brought to the full committee for a decision.

3.1. No Action: Allegation of misconduct was determined to be unsubstantiated or inconsequential to the credential.

3.2. Probation: A letter will be sent from NERC to the offender specifying:

3.2.1. The length of time of the probationary period (to be determined by the PCGC).

3.2.2. Credential will remain valid during the probationary period.

3.2.3. The probationary period does not affect the expiration date of the current certificate.

3.2.4. During the probationary period, a subsequent offense of misconduct, as determined through the same process as described above, may be cause for more serious consequences.

3.3. Revoke for Cause: A letter will be sent from NERC to the offender specifying:

3.3.1. The length of time of the probationary period (to be determined by the PCGC).

3.3.2. Credential is no longer valid.

3.3.3. Successfully passing an exam will be required to become recertified.

3.3.4. An exam will not be authorized until the revocation period expires

3.4. Termination of Credential: A letter will be sent from NERC to the offender specifying permanent removal of credential.

4. Credential Review Task Force: The Credential Review Task Force shall be comprised of three active members of the PCGC assigned by the Chairman of the PCGC on an ad hoc basis. No one on the credential review task force may have an interest in the particular matter. The task force will meet in a venue determined by the task force chairman.

5. Appeal Process: The decision of the task force may be appealed using the NERC System Operator Certification Dispute Resolution Process.

~~603.~~606 Candidate Testing Mechanisms

1. The personnel certification program shall utilize reliable testing mechanisms to evaluate individual competence in a manner that is objective, fair to all candidates, job-related, and based on the knowledge and skill needed to function in the discipline.

2. The personnel certification program shall implement a formal policy of periodic review of the testing mechanisms to ensure ongoing relevance of the mechanisms to knowledge and skill needed in the discipline.

3. The personnel certification program shall utilize policies and procedures to ensure that all test administration and development materials are secure and demonstrate that these policies and procedures are consistently implemented.

4. The personnel certification program shall establish pass/fail levels that protect the public with a method that is based on competence and generally accepted in the psychometric community as being fair and reasonable.

5. The personnel certification program shall conduct ongoing studies to substantiate the reliability and validity of the testing mechanisms.

6. The personnel certification program shall utilize policies and procedures that govern how long examination records are kept in their original format.

7. The personnel certification program shall demonstrate that different forms of the testing mechanisms assess equivalent content and that candidates are not penalized for taking forms of varying difficulty.

~~604.~~607. Public Information About the Personnel Certification Program

1. The personnel certification program shall ~~provide for publishing and availability of general descriptive material on~~maintain and publish publicly a System Operator Certification Program Manual describing the procedures used in examination construction and validation; all eligibility requirements and determination; fees; and examination administration documents, including: reporting of results, recertification requirements, and disciplinary and ~~grievance procedures~~dispute resolution.

2. The personnel certification program shall maintain and publish publicly ~~and make available~~ a comprehensive summary or outline of the information, knowledge, or functions covered by each~~the~~ examination.

3. The personnel certification program shall publish publicly and make available at least annually a summary of certification activities for the program, including at least the following information: number of examinations delivered, the number passed, the number failed, and the number certified.

~~605.~~608. Responsibilities to Applicants for Certification or Recertification

The personnel certification program:

1. Shall not discriminate among applicants as to age, gender, race, religion, national origin, disability, or marital status and shall include a statement of non-discrimination in announcements of the program.

2. Shall comply with all requirements of applicable federal and state/provincial laws with respect to all certification and recertification activities, and shall require compliance of all contractors and/or providers of services.

3. Shall make available to all applicants copies of formalized procedures for application for, and attainment of, personnel certification and recertification and shall uniformly follow and enforce such procedures for all applicants.

4. Shall implement a formal policy for the periodic review of eligibility criteria and application procedures to ensure that they are fair and equitable.

5. Shall provide competently proctored examination sites.

6. Shall uniformly report examination results to applicants in a timely manner.

7. Shall give applicants failing the examination information on general content areas of deficiency.

~~8.Shall implement policies and procedures providing due process for applicants questioning eligibility determination, examination results, and certification status, and shall publish this information. A current version of such a procedure is the NERC *System Operator Certification Dispute Resolution Process*, which is incorporated into these rules as part of **Appendix 6**.~~

~~9.Shall develop and maintain a program manual containing the processes and procedures for applicants for certification and recertification.~~

~~606.~~609 Responsibilities to the Public and to Employers of Certified Practitioners

The personnel certification program:

1. Shall demonstrate that the testing mechanisms adequately measure the knowledge and skill required for entry, maintenance, and/or advancement in the profession for each position to be certified.

2. Shall award certification and recertification only after the skill and knowledge of the individual have been evaluated and determined to be acceptable.

3. Shall ~~periodically publish or~~ maintain, in an electronic format, a current list of those persons certified in the programs and have polices and procedures that delineate what information about a credential holder may be made public and under what circumstances.

4. Shall have formal policies and procedures for discipline of a credential holder, including the revocation of the certificate, for conduct deemed harmful to the public or inappropriate to the discipline (e.g., incompetence, unethical behavior, physical or mental impairment affecting performance). These procedures shall incorporate due process. ~~The current procedure is the *NERC Certified System Operator Credential Disciplinary Action Procedure*, which is incorporated into these rules as part of **Appendix 6**.~~

5. Shall demonstrate that any title or credential awarded accurately reflects or applies to the practitioner's daily occupational or professional duties and is not confusing to employers, consumers, regulators, related professions, and/or other interested parties.

SECTION 700 — RELIABILITY READINESS EVALUATION AND IMPROVEMENT AND FORMATION OF SECTOR FORUMS

701. Confidentiality Requirements for Readiness Evaluations and Evaluation Team Members

1. All information made available or created during the course of any reliability readiness evaluation including, but not limited to, data, documents, observations and notes, shall be maintained as confidential by all evaluation team members, in accordance with the requirements of Section 1500.

2. Evaluation team members are obligated to destroy all confidential evaluation notes following the posting of the final report of the reliability readiness evaluation.

3. NERC will retain reliability readiness evaluation-related documentation, notes, and materials for a period of time as defined by NERC.

4. These confidentiality requirements shall survive the termination of the NERC Reliability Readiness Evaluation and Improvement Program.

702. Formation of Sector Forum

1. NERC will form a sector forum at the request of any five members of NERC that share a common interest in the safety and reliability of the bulk power system. The members of sector forum may invite such others of the members of NERC to join the sector forum as the sector forum deems appropriate.

2. The request to form a sector forum must include a proposed charter for the sector forum. The board must approve the charter.

3. NERC will provide notification of the formation of a sector forum to its membership roster. Notices and agendas of meetings shall be posted on NERC's Web site.

4. A sector forum may make recommendations to any of the NERC committees and may submit a standards authorization request to the NERC *Reliability Standards Development Procedure*.

SECTION 800 — RELIABILITY ASSESSMENT AND PERFORMANCE ANALYSIS

801. Objectives of the Reliability Assessment and Performance Analysis Program

The objectives of the NERC reliability assessment and performance analysis program are to: (1) conduct, and report the results of, an independent assessment of the overall reliability and adequacy of the interconnected North American bulk power systems, both as existing and as planned; (2) analyze off-normal events on the bulk power system; (3) identify the root causes of events that may be precursors of potentially more serious events; (4) assess past reliability performance for lessons learned; (5) disseminate findings and lessons learned to the electric industry to improve reliability performance; and (6) develop reliability performance benchmarks. The final reliability assessment reports shall be approved by the board for publication to the electric industry and the general public.

802. Scope of the Reliability Assessment Program

1. The scope of the reliability assessment program shall include:

   1.1 Review, assess, and report on the overall electric generation and transmission reliability (adequacy and operating reliability) of the interconnected bulk power systems, both existing and as planned.

   1.2 Assess and report on the key issues, risks, and uncertainties that affect or have the potential to affect the reliability of existing and future electric supply and transmission.

   1.3 Review, analyze, and report on regional self-assessments of electric supply and bulk power transmission reliability, including reliability issues of specific regional concern.

   1.4 Identify, analyze, and project trends in electric customer demand, supply, and transmission and their impacts on bulk power system reliability.

   1.5 Investigate, assess, and report on the potential impacts of new and evolving electricity market practices, new or proposed regulatory procedures, and new or proposed legislation (e.g. environmental requirements) on the adequacy and operating reliability of the bulk power systems.

2. The reliability assessment program shall be performed in a manner consistent with the reliability standards of NERC including but not limited to those that specify reliability assessment requirements.

803. Reliability Assessment Reports

The number and type of periodic assessments that are to be conducted shall be at the discretion of NERC. The results of the reliability assessments shall be documented in three reports: the long-term and the annual seasonal (summer) and the annual seasonal (winter) assessment reports. NERC shall also conduct special reliability assessments from time to time as circumstances warrant. The reliability assessment reports shall be reviewed and approved for publication by the board. The three regular reports are described below.

1. **Long-Term Reliability Assessment Report** — The annual long-term report shall cover a ten-year planning horizon. The planning horizon of the long-term reliability assessment report shall be subject to change at the discretion of NERC. Detailed generation and transmission adequacy assessments shall be conducted for the first five years of the review period. For the second five years of the review period, the assessment shall focus on the identification, analysis, and projection of trends in peak demand, electric supply, and transmission adequacy, as well as other industry trends and developments that may impact future electric system reliability. Reliability issues of concern and their potential impacts shall be presented along with any mitigation plans or alternatives. The long-term reliability assessment reports will generally be published in the fall (September) of each year. NERC will also publish electricity supply and demand data associated with the long-term reliability assessment report.

2. **Summer Assessment Report** — The annual summer seasonal assessment report typically shall cover the four-month (June–September) summer period. It shall provide an overall perspective on the adequacy of the generation resources and the transmission systems necessary to meet projected summer peak demands. It shall also identify reliability issues of interest and regional and subregional areas of concern in meeting projected customer demands and may include possible mitigation alternatives. The report will generally be published in mid-May for the upcoming summer period.

3. **Winter Assessment Report** — The annual winter seasonal assessment report shall cover the three-month (December–February) winter period. The report shall provide an overall perspective on the adequacy of the generation resources and the transmission systems necessary to meet projected winter peak demands. Similar to the summer assessment, the winter assessment shall identify reliability issues of interest and regional and subregional areas of concern in meeting projected customer demands and may also include possible mitigation alternatives. The winter assessment report will generally be published in mid-November for the upcoming winter period.

4. **Special Reliability Assessment Reports** — In addition to the long-term and seasonal reliability assessment reports, NERC shall also conduct special reliability assessments on a regional, interregional, and interconnection basis as conditions warrant, or as requested by the board or applicable governmental authorities. The teams of reliability and technical experts also may initiate special assessments of

key reliability issues and their impacts on the reliability of a regions, subregions, or interconnection (or a portion thereof). Such special reliability assessments may include, among other things, operational reliability assessments, evaluations of emergency response preparedness, adequacy of fuel supply, hydro conditions, reliability impacts of new or proposed environmental rules and regulations, and reliability impacts of new or proposed legislation that affects or has the potential to affect the reliability of the interconnected bulk power systems in North America.

804. Reliability Assessment Data and Information Requirements

To carry out the reviews and assessments of the overall reliability of the interconnected bulk power systems, the regional entities and other entities shall provide sufficient data and other information requested by NERC in support of the annual long-term and seasonal assessments and any special reliability assessments.

Some of the data provided for these reviews and assessment may be considered confidential from a competitive marketing perspective, a critical energy infrastructure information perspective, or for other purposes. Such data shall be treated in accordance with the provisions of Section 1500 – Confidential Information.

While the major sources of data and information for this program are the regional entities, a team of reliability and technical experts is responsible for developing and formulating its own independent conclusions about the near-term and long-term reliability of the bulk power systems.

In connection with the reliability assessment reports, requests shall be submitted to each of the regional entities for required reliability assessment data and other information, and for each region's self-assessment report. The timing of the requests will be governed by the schedule for the preparation of the assessment reports.

The regional self-assessments are to be conducted in compliance with NERC standards and the respective regional planning criteria. The team(s) of reliability and technical experts shall also conduct interviews with the regional entities as needed. The summary of the regional self-assessments that are to be included in the assessment reports shall follow the general outline identified in NERC's request. This outline may change from time to time as key reliability issues change.

In general, the regional reliability self-assessments shall address, among other areas, the following topics: demand and net energy for load; assessment of projected resource adequacy; any transmission constraints that may impact bulk transmission adequacy and plans to alleviate those constraints; any unusual operating conditions that could impact reliability for the assessment period; fuel supply adequacy; the deliverability of generation (both internal and external) to load; and any other reliability issues in the region and their potential impacts on the reliability of the bulk power systems.

805. Reliability Assessment Process

Based on their expertise, the review of the collected data, the review of the regional self-assessment reports, and interviews with the regional entities, as appropriate, the teams of reliability and technical experts shall perform an independent review and assessment of the generation and transmission adequacy of each region's existing and planned bulk power system. The results of the review teams shall form the basis of NERC's long-term and seasonal reliability assessment reports. The review and assessment process is briefly summarized below.

1. **Resource Adequacy Assessment** — The teams shall evaluate the regional demand and resource capacity data for completeness in the context of the overall resource capacity needs of the region. The team shall independently evaluate the ability of the regional entity members to serve their obligations given the demand growth projections, the amount of existing and planned capacity, including committed and uncommitted capacity, contracted capacity, or capacity outside of the region. If the region relies on capacity from outside of the region to meet its resource objectives, the ability to deliver that capacity shall be factored into the assessment. The demand and resource capacity information shall be compared to the resource adequacy requirements of the regional entity for the year(s) or season(s) being assessed. The assessment shall determine if the resource information submitted represents a reasonable and attainable plan for the regional entity and its members. For cases of inadequate capacity or reserve margin, the regional entity will be requested to analyze and explain any resource capacity inadequacies and its plans to mitigate the reliability impact of the potential inadequacies. The analysis may be expanded to include surrounding areas. If the expanded analysis indicates further inadequacies, then an interregional problem may exist and will be explored with the applicable regions. The results of these analyses shall be described in the assessment report.

2. **Transmission Adequacy and Operating Reliability Assessment** — The teams shall evaluate transmission system information that relates to the adequacy and operating reliability of the regional transmission system. That information shall include: regional planning study reports, interregional planning study reports, and/or regional operational study reports. If additional information is required, another data request shall be sent to the regional entity. The assessment shall provide a judgment on the ability of the regional transmission system to operate reliably under the expected range of operating conditions over the assessment period as required by NERC reliability standards. If sub-areas of the regional system are especially critical to the reliable operation of the regional bulk transmission system, these facilities or sub-areas shall be reviewed and addressed in the assessment. Any areas of concern related to the adequacy or operating reliability of the system shall be identified and reported in the assessment.

3. **Seasonal Operating Reliability Assessment** — The team(s) shall evaluate the overall operating reliability of the regional bulk transmission systems. In areas with potential resource adequacy or system operating reliability problems, operational readiness of the affected regional entities for the upcoming season

shall be reviewed and analyzed. The assessment may consider unusual but possible operating scenarios and how the system is expected to perform. Operating reliability shall take into account a wide range of activities, all of which should reinforce the regional entity's ability to deal with the situations that might occur during the upcoming season. Typical activities in the assessment may include: facility modifications and additions, new or modified operating procedures, emergency procedures enhancement, and planning and operating studies. The teams shall report the overall seasonal operating reliability of the regional transmission systems in the annual summer and winter assessment reports.

4. **Reporting of Reliability Assessment Results** — The teams of reliability and technical experts shall provide an independent assessment of the reliability of the regional entities and the North American interconnected bulk power system for the period of the assessment. While the regional entities are relied upon to provide the information to perform such assessments, the review team is not required to accept the conclusions provided by the regional entities. Instead, the review team is expected, based on their expertise, to reach their own independent conclusions about the status of the adequacy of the generation and bulk power transmission systems of North America.

   The review team also shall strive to achieve consensus in their assessments. The assessments that are made are based on the best information available at the time. However, since judgment is applied to this information, legitimate differences of opinion can develop. Despite these differences, the review team shall work to achieve consensus on their findings.

   In addition to providing long-term and seasonal assessments in connection with the reliability assessment program, the review team of experts shall also be responsible for recommending new and revised reliability standards related to the reliability assessments and the reliability of the bulk power systems. These proposals for new or revised standards shall be entered into NERC's Standards Development Process.

   Upon completion of the assessment, the team shall share the results with the regional entities. The regional entities shall be given the opportunity to review and comment on the conclusions in the assessment and to provide additional information as appropriate. The reliability assessments and their conclusions are the responsibility of NERC's technical review team and NERC.

   The preparation and approval of NERC's reliability assessment reports shall follow a prescribed schedule including review, comment, and possible approval by appropriate NERC committees. The long-term and seasonal (summer and winter) reliability assessment reports shall be further reviewed for approval by the board for publication to the electric industry.

806. Scope of the Reliability Performance and Analysis Program

The components of the program will include analysis of large-scale outages, disturbances, and near misses to determine root causes and lessons learned; identification and continuous monitoring of performance indices to detect emerging trends and signs of a decline in reliability performance; and communications of performance results, trends, recommendations, and initiatives to those responsible to take actions; followed with confirmation of actions to correct any deficiencies identified. Within NERC, the reliability performance program will provide performance results to the standards development and compliance enforcement programs to make the necessary adjustments to preserve reliability based on a risk-based approach.

807. Analysis of Major Events

Responding to major events affecting the bulk power system such as significant losses of load or generation, ~~blackouts and others~~significant bulk power system disturbances, or other emergencies on the bulk power system, can be divided into four phases: situation~~al~~ assessment and communications; situation tracking and communications; data collection, investigation, analysis, and reporting; and follow-up on recommendations.

a. NERC's role following a major event~~blackout or other major bulk power system disturbance or emergency~~ is to provide leadership, coordination, technical expertise, and assistance to the industry in responding to the major event. Working closely with the regional entities and reliability coordinators, and other appropriate registered entities, NERC will coordinate and facilitate efforts among industry participants, and with state, federal, and provincial governments in the United States and Canada to support the industry's response.

b. When responding to any major event where physical or cyber security is suspected as a cause or contributing factor to ~~an~~the major event, NERC will immediately notify appropriate government agencies and coordinate its activities with them.

c. NERC Reliability Standard EOP-004 sets forth specific criteria and procedures for reporting the bulk power system disturbances and events described in that reliability standard. All registered entities that are subject to the requirements of NERC Reliability Standard EOP-004 must report the information required by that reliability standard within the time periods specified. Each user, owner, and operator of the bulk power system shall also provide NERC and the applicable regional entities with such additional information requested by NERC or the applicable regional entity as is necessary to enable NERC and the applicable regional entities to carry out their responsibilities under this section.

d. During the conduct of ~~some~~ NERC analyses, assistance may be needed from government agencies. This assistance could include: authority to require data reporting from affected or involved parties; communications with other agencies of government; investigations related to possible criminal or terrorist involvement in the major event; resources for initial data gathering immediately after the major

event; authority to call meetings of affected or involved parties; and technical and analytical resources for studies.

e. NERC shall work with all other participants to establish a clear delineation of roles, responsibilities, and coordination requirements among industry and government for the investigation and reporting of findings, conclusions, and recommendations related to major events ~~blackouts~~, ~~disturbances, or other emergencies affecting the bulk power system~~ with the objective of avoiding, to the extent possible, multiple investigations of the same major event. If the major event is confined to a single regional entity, NERC representatives will participate as members of the regional entity analysis team. NERC will establish, maintain, and revise from time to time as appropriate based on experience, a manual setting forth procedures and protocols for communications and sharing and exchange of information between and among NERC, the affected regional entity or entities. and relevant governmental authorities, industry organizations and bulk power system users, owners, and operators concerning the investigation and analysis of major events.

f. NERC and applicable entity(s) ~~shall~~will apply, as appropriate to the circumstances of the major event, the NERC ~~*Blackout and Disturbance*~~ *Event Response Procedures*, which are incorporated into these rules as **Appendix 8**. These procedures provide a framework to guide NERC's response to major events that may have multiregional, national, or international implications. Experienced industry leadership shall be applied to tailor the response to the specific circumstances of the major event. In accordance with ~~that~~those procedures, the NERC president will determine whether the major event warrants analysis at the ~~NERC level~~NERC level. A regional entity may request that NERC elevate any analysis of a major event to ~~a~~the NERC level.

g. NERC will screen and analyze the findings and recommendations from the analysis, and those with generic applicability will be disseminated to the industry through various means appropriate to the circumstances, including in accordance with section 810.

808. Analysis of Off-Normal Occurrences~~Events~~, ~~Potential~~Bulk Power System Performance~~Vulnerabilities~~, and Bulk Power System ~~Performance~~Vulnerabilities

1. NERC and regional entities ~~shall~~will analyze bulk power system and equipment performance occurrences~~events~~ that do not rise to the level of a major event~~blackout, disturbance, or system emergency~~, as described in section 807. NERC and regional entities ~~shall~~will also analyze potential vulnerabilities in the bulk power system that they discover or that are brought to their attention by other sources including government agencies. The purpose of these analyses is to identify the root causes of ~~events~~occurrences or conditions that may be precursors of major events or other potentially more serious ~~events~~occurrences, or that have the potential to cause major events or other more serious occurrences~~events~~, to

assess past reliability performance for lessons learned, and to develop reliability performance benchmarks and trends.

2. NERC and regional entities will screen and analyze off-normal occurrences, bulk power system performance,~~events~~ and potential bulk power system vulnerabilities for significance, and information from those indicated as having~~with~~ generic applicability will be disseminated to the industry through various means appropriate to the circumstances, including in accordance with section 810.

3. NERC Reliability Standard EOP-004 sets forth specific criteria and procedures for reporting the bulk power system disturbances and events described in that reliability standard. All registered entities that are subject to the requirements of NERC Reliability Standard EOP-004 must report the information required by that reliability standard within the time periods specified. Each user, owner, and operator, of the bulk power system shall provide NERC and the applicable regional entities with such additional information requested by NERC or the applicable regional entities as is necessary to enable NERC and the applicable regional entities to carry out their responsibilities under this section.

809. Reliability Benchmarking

NERC shall identify and track key reliability indicators as a means of benchmarking reliability performance and measuring reliability improvements. This program will include assessing available metrics, developing guidelines for acceptable metrics, maintaining a performance metrics "dashboard" on the NERC Web site, and developing appropriate reliability performance benchmarks.

810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions

1 Members of NERC and bulk power system owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.

2. In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and other information will be used to guide the reliability assessment program.

3. When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:

3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the bulk power system of findings and lessons learned;

3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the bulk power system according to each entity's facts and circumstances;

3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system to take to ensure the reliability of the bulk power system. Such Essential Actions require NERC board approval before issuance.

4. The bulk power system owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such bulk power system owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.

5. NERC will advise the Commission and other applicable governmental authorities of its intent to issue all Level 1 Advisories, Level 2 Recommendations, and Level 3 Essential Actions at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other applicable governmental authorities no later than thirty (30) days following the date by which NERC has requested the bulk power system owners, operators, and users to which a Level 2 Recommendation or Level 3 Essential Action issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other applicable governmental authorities will describe the actions taken by the relevant owners, operators, and users of the bulk power system and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for confidential or critical infrastructure information.

811. Equipment Performance Data

Through its Generating Availability Data System (GADS), NERC shall collect operating information about the performance of electric generating equipment; provide assistance to those researching information on power plant outages stored in its database; and support equipment reliability as well as availability analyses and other decision-making processes developed by GADS subscribers. GADS data is also used in conducting assessments of generation resource adequacy.

SECTION 900 — TRAINING AND EDUCATION

901. Scope of the Training and Education Program

Maintaining the reliability of the bulk electric system through implementation of the Reliability Standards requires informed and trained personnel. The training and education program will provide the education and training necessary for bulk power system personnel and regulators to obtain the essential knowledge necessary to understand and operate the bulk electric system.

NERC shall develop and maintain training and education programs for the purpose of establishing training requirements, developing materials, and developing training activities. The target audience of the training and education programs shall be bulk power system operating personnel including system operations personnel, operations support personnel (engineering and information technology), supervisors and managers, training personnel, and other personnel directly responsible for complying with NERC reliability standards who, through their actions or inactions, may impact the real-time, or day-ahead reliability of the bulk power system.

NERC shall also develop and provide appropriate training and education for industry participants and regulators affected by new or changed reliability standards or compliance requirements.

To accomplish those objectives:

1. NERC shall periodically conduct job task analyses for targeted bulk power system personnel to ensure that the training program content is properly aligned to the job tasks performed by those personnel.

2. NERC shall develop and maintain personnel training program curriculum requirements based on valid job-task analysis.

3. NERC shall periodically conduct performance surveys to determine the effectiveness of the training program and identify areas for further training development and improvement.

4. NERC shall develop training and education materials and activities to assist bulk power system entities implementing new or revised reliability standard requirements or other NERC-related changes.

5. NERC shall develop and provide training to people who participate in NERC and regional entity evaluations, audits, and investigations for the compliance enforcement program, organization certification program, and the continuing education program.

902. Continuing Education Program

NERC shall develop and maintain a continuing education program to foster the improvement of training and to promote quality in the training programs used by and

implemented by bulk power system entities. The program shall approve or accredit those activities and entities meeting NERC continuing education requirements.

1. NERC shall develop and implement continuing education program requirements that promote excellence in training programs and advance improved performance for bulk system personnel identified in Section 901.

2. NERC shall develop and maintain a process to approve or accredit continuing education providers and activities seeking approval or accreditation and meeting NERC-approved continuing education requirements.

3. NERC shall perform periodic audits on continuing educaiton providers and training activities to ensure that the approved or accredited providers and training activities satisfy NERC continuing education requirements.

4. NERC shall develop and maintain an appeals process for disputed application reviews, interpretations of guidelines and standards, probation or suspension of NERC-approved provider status, or continuing education hour disputes.

SECTION 1000 — SITUATION AWARENESS AND INFRASTRUCTURE SECURITY

1001. Situation Awareness

NERC shall through the use of reliability coordinators and available tools, monitor present conditions on the bulk power system and provide leadership coordination, technical expertise, and assistance to the industry in responding to events as necessary. To accomplish these goals, NERC will:

1. Maintain real-time situation awareness of conditions on the bulk power system;

2. Notify the industry of significant bulk power system events that have occurred in one area, and which have the potential to impact reliability in other areas;

3. Maintain and strengthen high-level communication, coordination, and cooperation with governments and government agencies regarding real-time conditions; and

4. Enable the reliable operation of interconnected bulk power systems by facilitating information exchange and coordination among reliability service organizations.

1002. Reliability Support Services

NERC ~~will provide~~may assist in the development of tools and other support services for the benefit of reliability coordinators and other system operators to enhance reliability, operations and planning. NERC will work with the industry to identify new tools, collaboratively develop requirements, support development, provide an incubation period, and at the end of that period, transition the tool or service to another group or owner for long term operation of the tool or provision of the service~~, including the Area Control Error (ACE) and Frequency Monitoring System, NERC Hotline, Real-time Flows, System Data Exchange (SDX), Reliability Coordinator Information System (RCIS), Transmission Services Information Network (TSIN), Interchange Distribution Calculator (IDC), Interregional Security Network (ISN), and Central Repository for Security Events (CRC)~~. To accomplish this goal, NERC will:

1. ~~Maintain~~Collaborate with industry to determine the ~~reliability and effectiveness~~necessity of ~~all mission-critical operating reliability support systems and~~new tools or services to enhance reliability;

2. For those tools that the collaborative process determines should proceed to a development phase, provide a start-up mechanism and development system~~Continue to support maintenance of a transmission provider curtailment report on the CRC site in response to Federal Energy Regulatory Commission Order 605~~;

3. Implement the tool either on its own or through an appropriate group or organization~~Investigate and analyze the use of high-speed real-time system measurements, including phasors, in predicting the behavior and performance of the Eastern Interconnection~~; and

4. Where NERC conducts the implementation phase of a new tool or service, develop a transition plan to turn maintenance and provision of the tool or service over to an organization identified in the development stage~~Facilitate real-time voice and data exchange services among reliability coordinators (e.g., Hotline, Interregional Security Network, NERCnet, System Data Exchange, etc.)~~.

In addition to tools developed as a result of a collaborative process with industry, NERC may develop reliability tools on its own, but will consult with industry concerning the need for the tool prior to proceeding to development.

Tools and services being maintained by NERC as of January 1, 2012, will be reviewed and, as warranted, transitioned to an appropriate industry group or organization. NERC will develop and maintain a strategic reliability tools plan that will list the tools and services being maintained by NERC, and, where applicable, the plans for transition to an appropriate industry group or organization.

1003. Infrastructure Security Program

NERC shall coordinate electric industry activities to promote critical infrastructure protection of the bulk power system in North America by taking a leadership role in critical infrastructure protection of the electricity sector so as to reduce vulnerability and improve mitigation and protection of the electricity sector's critical infrastructure. To accomplish these goals, NERC shall perform the following functions.

1. Electric Sector Information Sharing and Analysis Center (ESISAC)

   1.1 NERC shall serve as the electricity sector's Sector Coordinator and operate its Information Sharing and Analysis Center to gather information and communicate security-related threats and incidents within the sector, with United States and Canadian government agencies, and with other critical infrastructure sectors.

   1.2 NERC shall improve the capability of the ESISAC to analyze security threats and incident information and provide situational assessments for the electricity sector and governments.

   1.3 NERC shall work closely with the United States Department of Homeland Security, Department of Energy, Natural Resources Canada, and Public Safety and Emergency Preparedness Canada.

   1.4 NERC shall strengthen and expand these functions and working relationships with the electricity sector, other critical infrastructure industries, governments, and government agencies throughout North America to ensure the protection of the infrastructure of the bulk power system.

   1.5 NERC shall fill the role of the Electricity Sector Coordinating Council and coordinate with the Government Coordinating Council.

1.6 NERC shall coordinate with other critical infrastructure sectors through active participation with the other Sector Coordinating Councils, the other ISACs, and the National Infrastructure Advisory Committee.

1.7 NERC shall encourage and participate in coordinated critical infrastructure protection exercises, including interdependencies with other critical infrastructure sectors.

2. Security Planning

2.1 NERC shall take a risk management approach to critical infrastructure protection, considering probability and severity, and recognizing that mitigation and recovery can be practical alternatives to prevention.

2.2 NERC shall keep abreast of the changing threat environment through collaboration with government agencies.

2.3 NERC shall develop criteria to identify critical physical and cyber assets, assess security threats, identify risk assessment methodologies, and assess effectiveness of physical and cyber protection measures.

2.4 NERC shall enhance and maintain the bulk power system critical spare transformer program, encourage increased participation by asset owners, and continue to assess the need to expand this program to include other critical bulk power system equipment.

2.5 NERC shall support implementation of the Cyber Security Standards through education and outreach.

2.6 NERC shall review and improve existing Security Guidelines, develop new Security Guidelines to meet the needs of the electricity sector, and consider whether any guidelines should be developed into standards.

2.7 NERC shall conduct education and outreach initiatives to increase awareness and respond to the needs of the electricity sector.

2.8 NERC shall strengthen relationships with federal, state, and provincial government agencies on critical infrastructure protection matters.

2.9 NERC shall maintain and improve mechanisms for the sharing of sensitive or classified information with federal, state, and provincial government agencies on critical infrastructure protection matters; work with DOE and DHS to implement the National Infrastructure Protection Plan, as applicable to the electricity sector; and coordinate this work with PSEPC.

2.10 NERC shall improve methods to better assess the impact of a possible physical attack on the bulk power system and means to deter, mitigate, and respond following an attack.

2.11 NERC shall assess the results of vulnerability assessments and enhance the security of System Control and Data Acquisition (SCADA) and process control systems by developing methods to detect an emerging cyber attack and the means to mitigate impacts on the bulk power systems.

2.12 NERC shall work with the National SCADA Test Bed and the Process Control Systems Forum to accelerate the development of technology that will enhance the security, safety, and reliability of process control and SCADA systems.

SECTION 1100 — ANNUAL NERC BUSINESS PLANS AND BUDGETS

1101. Scope of Business Plans and Budgets

The board shall determine the content of the budgets to be submitted to the applicable ERO governmental authorities with consultation from the members of the Members Representatives Committee, regional entities, and others in accordance with the bylaws. The board shall identify any activities outside the scope of NERC's statutory reliability functions, if any, and the appropriate funding mechanisms for those activities.

1102. NERC Funding and Cost Allocation

1. In order that NERC's costs shall be fairly allocated among interconnections and among regional entities, the NERC funding mechanism for all statutory functions shall be based on net energy for load (NEL).

2. NERC's costs shall be allocated so that all load (or, in the case of costs for an interconnection or regional entity, all load within that interconnection or regional entity) bears an equitable share of such costs based on NEL.

3. Costs shall be equitably allocated between countries or regional entities thereof for which NERC has been designated or recognized as the electric reliability authority.

4. Costs incurred to accomplish the statutory functions for one interconnection, regional entity, or group of entities will be directly assigned to that interconnection, regional entity, or group of entities provided that such costs are allocated equitably to end-users based on net energy for load.

1103. NERC Budget Development

1. The NERC annual budget process shall be scheduled and conducted for each calendar year so as to allow a sufficient amount of time for NERC to receive member inputs, develop the budget, and receive board and, where authorized by applicable legislation or agreement, ERO governmental authority approval of the NERC budget for the following fiscal year, including timely submission of the proposed budget to FERC for approval in accordance with FERC regulations.

2. The NERC budget submittal to ERO governmental authorities shall include provisions for all ERO functions, all regional entity delegated functions as specified in delegation agreements and reasonable reserves and contingencies.

3. The NERC annual budget submittal to ERO governmental authorities shall include description and explanation of NERC's proposed ERO program activities for the year; budget component justification based on statutory or other authorities; explanation of how each budgeted activity lends itself to the accomplishment of the statutory or other authorities; sufficiency of resources

provided for in the budget to carry out the ERO program responsibilities; explanation of the calculations and budget estimates; identification and explanation of changes in budget components from the previous year's budget; information on staffing and organization charts; and such other information as is required by FERC and other ERO governmental authorities having authority to approve the proposed budget.

4. NERC shall develop, in consultation with the regional entities, a reasonable and consistent system of accounts, to allow a meaningful comparison of actual results at the NERC and regional entity level by the applicable ERO governmental authorities.

1104. Submittal of Regional Entity Budgets to NERC

1. Each regional entity shall submit its proposed annual budget for carrying out its delegated authority functions as well as all other activities and funding to NERC in accordance with a schedule developed by NERC and the regional entities, which shall provide for the regional entity to submit its final budget that has been approved by its board of directors or other governing body no later than July 1 of the prior year, in order to provide sufficient time for NERC's review and comment on the proposed budget and approval of the regional entity budget by the NERC Board of Trustees in time for the NERC and regional budgets to be submitted to FERC and other ERO governmental authorities for approval in accordance with their regulations. The regional entity's budget shall include supporting materials in accordance with the budget and reporting format developed by NERC and the regional entities, including the regional entity's complete business plan and organization chart, explaining the proposed collection of all dues, fees, and charges and the proposed expenditure of funds collected in sufficient detail to justify the requested funding collection and budget expenditures.

2. NERC shall review and approve each regional entity's budget for meeting the requirements of its delegated authority. Concurrent with approving the NERC budget, NERC shall review and approve, or reject, each regional entity budget for filing.

3. NERC shall also have the right to review from time to time, in reasonable intervals but no less frequently than every three years, the financial books and records of each regional entity having delegated authority in order to ensure that the documentation fairly represents in all material respects appropriate funding or delegated functions.

1105. Submittal of NERC and Regional Entity Budgets to Governmental Authorities for Approval

1. NERC shall file for approval by the applicable ERO governmental authorities at least 130 days in advance of the start of each fiscal year. The filing shall include: (1) the complete NERC and regional entity budgets including the business plans and organizational charts approved by the board, (2) NERC's annual funding requirement (including regional entity costs for delegated functions), and (3) the

mechanism for assessing charges to recover that annual funding requirement, together with supporting materials in sufficient detail to support the requested funding requirement.

2. NERC shall seek approval from each governmental authority requiring such approval for the funding requirements necessary to perform ERO activities within their jurisdictions.

1106. NERC and Regional Entity Billing and Collections

1. NERC shall request the regional entities to identify all load-serving entities[3] within each regional entity and the NEL assigned to each load-serving entity, and the regional entities shall supply the requested information. The assignment of a funding requirement to an entity shall not be the basis for determining that the entity must be registered in the compliance registry.

2. NERC shall accumulate the NEL by load-serving entities for each ERO governmental authority and submit the proportional share of NERC funding requirements to each ERO governmental authority for approval together with supporting materials in sufficient detail to support the requested funding requirement.

3. NEL reported by balancing authorities within a region shall be used to rationalize and validate amounts allocated for collection through regional entity processes.

4. The billing and collection processes shall provide:

   4.1 A clear validation of billing and application of payments.

   4.2 A minimum of data requests to those being billed.

   4.3 Adequate controls to ensure integrity in the billing determinants including identification of entities responsible for funding NERC's activities.

   4.4 Consistent billing and collection terms.

5. NERC will bill and collect all budget requirements approved by applicable ERO governmental authorities (including the funds required to support those functions assigned to the regional entities through the delegation agreements) directly from the load-serving entities or their designees or as directed by particular ERO governmental authorities, except where the regional entity is required to collect the budget requirements for NERC, in which case the regional entity will collect directly from the load-serving entities or as otherwise provided by agreement and

[3] A regional entity may allocate funding obligations using an alternative method approved by NERC and by FERC and other appropriate ERO governmental authorities, as provided for in the regional delegation agreement.

submit funds to NERC. Alternatively, a load-serving entity may pay its allocated ERO costs through a regional entity managed collection mechanism.

6. NERC shall set a minimum threshold limit on the billing of small LSEs to minimize the administrative burden of collection.

7. NERC shall pursue any non-payments and shall request assistance from applicable governmental authorities as necessary to secure collection.

8. In the case where a Regional Entity performs the collection for ERO, the Regional Entity will not be responsible for non-payment in the event that a user, owner or operator of the Bulk Power System does not pay its share of dues, fees and charges in a timely manner, provided that such a Regional Entity shall use reasonably diligent efforts to collect dues, fees, and other charges from all entities obligated to pay them. However, any revenues not paid shall be recovered from others within the same region to avoid cross-subsidization between regions.

9. Both NERC and the regional entities also may bill members or others for functions and services not within statutory requirements or otherwise authorized by the appropriate governmental authorities. Costs and revenues associated with these functions and services shall be separately identified and not commingled with billings associated with the funding of NERC or of the regional entities for delegated activities.

1107. Penalty Applications

1. Where NERC or a regional entity initiates a compliance monitoring and enforcement process that leads to imposition of a penalty, the entity that initiated the process shall receive any penalty monies imposed and collected as a result of that process, unless a different disposition of the penalty monies is provided for in the delegation agreement, or in a contract or a disposition of the violation that is approved by NERC and FERC.

2. All funds from financial penalties assessed in the United States received by the entity initiating the compliance monitoring and enforcement process shall be applied as a general offset to the entity's budget requirements for the subsequent fiscal year, if received by July 1, or for the second subsequent fiscal year, if received on or after July 1. Funds from financial penalties shall not be directly applied to any program maintained by the entity conducting the compliance monitoring and enforcement process. Funds from financial penalties assessed against a Canadian entity shall be applied as specified by legislation or agreement.

3. In the event that a compliance monitoring and enforcement process is conducted jointly by NERC and a regional entity, the regional entity shall receive the penalty monies and offset the entity's budget requirements for the subsequent fiscal year.

4. Exceptions or alternatives to the foregoing provisions will be allowed if approved by NERC and by FERC any other applicable ERO governmental authority.

1108. Special Assessments

On a demonstration of unforeseen and extraordinary circumstances requiring additional funds prior to the next funding cycle, NERC shall file with the applicable ERO governmental authorities, where authorized by applicable legislation or agreement, for authorization for an amended or supplemental budget for NERC or a regional entity and, if necessary under the amended or supplemental budget, to collect a special or additional assessment for statutory functions of NERC or the regional entity. Such filing shall include supporting materials to justify the requested funding, including any departure from the approved funding formula or method.

SECTION 1200 — REGIONAL DELEGATION AGREEMENTS

1201. Pro Forma Regional Delegation Agreement

NERC shall develop and maintain a pro forma regional entity delegation agreement, which shall serve as the basis for negotiation of consistent agreements for the delegation of ERO functions to regional entities.

1202. Regional Entity Essential Requirements

NERC shall establish the essential requirements for an entity to become qualified and maintain good standing as a regional entity.

1203. Negotiation of Regional Delegation Agreements

NERC shall, for all areas of North America that have provided NERC with the appropriate authority, negotiate regional delegation agreements for the purpose of ensuring all areas of the North American bulk power systems are within a regional entity area. In the event NERC is unable to reach agreement with regional entities for all areas, NERC shall provide alternative means and resources for implementing NERC functions within those areas. No delegation agreement shall take effect until it has been approved by the appropriate ERO governmental authority.

1204. Conformance to Rules and Terms of Regional Delegation Agreements

NERC and each regional entity shall comply with all applicable ERO rules of procedure and the obligations stated in the regional delegation agreement.

1205. Sub-delegation

The regional entity shall not sub-delegate any responsibilities and authorities delegated to it by its regional delegation agreement with NERC except with the approval of NERC and FERC and other appropriate ERO governmental authorities. Responsibilities and authorities may only be sub-delegated to another regional entity. Regional entities may share resources with one another so long as such arrangements do not result in cross-subsidization or in any sub-delegation of authorities.

1206. Nonconformance to Rules or Terms of Regional Delegation Agreement

If a regional entity is unable to comply or is not in compliance with an ERO rule of procedure or the terms of the regional delegation agreement, the regional entity shall immediately notify NERC in writing, describing the area of nonconformance and the reason for not being able to conform to the rule. NERC shall evaluate each case and inform the affected regional entity of the results of the evaluation. If NERC determines that a rule or term of the regional delegation agreement has been violated by an entity or cannot practically be implemented by an entity, NERC shall notify the applicable ERO governmental authorities and take any actions necessary to address the situation.

1207. Regional Entity Audits

Approximately every five years and more frequently if necessary for cause, NERC shall audit each regional entity to verify that the regional entity continues to comply with NERC rules of procedure and the obligations of NERC delegation agreement. Audits of regional entities shall be conducted, to the extent practical, based on professional auditing standards recognized in the U.S., including Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards, and standards sanctioned by the Institute of Internal Auditors, and if applicable to the coverage of the audit, may be based on Canadian or other international standards. The audits required by this section 1207 shall not duplicate the audits of regional entity compliance monitoring and enforcement programs provided for in **Appendix 4A**, Audit of Regional Compliance Programs, to these rules of procedure.

1208. Process for Considering Registered Entity Requests to Transfer to Another Regional Entity ~~Audits~~

1. A registered entity that is registered in the region of one regional entity and believes its registration should be transferred to a different regional entity may submit a written request to both regional entities requesting that they process the proposed transfer in accordance with this section. The registered entity's written request shall set forth the reasons the registered entity believes justify the proposed transfer and shall describe any impacts of the proposed transfer on other bulk power system owners, operators, and users.

2. After receiving the registered entity's written request, the two regional entities shall consult with each other as to whether they agree or disagree that the requested transfer is appropriate. The regional entities may also consult with affected reliability coordinators, balancing authorities and transmission operators as appropriate. Each regional entity shall post the request on its web site for public comment period of 21 days. In evaluating the proposed transfer, the regional entities shall consider the location of the registered entity's bulk power system facilities in relation to the geographic and electrical boundaries of the respective regions; the impacts of the proposed transfer on other bulk power system owners, operators; and users, the impacts of the proposed transfer on the current and future staffing, resources, budgets and assessments to other load-serving entities of each regional entity, including the sufficiency of the proposed transferee regional entity's staffing and resources to perform compliance monitoring and enforcement activities with respect to the registered entity; the registered entity's compliance history with its current regional entity; and the manner in which pending compliance monitoring and enforcement matters concerning the registered entity would be transitioned from the current regional entity to the transferee regional entity; along with any other reasons for the proposed transfer stated by the registered entity and any other reasons either regional entity considers relevant. The regional entities may request that the registered entity provide additional data and information concerning the proposed transfer for the regional entities' use in their evaluation. The registered entity's

current regional entity shall notify the registered entity in writing as to whether (i) the two regional entities agree that the requested transfer is appropriate, (ii) the two regional entities agree that the requested transfer is not appropriate and should not be processed further, or (iii) the two regional entities disagree as to whether the proposed transfer is appropriate.

3. If the two regional entities agree that the requested transfer is appropriate, they shall submit a joint written request to NERC requesting that the proposed transfer be approved and that the delegation agreement between NERC and each of the regional entities be amended accordingly. The regional entities' joint written submission to NERC shall describe the reasons for the proposed transfer; the location of the registered entity's bulk power system facilities in relation to the geographic and electrical boundaries of the respective regions; the impacts of the proposed transfer on other bulk power system owners, operators, and users; the impacts of the proposed transfer on the current and future staffing, resources, budgets and assessments of each regional entity, including the sufficiency of the proposed transferee regional entity's staffing and resources to perform compliance monitoring and enforcement activities with respect to the registered entity; the registered entity's compliance history with its current registered entity; and the manner in which pending compliance monitoring and enforcement matters concerning the registered entity will be transitioned from the current regional entity to the transferee regional entity. The NERC Board of Trustees shall consider the proposed transfer based on the submissions of the regional entities and any other information the board considers relevant, and shall approve or disapprove the proposed transfer and the related delegation agreement amendments. The NERC board may request that the regional entities provide additional information, or obtain additional information from the registered entity, for the use of the NERC board in making its decision. If the NERC board approves the proposed transfer, NERC shall file the related delegation agreements with FERC for approval.

4. If the two regional entities do not agree with each other that the proposed transfer is appropriate, the regional entity supporting the proposed transfer shall, if requested by the registered entity, submit a written request to NERC to approve the transfer and the related delegation agreement amendments. The regional entity's written request shall include the information specified in section 1208.3. The regional entity that does not believe the proposed transfer is appropriate will be allowed to submit a written statement to NERC explaining why the regional entity believes the transfer is not appropriate and should not be approved. The NERC Board of Trustees shall consider the proposed transfer based on the submissions of the regional entities and any other information the board considers relevant, and shall approve or disapprove the proposed transfer and the related delegation agreement amendments. The NERC board may request that the regional entities provide additional information, or obtain additional information from the registered entity, for the use of the NERC board in making its decision.

If the NERC board approves the proposed transfer, NERC shall file the related delegation agreements with FERC for approval.

5. Prior to action by the NERC Board of Trustees on a proposed transfer of registration under Section 1208.3 or 1208.4, NERC shall post information concerning the proposed transfer, including the submissions from the regional entities, on its Web site for at least twenty-one (21) days for the purpose of receiving public comment.

6. If the NERC Board of Trustees disapproves a proposed transfer presented to it pursuant to either section 1208.3 or 1208.4, the regional entity or entities that believe the transfer is appropriate may, if requested to do so by the registered entity, file a petition with FERC pursuant to 18 C.F.R. section 39.8(f) and (g) requesting that FERC order amendments to the delegation agreements of the two regional entities to effectuate the proposed transfer.

7. No transfer of a registered entity from one regional entity to another regional entity shall be effective (i) unless approved by FERC, and (ii) any earlier than the first day of January of the second calendar year following approval by FERC, unless an earlier effective date is agreed to by both regional entities and NERC and approved by FERC.

SECTION 1300 — COMMITTEES

1301. Establishing Standing Committees

The board may from time to time create standing committees. In doing so, the board shall approve the charter of each committee and assign specific authority to each committee necessary to conduct business within that charter. Each standing committee shall work within its board-approved charter and shall be accountable to the board for performance of its board-assigned responsibilities. A NERC standing committee may not delegate its assigned work to a member forum, but, in its deliberations, may request the opinions of and consider the recommendations of a member forum.

1302. Committee Membership

Each committee shall have a defined membership composition that is explained in its charter. Committee membership may be unique to each committee, and can provide for balanced decision-making by providing for representatives from each sector or, where sector representation will not bring together the necessary diversity of opinions, technical knowledge and experience in a particular subject area, by bringing together a wide diversity of opinions from industry experts with outstanding technical knowledge and experience in a particular subject area. Committee membership shall also provide the opportunity for an equitable number of members from the United States and Canada, based approximately on proportionate net energy for load. All committees and other subgroups (except for those organized on other than a sector basis because sector representation will not bring together the necessary diversity of opinions, technical knowledge and experience in a particular subject area) must ensure that no two stakeholder sectors are able to control the vote on any matter, and no single sector is able to defeat a matter. With regard to committees and subgroups pertaining to development of, interpretation of, or compliance with standards, NERC shall provide a reasonable opportunity for membership from sectors desiring to participate. Committees and subgroups organized on other than a sector basis shall be reported to the NERC board and the Member Representatives Committee, along with the reasons for constituting the committee or subgroup in the manner chosen. In such cases and subject to reasonable restrictions necessary to accomplish the mission of such committee or subgroup, NERC shall provide a reasonable opportunity for additional participation, as members or official observers, for sectors not represented on the committee or subgroup.

1303. Procedures for Appointing Committee Members

Committee members shall be nominated and selected in a manner that is open, inclusive, and fair. Unless otherwise stated in these rules or approved by the board, all committee member appointments shall be approved by the board, and committee officers shall be appointed by the Chairman of the Board.

1304. Procedures for Conduct of Committee Business

1. Notice to the public of the dates, places, and times of meetings of all committees, and all nonconfidential material provided to committee members, shall be posted

on the Corporation's Web site at approximately the same time that notice is given to committee members. Meetings of all standing committees shall be open to the public, subject to reasonable limitations due to the availability and size of meeting facilities; provided that the meeting may be held in or adjourn to closed session to discuss matters of a confidential nature, including but not limited to personnel matters, compliance enforcement matters, litigation, or commercially sensitive or critical infrastructure information of any entity.

2. NERC shall maintain a set of procedures, approved by the board, to guide the conduct of business by standing committees.

1305. Committee Subgroups

Standing committees may appoint subgroups using the same principles as in Section 1302.

SECTION 1400 — AMENDMENTS TO THE NERC RULES OF PROCEDURE

1401. Proposals for Amendment or Repeal of Rules of Procedure

In accordance with the bylaws of NERC, requests to amend or repeal the rules of procedure may be submitted by (1) any ~~ten~~fifty members of NERC, which number shall include members from at least three membership sectors~~segments~~, (2) the Member Representatives Committee, (3) a ~~standing~~ committee of NERC to whose function and purpose the rule pertains, or (4) an officer of ~~the ERO~~NERC.

1402. Approval of Amendment or Repeal of Rules of Procedure

Amendment to or repeal of rules of procedure shall be approved by the board after public notice and opportunity for comment in accordance with the bylaws of NERC. In approving changes to the rules of procedure, the board shall consider the inputs of the Member Representatives Committee, other ERO committees affected by the particular changes to the rules, and other stakeholders as appropriate. After board approval, the amendment or repeal shall be submitted to the ERO governmental authorities for approval, where authorized by legislation or agreement. No amendment to or repeal of the rules of procedure shall be effective until it has been approved by the applicable ERO governmental authorities.

~~**1403. Alternative Procedure for Violation Risk Factors**~~

~~In the event the standards development process fails to produce violation risk factors for a particular standard in a timely manner, the Board of Trustees may adopt violation risk factors for that standard after notice and opportunity for comment. In adopting violation risk factors, the board shall consider the inputs of the Member Representatives Committee and affected stakeholders.~~

SECTION 1500 — CONFIDENTIAL INFORMATION

1501. Definitions

1. **Confidential information** means (i) confidential business and market information; (ii) critical energy infrastructure information; (iii) personnel information that identifies or could be used to identify a specific individual, or reveals personnel, financial, medical, or other personal information; (iv) work papers, including any records produced for or created in the course of an evaluation or audit; (v) investigative files, including any records produced for or created in the course of an investigation; or (vi) cybersecurity incident information; provided, that public information developed or acquired by an entity shall be excluded from this definition.

2. **Confidential business and market information** means any information that pertains to the interests of any entity, that was developed or acquired by that entity, and that is proprietary or competitively sensitive.

3. **Critical energy infrastructure information** means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that (i) relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) could be useful to a person in planning an attack on critical infrastructure; and (iii) does not simply give the location of the critical infrastructure.

4. **Critical infrastructure** means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.

5. **Cybersecurity incident information** means any information related to, describing, or which could be used to plan or cause a cybersecurity incident as defined in 18 C.F.R. § 39.1.

1502. Protection of Confidential Information

1. **Identification of Confidential Information** — An owner, operator, or user of the bulk power system and any other party (the "submitting entity") shall mark as confidential any information that it submits to NERC or a regional entity (the "receiving entity") that it reasonably believes contains confidential information as defined by these rules, indicating the category or categories ~~defied~~defined in Section 1501 in which the information falls. If the information is subject to a prohibition on public disclosure in the Commission-approved rules of a regional transmission organization or independent system operator or a similar prohibition in applicable federal, state, or provincial laws, the submitting entity shall so indicate and provide supporting references and details.

2. **Confidentiality** — Except as provided herein, a receiving entity shall keep in confidence and not copy, disclose, or distribute any confidential information or any part thereof without the permission of the submitting entity, except as otherwise legally required.

3. **Information no longer Confidential –** If a submitting entity concludes that information for which it had sought confidential treatment no longer qualifies for that treatment, the submitting entity shall promptly so notify NERC or the relevant regional entity.

1503. Requests for Information

1. **Limitation** — A receiving entity shall make information available only to one with a demonstrated need for access to the information from the receiving entity.

2. **Form of Request** — A person with such a need may request access to information by using the following procedure:

   2.1 The request must be in writing and clearly marked "Request for Information."

   2.2 The request must identify the individual or entity that will use the information, explain the requester's need for access to the information, explain how the requester will use the information in furtherance of that need, and state whether the information is publicly available or available from another source or through another means. If the requester seeks access to information that is subject to a prohibition on public disclosure in the Commission-approved rules of a regional transmission organization or independent system operator or a similar prohibition in applicable federal, state, or provincial laws, the requester shall describe how it qualifies to receive such information.

   2.3 The request must stipulate that, if the requester does not seek public disclosure, the requester will maintain as confidential any information received for which a submitting party has made a claim of confidentiality in accordance with NERC's rules. As a condition to gaining access to such information, a requester shall execute a non-disclosure agreement in a form approved by NERC's board of trustees.

3. **Notice and Opportunity for Comment** — Prior to any decision to disclose information marked as confidential, the receiving entity shall provide written notice to the submitting entity and an opportunity for the submitting entity to either waive objection to disclosure or provide comments as to why the confidential information should not be disclosed. Failure to provide such comments or otherwise respond is not deemed waiver of the claim of confidentiality.

4. **Determination by ERO or Regional Entity** — Based on the information provided by the requester under Rule 1503.2, any comments provided by the submitting entity, and any other relevant available information, the chief executive officer or his or her designee of the receiving entity shall determine whether to disclose such information.

5. **Appeal** — A person whose request for information is denied in whole or part may appeal that determination to the President of NERC (or the President's designee) within 30 days of the determination. Appeals filed pursuant to this Rule must be in writing, addressed to the President of NERC (or the President's designee), and clearly marked "Appeal of Information Request Denial."

   NERC will provide written notice of such appeal to the submitting entity and an opportunity for the submitting entity to either waive objection to disclosure or provide comments as to why the confidential information should not be disclosed; provided that any such comments must be received within 30 days of the notice and any failure to provide such comments or otherwise respond is not deemed a waiver of the claim of confidentiality.

   The President of NERC (or the President's designee) will make a determination with respect to any appeal within 30 days. In unusual circumstances, this time limit may be extended by the President of NERC (or the President's designee), who will send written notice to the requester setting forth the reasons for the extension and the date on which a determination on the appeal is expected.

6. **Disclosure of Information** — In the event the receiving entity, after following the procedures herein, determines to disclose information designated as confidential information, it shall provide the submitting entity no fewer than 21 days' written notice prior to releasing the information in order to enable such submitting entity to (a) seek an appropriate protective order or other remedy, (b) consult with the receiving entity with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Rule. Should a receiving entity be required to disclose confidential information, or should the submitting entity waive objection to disclosure, the receiving entity shall furnish only that portion of the confidential information which the receiving entity's counsel advises is legally required.

7. **Posting of Determinations on Requests for Disclosure of Confidential Information** — Upon making its determination on a request for disclosure of confidential information, NERC or the regional entity, as applicable, shall (i) notify the requester that the request for disclosure is granted or denied, (ii) publicly post any determination to deny the request to disclose confidential information, including in such posting an explanation of the reasons for the denial (but without in such explanation disclosing the confidential information), and (iii) publicly post any determination that information claimed by the submitting entity to be confidential information is not confidential information (but without in such

posting disclosing any information that has been determined to be confidential information).

1504. Employees, Contractors and Agents

A receiving entity shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom confidential information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein.

1505. Provision of Information to FERC and Other Governmental Authorities

1. **Request** — A request from FERC for reliability information with respect to owners, operators, and users of the bulk power system within the United States is authorized by Section 215 of the Federal Power Act. Other applicable ERO governmental authorities may have similar authorizing legislation that grants a right of access to such information. Unless otherwise directed by FERC or its staff or the other ERO governmental authority requesting the information, upon receiving such a request, a receiving entity shall provide contemporaneous notice to the applicable submitting entity. In its response to such a request, a receiving entity shall preserve any mark of confidentiality and shall notify FERC or other appropriate governmental authorities that the submitting entity has marked the information as confidential.

2. **Continued Confidentiality** — Each receiving entity shall continue to treat as confidential all confidential information that it has submitted to NERC or to FERC or another appropriate ERO governmental authority, until such time as FERC or the other appropriate ERO governmental authority authorizes disclosure of such information.

1506. Permitted Disclosures

1. **Confirmed Violations** — Nothing in this Section 1500 shall prohibit the disclosure of a violation at the point when the matter is filed with an appropriate governmental authority as a notice of penalty, the "violator" admits to the violation, or the alleged violator and NERC or the regional entity reach a settlement regarding the violation.

2. **Compliance Information** — NERC and the regional entities are authorized to exchange confidential information related to evaluations, audits, and investigations in furtherance of the compliance and enforcement program, on condition they continue to maintain the confidentiality of such information.

1507. Remedies for Improper Disclosure

Any person engaged in NERC or regional entity activity under section 215 of the Federal Power Act or the equivalent laws of other appropriate governmental authorities who improperly discloses information determined to be confidential may lose access to confidential information on a temporary or permanent basis and may be subject to

adverse personnel action, including suspension or termination. Nothing in Section 1500 precludes an entity whose information was improperly disclosed from seeking a remedy in an appropriate court.

SECTION 1600 — REQUESTS FOR DATA OR INFORMATION

1601. Scope of a NERC or Regional Entity Request for Data or Information

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

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

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

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

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

or "identity masking"); and (vi) an estimate of the relative burden imposed on the reporting entities to accommodate the data or information request.

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

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

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

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

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

1603. Owners, Operators, and Users to Comply

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

1604. Requests by Regional Entity for Data or Information

1. A regional entity may request that NERC seek authorization for a request for data or information to be applicable within the footprint of the regional entity, either as a freestanding request or as part of a proposed NERC request for data or information. Any such request must be consistent with this Section 1600.

2. A regional entity may also develop its own procedures for requesting data or information, but any such procedures must include at least the same procedural

elements as are included in this Section 1600. Any such regional entity procedures or changes to such procedures shall be submitted to NERC for approval. Upon approving such procedures or changes thereto, NERC shall file the proposed procedures or proposed changes for approval by the Commission and any other ERO governmental authorities applicable to the regional entity. The regional entity procedures or changes to such procedures shall not be effective in a jurisdiction until approved by, and in accordance with any revisions directed by, the Commission or other ERO governmental authority.

1605. Confidentiality

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

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

1. In the event NERC or a regional entity must obtain data or information by a date or within a time period that does not permit adherence to the time periods specified in Section 1602, the procedures specified in Section 1606 may be used to obtain the data or information. Without limiting the circumstances in which the procedures in Section 1606 may be used, such circumstances include situations in which it is necessary to obtain the data or information (in order to evaluate a threat to the reliability or security of the bulk-power system, or to comply with a directive in an order issued by the Commission or by another ERO governmental authority) within a shorter time period than possible under Section 1602. The procedures specified in Section 1606 may only be used if authorized by the NERC Board of Trustees prior to activation of such procedures.

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

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

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

From: Alex Zak
To: Alex Zak
Subject: NERC: Comment Period Opens for Proposed Changes to NERC Rules of Procedure and Associated Appendices
Date: Monday, November 07, 2011 8:53:34 PM

Proposed Changes to the NERC Rules of Procedure and Associated Appendices

Announcement: Comment Period Opens for Proposed Changes to NERC Rules of Procedure and Associated Appendices

November 7, 2011

Click Here for access to the proposed changes: (NERC Rules of Procedure webpage)

The North American Electric Reliability Corporation (NERC) is proposing changes to its Rules of Procedure (ROP), Sections 100-1600, and associated Appendices 4B, 4C, 5A and 8, and deletion of Appendices 3C and 6. NERC is soliciting comments on these proposed amendments. Redlined versions of ROP Sections 100-1600 and Appendices 4B, 4C, 5A and 8, showing the proposed additions, deletions and revisions, are now available at: http://www.nerc.com/page.php?cid=1|8|169. In addition, the posting includes a separate document that provides a detailed summary and discussion of the proposed revisions and the reasons they are being proposed.

Proposed revisions to ROP Sections 100-1600 and Appendices 4B and 4C were previously posted for stakeholder comment from July 1 – August 15, 2011. Based on consideration of the comments submitted on that posting and further discussions among NERC, the Regional Entities and stakeholders, numerous further revisions have been made to ROP Sections 100-1600 and Appendices 4B and 4C (including deletion or significant modifications of previously-proposed revisions). These deletions and additional modifications are incorporated into the versions of ROP Sections 100-1600 and Appendices 4B and 4C on which comments are now being solicited. The proposed revisions to Appendices 5A and 8 and the proposed deletion of Appendices 3C and 6 are being posted for stakeholder comment for the first time.

Comments are due December 22, 2011, and must be submitted electronically to ROPcomments@nerc.net**.** NERC presently intends to submit the proposed changes to the ROP and Appendices (as revised based on consideration of the comments received on this posting) to the NERC Board of Trustees for approval at its February 9, 2012 meeting. If approved by the Board, the proposed amendments would then be filed with applicable governmental authorities.

For further information, please contact Rebecca Michael at rebecca.michael@nerc.net.

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

Ms. Alex Zak

alex.zak@nerc.net

NERC -North American Electric Reliability Corporation

Legal Dept.

Tel: (202) 393-3998 ext. 429

Direct: (202) 383-2640; Cell: (202) 236-5764; Fax: (202) 393-3955

This e-mail and any of its attachments may contain NERC proprietary information that is privileged, confidential, or subject to copyright belonging to NERC. This e-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this e-mail is strictly prohibited and may be unlawful. If you receive this e-mail in error, please notify the sender immediately and permanently delete the original and any copy of this e-mail and any printout.

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1275547-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

Summary of Proposed Changes to the NERC Rules of Procedure and Associated Appendices

November 7, 2011

The North American Electric Reliability Corporation (NERC) is proposing changes to its Rules of Procedure (ROP), Sections 100-1600, and associated Appendices 4B, 4C, 5A and 8, and deletion of Appendices 3C and 6. NERC is soliciting comments on these proposed amendments. Redlined versions of ROP Sections 100-1600 and Appendices 4B, 4C, 5A and 8, showing the proposed additions, deletions and revisions, are now available at http://www.nerc.com/page.php?cid=1|8|169.[1] In addition, the posting includes a separate document that provides a detailed summary and discussion of the proposed revisions and the reasons they are being proposed.

Proposed revisions to ROP Sections 100-1600 and Appendices 4B and 4C were previously posted for stakeholder comment from July 1 – August 15, 2011. Based on consideration of the comments submitted on that posting and further discussions among NERC, the Regional Entities and stakeholders, numerous further revisions have been made to ROP Sections 100-1600 and Appendices 4B and 4C (including deletion or significant modifications of previously-proposed revisions). These deletions and additional modifications are incorporated into the versions of ROP Sections 100-1600 and Appendices 4B and 4C on which comments are now being solicited. The proposed revisions to Appendices 5A and 8 and the proposed deletion of Appendices 3C and 6 are being posted for stakeholder comment for the first time.[2]

Comments are due December 22, 2011, and must be submitted electronically to ROPcomments@nerc.net. NERC presently intends to submit the proposed changes to the ROP and Appendices (as revised based on consideration of the comments received on this posting) to the NERC Board of Trustees for approval at its February 9, 2012 meeting. If approved by the Board, the proposed amendments would then be filed with applicable governmental authorities.

Overview of Reasons for the Proposed Amendments

[1] Because extensive changes are proposed to the current Appendix 8, a "clean" version of proposed revised Appendix 8 is also included in this posting, for the convenience of readers.

[2] As described in the summary document included with this posting, in addition to the proposed deletion of Appendix 6 — System Operator Certification Program Manual, NERC is proposing to move to ROP Section 600 many provisions that are currently in Appendix 6.

The proposed revisions to the ROP and Appendices are the result of the continuation of a process that began with the preparation of NERC's *Three-Year ERO Performance Assessment Report* that was filed with the Commission on July 20, 2009 in accordance with 18 C.F.R. §39.3(c). The *Three-Year ERO Performance Assessment Report* identified a number of changes to be made in the ERO's operations and processes, some of which required amendments to the NERC ROP. Following submission of the *Three-Year ERO Performance Assessment Report*, NERC and the Regional Entities engaged in a process to identify, draft, and submit for approval (1) necessary changes to NERC's delegation agreements with the Regional Entities, and (2) associated amendments to the ROP. This process resulted in development of a new version of the delegation agreements as well as proposed revisions to ROP Sections 100-1600 and Appendices 4A, 4B and 4C and a new Appendix 5B.[3] These documents were filed with the Commission for approval on June 9, 2010, were conditionally approved by the Commission in an Order issued October 21, 2010, and became effective on January 1, 2011. Additional revisions resulting from the October 21, 2010 Commission Order were submitted in compliance filings on February 18, 2011 and November 7, 2011.

Although the proposed ROP amendments filed with the Commission on June 9, 2010, largely addressed revisions associated with, or identified in the development of, the revised delegation agreements, several NERC-Regional Entity working groups continued to work identify additional revisions to the ROP and Appendices that were necessary or appropriate, based on issues identified in the *Three-Year ERO Performance Assessment Report* as well as on the experience of NERC and the Regional Entities in implementing the existing ROP, and carrying out the duties and responsibilities of the ERO, over the period since NERC was certified as the ERO, the delegation agreements with the Regional Entities were initially approved by the Commission, and the Commission-approved reliability standards became mandatory and enforceable.[4] As of today, this period represents more than four years of operating experience. The working groups engaged in studying the need for, identifying and developing further revisions to the ROP and Appendices included a working group comprised of representatives of compliance program staffs of NERC and the Regional Entities, a working group comprised of representatives of the legal staffs of NERC and the Regional Entities, and an Event Analysis Working Group comprised of NERC and Regional Entity representatives. The experience brought to bear on these reviews of the ROP and Appendices has included the more than four years of experience of the NERC and Regional Entity staffs in administering and implementing the compliance monitoring and enforcement processes, determining penalties for violations of reliability standards pursuant to the NERC Sanction Guidelines, conducting or participating in hearings before Regional Entity Hearing Bodies on compliance enforcement matters, and responding to and conducting analyses of events on

[3] New Appendix 5B is the NERC Statement of Compliance Registry Criteria, which was not previously included in the ROP.

[4] NERC was certified as the ERO by the Commission in an Order issued July 20, 2006. The delegation agreements between NERC and the Regional Entities were originally approved by the Commission in an Order issued April 19, 2007. The initial set of reliability standards approved by the Commission became effective on June 18, 2007.

the bulk power system. In a number of instances, the working groups recognized, with the benefit of experience in implementing and applying particular ROP provisions, that the clarity of an ROP provision could be improved through rewriting it, or that two ROP provisions were inconsistent. In other instances, it was recognized, again based on experience, that the ROP did not address certain situations that had arisen in the development of reliability standards, implementation of the compliance monitoring and enforcement program, determination and assessment of penalties, conduct of hearings on compliance enforcement matters, registration and certification of entities, and other ERO activities, that should be addressed in the ROP. In addition, legal review of the ROP and Appendices was undertaken to identify provisions that are obsolete, unclear, constitute undue detail, or describe administrative or process details that do not rise the level of "ERO Rules" that need to be in the ROP and Appendices, but rather can be moved to lower-tiered documents or eliminated entirely.[5]

For example, the proposed revisions to the ROP that are being posted for comment include revisions that were identified from these diverse sources:

- Various provisions in ROP Section 300, Reliability Standards Development, were identified as inconsistent with revisions to Appendix 3A — Standard Processes Manual that were approved by the Commission in 2010 and 2011.

- It was recognized that Appendix 3C — Procedure for Coordinating Reliability Standards Approvals, Remands, and Directives, can be deleted as no longer necessary. Appendix 3C was originally developed in response to directives in P 286 of the Commission's July 2006 ERO Certification Order, concerning coordination among the applicable North American regulatory bodies with authority over development and approval of reliability standards for the bulk power system, specifying that NERC should identify the relevant regulatory bodies and their respective standards approval and remand processes that will be implicated in any remand of a proposed reliability standards, and specify the actual steps to coordinate all of these processing requirements, including those that may be necessary for an expedited deadline to return a remanded proposed reliability standards. As NERC has continued, subsequent to 2006, in its efforts to gain recognition as the ERO and adoption of mandatory reliability standards in the Canadian provinces and Mexico, the requirements and processes applicable to adoption and revision of reliability standards in the non-U.S. jurisdictions have been established by legislation or regulation with those jurisdictions or by memoranda of understanding between NERC and the applicable governmental authorities. As the concerns underlying the directives in P 286 of the ERO Certification Order are now addressed through legislation, regulation, or memoranda of understanding in or with the non-U.S. applicable governmental authorities, Appendix 3C can be deleted.

[5] Elimination from the ROP of administrative and other provisions that do not rise to the level of ERO Rules provides greater flexibility in revising those provisions in the future as needed, since the future changes can be effectuated without the need to post them for comments, submit them to the NERC Board for approval, and then file them with FERC for approval, before the revised provisions can become effective.

- A number of provisions were identified in Appendix 4B — Sanction Guidelines, that are not directly related to determining penalties and sanctions for violations of reliability standards and should be removed from Appendix 4B (some of these provisions are covered in other ROP sections or Appendices where they are more appropriately placed). Other provisions were identified in Appendix 4B that are internally redundant. This review resulted in proposed revisions that significantly simplify and streamline the text of Appendix 4B.

- It was recognized that the processes described in Appendix 4C — Compliance Monitoring and Enforcement Program, should be more clearly separated into "compliance processes" (Section 3.0 of Appendix 4C) and "enforcement" processes (Section 5.0).

- In the conduct of Regional Entity hearings to date, a number of procedural situations had arisen, in the experience of Regional Entities, that were not addressed in the current Hearing Procedures (Attachment 2 to Appendix 4C), or as to which the current Hearing Procedures did not provide sufficient guidance to the Hearing Officer, Hearing Body and the parties as to their roles, responsibilities and authorities in addressing these situations. The proposed amendments to the Hearing Procedures that are being presented for comment are intended to provide guidance and greater clarity with respect to these situations. The recognition of the need for these revisions to the Hearing Procedures was the result of the collective experience of the Regional Entities in conducting a number of hearings on compliance matters.

- It was determined that a number of changes need to made to Appendix 5A — Organization Registration and Certification Manual, to correctly reflect the respective responsibilities of NERC and the Regional Entities in the registration process based on the revised delegation agreements that became effective on January 1, 2011.

- The need was identified, based on experience, to provide a more streamlined process in Appendix 5A for certification of entities to perform the functions of Reliability Coordinator, Transmission Operator and Balancing Authority where an entity is already certified for a reliability function and seeks only to expand the footprint in which it will perform the reliability function.

- It was determined that Appendix 6 — System Operator Certification Manual, contains a very considerable amount of administrative details (such as procedures for registering for certification examinations, procedures and conduct at the testing center, and various fees) which do not rise to level of ERO Rules and do not need to be in the ROP. When these administrative provisions were removed, it was recognized that the remaining, substantive material in Appendix 6 could readily be moved to Section 600 of the ROP, and the separate Appendix 6 could be eliminated.

- As the result of concerns and comments about the event analysis process raised during the three-year ERO assessment process and directives in orders issued by the Commission in connection with

the three-year assessment and the subsequent revisions to the delegation agreements and associated revisions to the ROP,[6] it has been recognized that significant review and revision of the process was warranted. Among other things, it was determined that operational and administrative details of the event response and event analysis processes should be placed into a separate Event Analysis Process document that will not be part of the ROP; placement of such details in a separate document will facilitate revisions to these process details as warranted based on experience without the necessity of following the lengthy ROP revision process. An Event Analysis Working Group has developed an ERO Event Analysis Process which has been undergoing field testing since October 2010. As part of this effort, it was also recognized that requirements imposed on registered entities should remain in the ROP, as Commission-approved ERO Rules; and that the current ROP Appendix (Appendix 8) on responding to and analyzing events on the bulk power system, needed to be significantly revised to reflect the revised roles and responsibilities of NERC, the Regional Entities and registered entities in responding to and analyzing bulk power system events. The result is the proposed revised Appendix 8 — NERC Event Response Procedures, on which comments are being solicited in this posting.

The Summary of Proposed Rules of Procedure Revisions that is included as part of this posting provides a detailed summary and discussion, on a section-by-section basis, of the proposed amendments to ROP Sections 100-1600, as well as of the proposed revisions to Appendices 4B, 4C, 5A and 8 and the proposed deletions of Appendices 3C and 6. The discussion in the Summary includes explanation of the reasoning behind proposed substantive changes.

[6] *North American Electric Reliability Corp., Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010); *North American Electric Reliability Corp., Order Conditionally Approving Revised Pro Forma Delegation Agreement, Revised Delegation Agreements with Regional Entities, Amendments to Rules of Procedure and Certain Regional Entity Bylaws*, 133 FERC ¶ 61,061 (2010).

Summary of Proposed Rules of Procedure Revisions

I. Rules of Procedure Sections 100-1600[1]

A. Section 200 – Definitions of Terms

Certification – added definition relating to system operator certification which is currently provided in Appendix 6 which is being deleted; definition has also been revised from current Appendix 6 at the direction of the Personnel Certification Governance Committee

Compliance enforcement authority – added definition (same definition as in Appendix 4C, CMEP).

Confirmed violation – revised definition to be consistent with revised definition in Appendix 4C, Compliance Monitoring and Enforcement Program.

Continuing education hour or CE hour – added definition relating to system operator certification currently provided in Appendix 6, which is being deleted.

Entity variance – deleted definition – this term is not used.

Remedial action directive – added definition here (same definition as in Appendix 4C, CMEP).

Variance – revised definition to be consistent with definition in Appendix 3A, Standard Processes Manual.

B. Section 300 – Reliability Standards Development

Section 304.1 – Added "and entities" for clarity and completeness.

Section 304.4 – Revised for consistency with Appendix 3A, Standard Processes Manual.

Section 305.5 – Corrected Appendix reference from Appendix 3A to Appendix 3D.

Section 306.1 – Added text to reflect that the Standards Committee will include "two officers elected to represent the interests of the industry as a whole."

Section 306.2 – Corrected reference from Appendix 2 to Appendix 3B.

[1] Sections that do not have proposed revisions are not listed in this Summary.

Section 306.3 – Deleted specific provisions on Canadian representation and replaced them with: "The Standards Committee will include Canadian representation as provided in **Appendix 3B**, *Procedure for the Election of Members of the NERC Standards Committee*." This topic is covered substantively in Appendix 3B.

Section 307 – Changed title to "Standards Process Management"; revised text to describe functions of the NERC regional standards manager as well as the NERC standards process manager.

Sections 308.1 – Revised text to refer to expedited processes for developing reliability standards, including developing reliability standards to address national security situations that involve confidential issues (replacing reference to "urgent action" reliability standards). "Urgent action" is no longer used in Appendix 3A.

Section 308.2 & 308.3 – Revised text to reflect that reliability standards are "adopted," not "approved," by the NERC Board of Trustees (in accordance with ANSI requirements).

Section 309.1 -- Revised text to reflect that reliability standards are "adopted," not "approved," by the NERC Board of Trustees (in accordance with ANSI requirements).

Section 309.2 – Changed reference from "expedited action procedure" to "expedited standards development process".

Section 309.3 – Deleted provision that where an ERO governmental authority directs development of a standard by a deadline, NERC staff must, after preparing a SAR, attempt to find a stakeholder sponsor for the SAR. Also changed reference from "expedited action procedures" to "expedited action process" for consistency with Appendix 3A.

Section 309.3.1 – Deleted this section as no longer necessary based on the current version of Appendix 3A.

Section 311.3.1.3 – Changed text from "control the vote on a matter" to "dominate a matter" to be consistent with terminology in §304.4 and in Appendix 3A.

Section 311.3.1.6 – Deleted reference to accreditation of a Regional Standards Development Procedure by the Standards Council of Canada as sufficient to establish compliance with the evaluation criteria in §311.3.1. The Standards Council of Canada has advised NERC that accreditation by that body is not available to entities based in the U.S.

Section 312.1 – Revised text to make clear that Regional Reliability Standards must be submitted to NERC for adoption, and, if adopted, become part of the NERC reliability standards.

Section 313.1 – Added "NERC" before "reliability standards" for clarity.

Section 315 – Changed title of section to refer to the NERC Standard Processes Manual, which is the current title of Appendix 3A.

Section 316 – Deleted reference to seeking "continuing" accreditation since ANSI does not grant "continuing" accreditation, and replaced it with a statement that NERC will "seek and maintain" accreditation. Also, deleted reference to seeking accreditation from the Standards Council of Canada; the Standards Council of Canada has advised that accreditation is not available to NERC since it is not based in Canada.

Section 317 – Revised text as follows: "NERC shall complete a review of each NERC reliability standard at least once every five years, or such longer period as is permitted by the American National Standards Institute, from the effective date of the standard or the latest revision to the standard, whichever is later." It may be possible to obtain relief from ANSI from the requirement that each standard be reviewed at least every five years.

Section 318 – Deleted reference to ISO/RTO Council. Although NERC strives to maintain close working relationships with the ISO/RTO Council and with industry associations and other, similar organizations, based on experience NERC has not found it necessary to work specifically with the ISO/RTO Council to coordinate wholesale electric business standards and market protocols with NERC reliability standards.

Section 319 – Changed reference to "standards that expired or were replaced" to "standards that have been retired," which is consistent with the terminology NERC uses elsewhere to describe standards no longer in effect. Also, changed reference to "NERC standards manager" to "NERC standards information manager" – the position of standards information process manager will be responsible for receiving and responding to requests for archived standards information.

Section 320 – The section has been revised to describe generally the process for developing and approving VRFs and VSLs, rather than just the alternate method for adopting VRFs. New §320.1 states that NERC will follow the process for developing VRFs and VSLs set forth in the Standard Processes Manual. New §320.2 states that if an ERO governmental authority remands or directs a revision to a Board-approved VRF or VSL, the NERC director of standards (based on consultation with the standard drafting team), the Standards Committee, and the NERC director of compliance options, will recommend one of three actions to the Board: (1) file a request for clarification, (2) file a request for rehearing, or (3) approve the directed revision. Section 320.3, which now contains the "alternative procedure," has been amended to apply to VSLs and well as to VRFs. Section 320.3 (which includes content being moved from ROP §1403, as it is more appropriately located in §300), has also been amended to specify that there will be notice and opportunity for comment before the Board approves a VRF or VSL, and that the Board will consider the inputs of the MRC and affected stakeholders.

C. Section 400 – Compliance Enforcement

Section 401.6 – For clarity of this point, the second sentence is amended as follows: "Compliance is required, and NERC and the regional entities have authority to monitor compliance, with all NERC reliability standards whether or not they are included in the subset of reliability standards and requirements designated to be actively monitored and audited in the NERC annual compliance program." Registered entities are subject to monitoring for compliance with all standards applicable to their registered functions, not just the standards on the actively monitored list.

Section 401.7 – Changed reference to "remedial actions" to "remedial action directives," which is a defined term. (This change has been made in a number of places throughout the ROP.)

Section 401.8 – Amended section to specify that a registered entity shall not be subject to an enforcement action by more than one Regional Entity for the same violation.

Section 401.9 – Changed reference to "remedial actions" to "remedial action directives."
Section 401.11 – Added reference to "or other mitigating activities" after "mitigation plan." This revision, which is made in a number of places throughout the ROP, reflects the fact that actions taken by a registered entity to correct and prevent recurrence of a non-compliance, while they are accepted by the CEA, are not always memorialized in a formal mitigation plan.

Section 402.5 – The revisions are intended to make the text more consistent with the definition of remedial action directive.

Section 402.6 – Changed reference to "remedial actions" to "remedial action directives."

Section 403.4 – Changed reference to "Hearing Process" to "Hearing Procedures" (Attachment 2 to Appendix 4C).

Section 403.6 – Added reference to "mitigating activities" and changed reference to "remedial actions" to "remedial action directives."

Section 403.7.3 – Changed reference to "remedial actions" to "remedial action directives."

Section 403.14 – In the title of this section, changed reference to "remedial actions" to "remedial action directives." Also, this section is amended to make clear that confirmed violations, penalties and sanctions specified in a Regional Entity hearing body final decision (as well as confirmed violations, penalties and sanctions developed by the Regional Entity through the enforcement process without a hearing) will be provided to NERC for review and filing with the applicable ERO governmental authorities as a notice of penalty.

Section 403.15 – The last paragraph of this section is amended to provide that a regional entity (as well as a bulk power system owner, operator or user) may appeal a Regional Entity hearing body decision to NERC in accordance with §409.

Section 403.16 – Amended to advance the date by which annual Regional Entity compliance enforcement program implementation plans are to be submitted to NERC, from November 1 to October 1 of the preceding year.

Section 407.1 – Changed references to "remedial actions" to "remedial action directives" to reflect the context. In addition, the section is amended to provide that NERC will review penalties, sanctions and remedial action directives specified by a Regional Entity hearing body final decision, to determine if the determination is supported by a sufficient record, consistent with the *Sanction Guidelines* and other directives, guidance and directions issued by NERC pursuant to the delegation agreement, and consistent with penalties, sanctions and remedial action directives imposed by the Regional Entity and by other Regional Entities for violations involving the same or similar facts and circumstances. In order to perform its function of ensuring consistency in penalty determinations for similar violations and among Regional Entities, it is necessary for NERC to review penalties determined by Regional Entity hearing bodies just as it determines penalties determined by Regional Entity compliance enforcement staff.

Section 408 – Several references to the NERC director of compliance are changed to the NERC director of enforcement. Additionally, §408.1 is revised to add reference to Regional Entities appealing decisions of Regional Entity hearing bodies pursuant to ROP §409.

Section 409.1 – The section is amended to reflect that a Regional Entity acting as the compliance enforcement authority, as well as a bulk power system owner, operator or user, may appeal a final decision of a Regional Entity hearing body. Additional amendments are made to use defined terms. Another amendment specifies that the entity appealing must submit its notice of appeal to the NERC director of enforcement (formerly director of compliance) and provide copies to the Regional Entity and any other participants in the Regional Entity hearing body proceeding. The last sentence of the section is deleted as unnecessary.

Section 409.2 – Changed "compliance hearing" to "proceeding."

Section 409.3 & 409.4 – Changed to reflect that the Regional Entity may file an appeal of a Regional Entity hearing body decision, to specify that the Regional Entity shall file the entire record of the Regional Entity hearing body with the NERC director of enforcement, to specify that participants in the hearing body proceeding other than the appellant shall file their responses to the issues raised in the notice of appeal 35 days after the date of appeal (which will allow for at least a 14-day period after the record of the hearing body proceedings is filed with the NERC director of enforcement), and to provide that the appellant may file a reply to the responses within 7 days.

Section 409.5 – Changed to specify that in considering an appeal from a Regional Entity hearing body decision, the BOTCC may allow other participants to the Regional Entity (in addition to the party appealing), to appear before the BOTCC.

Section 409.8 – New section is added to specify that Section 409 is not applicable to an appeal taken from a decision of the Regional Entity hearing body granting or denying a motion to intervene in the Regional Entity hearing, and that such appeals shall be conducted in accordance with ROP §414.

Section 412 – This new section sets forth the procedures by which the NERC BOTCC will accept or reject a question certified to the BOTCC by a Regional Entity hearing body (pursuant to §1.5.12 of the Hearing Procedures in Appendix 4C), and if the BOTCC decides to accept the certified question, the procedure for receiving argument from the participants on, and deciding, the question. Section 412.2 specifies that written decisions of the BOTCC on certified questions will be posted on the NERC web site, with redaction of the names of the participants and of any other information that is necessary to maintain the non-public nature of the Regional Entity hearing body proceeding.

Section 413 – This new section specifies that NERC shall review and process final decisions of Regional Entity hearing bodies concerning alleged violations, proposed penalties or sanctions, or proposed mitigation plans, that are not appealed to the BOTCC, as though the determination was made by the Regional Entity compliance program, and may require that the decision be modified by the Regional Entity, in accordance with sections 5.8, 5.9 and 6.5 of Appendix 4C. In order to perform its function of ensuring consistency in violation, penalty and mitigation plan determinations for similar facts and circumstances and among Regional Entities, it is necessary for NERC to review penalties determined by Regional Entity hearing bodies just as it reviews violations, penalties and mitigation plans determined or approved by Regional Entity compliance enforcement staffs.

Section 414 – This new section establishes procedures for review and decision by the NERC BOTCC of appeals of decisions of a Regional Entity hearing body to grant or deny a request for intervention in the Regional Entity hearing body proceeding. Addition of these procedures is needed due to the proposed amendment to §1.4.4 of the Hearing Procedures to allow the Regional Entity hearing body to grant requests to intervene in limited circumstances. New §414.5 recognizes that the BOTCC's decision on the appeal may thereafter be appealed to FERC or to another ERO governmental authority having jurisdiction over the matter, in accordance with the authorities, rules and procedures of the ERO governmental authority.

D. Section 500 – Organization Registration and Certification

Section 501 – The first paragraph is revised for clarification to refer to certification of entities performing certain specified functions, rather than entities applying to be a RC, BA or TOP.

Section 501.1.3.1 – This section is revised to provide greater specificity with respect to the effective date of an entity's registration, particularly in the case of registrations resulting from sales or transfers of BPS assets or from corporate reorganizations that result in a new legal entity owning BPS assets formerly owned by another registered entity. The effective date will be stated in NERC's notification of registration. Where the organization is being registered for the first time and its BPS facilities were not previously owned by another registered entity, the effective date of the registration will be the date agreed to by the entity to be registered and the applicable Regional Entity. Where the organization is being registered because it has acquired BPS facilities from a registered entity, or based on an internal restructuring or name change where the organization has been registered under a different entity name, the effective date of the registration will be the effective date of the transaction that results in the organization performing the reliability functions that require it to be registered.

Section 501.2 – This section is amended to refer to the need for certification of RCs, TOPs and BAs and entities that perform some or all of the reliability functions of RCs, TOPs and BAs. Additionally, reference to the NERC Provisional Certification Process is deleted, as that process is no longer needed and is being eliminated.

Section 501.2.1 – Amended to refer to entities intending to perform (as well as entities performing) the functions of RC, TOPs and BAs, since the certification process applies to entities seeking to perform these functions as well as entities already performing the functions.

E. Section 600 – Personnel Certification

Section 600 has been substantially revised and expanded. Appendix 6, System Operator Certification Program Manual, is being deleted in its entity and its substantive provisions are being moved into Section 600.

Section 601 – Scope of Personnel Certification – This section is amended to state (1) that the Personnel Certification Program awards system operator certification credentials to individuals who demonstrate that they have attained essential knowledge relating to NERC reliability standards as well as principles of BPS operations, and (2) that except as necessary to obtain approval of the ROP, the NERC Personnel Certification Governance Committee (PCGC) is the governing body that establishes the polices, sets fees, and monitors the performance of the Personnel Certification Program for system operators.

Section 602 – Structure of ERO Personnel Certification Program – This section contains existing provisions describing the structure of the Personnel Certification Program.

Section 603 – Examination and Maintenance of NERC System Operator Certification Credentials – Section 603 is a new section encompassing material being moved from Appendix 6. It describes the basic requirements for obtaining a system operator certification (*i.e.*, passing an examination) and maintaining the certification (*i.e.*, earning the necessary number of Continuing Education (CE) hours

during the ensuing three-year period). It also states what occurs should the certified operator fail to obtain the necessary amount of CE hours during the three-year period, including the procedure for requested a hardship clause exception.

Section 604 – Dispute Resolution Process – Section 604 is a new section encompassing material being moved from Appendix 6. It describes the NERC System Operator Certification Dispute Resolution Process for resolving disputes that arise under the System Operator Certification Program concerning any aspect of the certification process. The Dispute Resolution Process is for the use of persons who hold an operator certification or persons wishing to be certified to dispute the validity of the examination, the content of the test, the content outlines, or the registration process.

Section 605 – Disciplinary Action – Section 605 is a new section encompassing material being moved from Appendix 6. It describes the grounds and procedures for disciplinary action against a system operator, including the hearing process and the possible decisions that may be rendered against the system operator. It also describes the Credential Review Task Force, which will make factual determinations and ultimate determinations as to disciplinary action.

Section 606 – Candidate Testing Mechanisms – This section is currently Section 603 of the ROP. The text has not been revised.

Section 607 – Public Information About the Personnel Certification Program – This section is currently Section 604 of the ROP. It has been revised to state that the Personnel Certification Program shall maintain and publish publicly a System Operator Certification Program Manual, covering listed topics; and shall maintain and publish publicly a comprehensive summary or outline of the of the information, knowledge, or functions covered by each system operator certification examination and a summary of certification activities for the program.

Section 608 – Responsibilities to Applicants for Certification or Recertification – This section is currently Section 605 of the ROP. Items 8 and 9 in the list of duties and responsibilities of the Personnel Certification Program (implement and publish policies and procedures providing due process for applicants questioning eligibility determination, examination results and certification status, and develop and maintain a program manual containing the processes and procedures for applicants for certification and recertification) have been deleted since these topics are covered in Sections 604 and 607.

Section 609 – Responsibilities to the Public and to Employers of Certified Practitioners – This section is currently Section 606 of the ROP. It has been revised (1) to delete the provision that the Personnel Certification Program shall periodically publish a current list of those persons who are certified, and (2) to delete a reference to the disciplinary action program being contained in Appendix 6, as it will be included in Section 605.

F. Section 800 – Reliability Assessment and Performance Analysis

Sections 807 and 808 have been revised to provide for a more consistent use of terms in these sections including "major event" and "occurrences." Similar revisions have been made in Appendix 8.

Section 807a is revised to state that in responding to a major event, NERC will work with registered entities as well as with Regional Entities and Reliability Coordinators.

Sections 807c and 808.3 are amended to refer to NERC Reliability Standard EOP-004 which sets forth specific criteria and procedures for reporting BPS disturbances and events described in that standard, with which registered entities subject to EOP-004 must comply. These sections further states that BPS users, owners and operators shall also provide NERC and Regional Entities with such additional information they request as is necessary to enable them to carry out their responsibilities under these sections.

Section 807e is amended to provide that NERC will establish, maintain, and revise from time to time based on experience a manual setting forth procedures and protocols for communications and sharing and exchange of information between and among NERC, Regional Entities, governmental authorities, industry organizations, and BPS users, owners and operators, concerning the investigation and analysis of major events.

Section 807f is amended to reflect the revised title of Appendix 8.

Section 807g is amended to state that NERC will disseminate to the industry findings and recommendations of general applicability from event analyses, "through various means appropriate to the circumstances," including in accordance with ROP §810. This revision will give NERC greater flexibility in determining and using the most effective means to disseminate information gained from event analyses to the industry.

Section 808.2 has a similar amendment to §807g as described immediately above.

G. Section 1000 – Situation Awareness and Infrastructure Security

Section 1002 has been amended to state NERC's new policy regarding maintenance and financial support of existing and potential new reliability tools and support services. NERC will work with industry to identify new tools, collaboratively develop requirements, support development, provide an incubation period, and at the end of that period transition the tool or service to another group or owner for long term operation of the tool or provision of the service. NERC may also develop reliability tools on its own, but will consult with industry concerning the need for the tool prior to development. Tools and services being maintained by NERC as of January 1, 2012 will be reviewed and, as warranted, transitioned to an appropriate industry group or organization.

H. Section 1200 – Regional Delegation Agreements

Section 1208 – The title is revised to delete the word "Audits," thereby correcting a previous scrivener's error.

I. Section 1400 – Amendments to the NERC Rules of Procedure

Section 1401 is revised to provide that requests to amend or repeal the ROP may be submitted by (among other sources) (i) fifty (rather than ten) members of NERC, which must include members from at least three membership sectors (rather than "segments"), (ii) a committee (rather than "standing committee") of NERC, or (iii) an officer of NERC (rather than of "the ERO"). These revisions are necessary to correct inconsistencies with Article XI, section 2 of the NERC Bylaws.

Section 1403 is deleted and its subject matter, which is more appropriately placed in ROP §300, is moved to §320.3.

J. Section 1500 – Confidential Information

Section 1502.1 is revised to correct an existing typographical error.

II. Appendix 3C – Procedure for Coordinating Reliability Standards Approvals, Remands, and Directives

NERC is proposing to delete Appendix 3C as no longer necessary. Appendix 3C was originally developed in response to directives in P 286 of the Commission's July 2006 ERO Certification Order, concerning coordination among the applicable North American regulatory bodies with authority over development and approval of reliability standards for the bulk power system, specifying that NERC should identify the relevant regulatory bodies and their respective standards approval and remand processes that will be implicated in any remand of a proposed reliability standards, and specify the actual steps to coordinate all of these processing requirements, including those that may be necessary for an expedited deadline to return a remanded proposed reliability standards. As NERC has continued, subsequent to 2006, in its efforts to gain recognition as the ERO and adoption of mandatory reliability standards in the Canadian provinces and Mexico, the requirements and processes applicable to adoption and revision of reliability standards in the non-U.S. jurisdictions have been established by legislation or regulation with those jurisdictions or by memoranda of understanding between NERC and the applicable governmental authorities. As the concerns underlying the directives in P 286 of the ERO Certification Order are now addressed through legislation, regulation, or memoranda of understanding in or with the non-U.S. applicable governmental authorities, Appendix 3C can be deleted.

III. Appendix 4B – Sanction Guidelines

A principal objective of the proposed amendments to Appendix 4B is to eliminate text that does not relate to the purpose of the Sanction Guidelines, namely, how penalties and sanctions for violations of reliability standards are determined, and to eliminate internally duplicative or repetitive text. The following portions of Appendix 4B are being completely or substantially deleted consistent with this objective: (1) current section 2, Document Scope and Exclusions; (2) current §3.1, Necessary Elements of NERC Compliance Program; (3) current §3.2, Settlement of Compliance Violations, as well as the current sections captioned "Settlement Request" and "Settlement Effect on Continuation of Determination of Penalties, Sanctions, or Remedial Actions;" (4) current §3.7, "No Influence of Penalty, Sanction or Remedial Action Upon Violation Confirmation Process;" and (5) current §6, "Remedial Action" (remedial action directives are covered in §7.0 of Appendix 4C); as well as portions of the texts of other sections.

Text paraphrasing or referring to various statutory provisions and Commission regulations and orders has also been deleted, as these authorities speak for themselves; however, a statement has been added in §1 that "NERC and the regional entities will apply the provisions of this document in accordance with applicable statutory provisions and with the regulations, orders, and statements of policy of FERC and other ERO governmental authorities that are applicable to the determination and imposition of penalties and sanctions for violations of reliability standards in the respective jurisdictions."

Revisions have been made throughout Appendix 4B for more consistent use of terms within the document and as used elsewhere in the ROP, such as remedial action directive, possible violation, alleged violation, and registered entity.

In current §3.2/renumbered §2.1, text is retained specifying that provisions in a settlement agreement regarding penalties or sanctions can supersede any corresponding penalties or sanctions that would otherwise be determined pursuant to the Sanction Guidelines.

In renumbered §2.5, "Multiple Violations," text has been added to state that where penalties or sanctions for several unrelated violations by an entity are being determined at the same time, NERC or the regional entity may determine and issue a single aggregate penalty or sanction bearing a reasonable relationship to the aggregate of the violations. This is consistent with long-standing practice.

In renumbered §3.2.2, which discusses how the fact that a violation is a registered entity's first violation will be considered in determining (reducing or excusing) the Base Penalty Amount, text has been added to provide that this relief generally will not be afforded if NERC or the regional entity determines the violator has a poor internal compliance program or culture of compliance (as well as a poor compliance record, as stated in the existing text). This is consistent with longstanding practice,

and also consistent with the increased emphasis NERC is placing in compliance monitoring and enforcement activities on the registered entity's internal compliance program and culture of compliance.

In renumbered §3.3, which lists adjustment factors that will be considered in determining the penalty after the Base Penalty Amount is established, subpart c lists as an adjustment factor disclosure of the violation by the violator through self-reporting, or as the result of a compliance self-analysis following a bulk power system event, and voluntary mitigating activities (which is a broader term than the current "corrective action") by the violator. Subpart d, which refers to the degree and quality of cooperation by the violator in the investigation, has been amended to include reference to the violator's cooperation in an event analysis concerning, and the performance of a compliance self-analysis by the violator following, a BPS event in which the violation occurred or to which it related. The references to cooperation in the analysis of, and performance of a compliance self-analysis following, a system event, is consistent with proposed amendments to Appendix 8 to reflect expectations that registered entities will conduct self-analyses of system events in which they are involved. In subpart f, "settlement" has been added as an explicit adjustment factor.

In renumbered §3.3.1, which discusses repetitive violations and the violator's compliance history as an adjustment factor, text has been added to state that in evaluating the violator's compliance history, NERC or the regional entity will take into account previous violations by affiliates of the violator, particularly violations of the same or similar reliability standard requirements, and will evaluate whether any such prior violations reflect recurring conduct by affiliates that are operated by the same corporate entity or whose compliance activities are conducted by the same corporate entity. This addition is consistent with a 2010 guidance order from FERC, and should also promote the sharing of compliance information and lessons learned between registered entities that are corporate affiliates.

Also, in renumbered §3.3.1, the term "violation reset time period" has been changed to "reset period or reset time frame," as these are the terms used in several reliability standards.

Renumbered §3.3.3, retitled "Disclosure of the Violation Through Self-reporting and Voluntary Mitigating Activities by the Violator," has been revised consistent with subpart c of §3.3.3 as described above. In addition, the following text has been added: "If a self-report or a self-certification submitted by the violator accurately identifies a violation of a Reliability Standard, an identification of the same violation in a subsequent compliance audit or spot check will not subject the violator to an escalated penalty as a result of the compliance audit process unless the severity of the violation is found to be greater than reported by the violator in the self-report or self-certification." A similar statement is currently contained in §3.0 of Appendix 4C, but it is being moved to Appendix 4B as it more appropriately relates to penalty determinations than to compliance monitoring processes.

Renumbered §3.3.4, retitled "Degree and Quality of Cooperation," has been revised consistent with subpart d of §3.3 as described above.

Renumbered §3.3.5, retitled "Presence and Quality of the Violator's Internal Compliance Program," has been revised to add reference to "other indicators of the violator's culture of compliance" as an adjustment factor.

Section 3.3.6, "Settlement," has been added consistent with the addition of subpart f in §3.3 as described above.

Renumbered §3.3.7, retitled "Violation Concealment and Responsiveness," has been revised to state that NERC or the regional entity shall consider an increase to the penalty if NERC or the regional entity determines, based on its review of the facts, that the violator resisted or impeded the discovery and review of a violation.

In numerous other areas of Appendix 4B, revisions have been made for the purpose of simplifying the text. The text of current Appendix 4B is extremely elaborate and the simplification of the text will make the document easier to use for all participants. As part of this effort, in numerous places text has been revised to state that "NERC and the regional entity will do X," rather than the current text structure of "X will occur" or "X will be taken into account."

IV. Appendix 4C – Compliance Monitoring and Enforcement Program

Throughout Appendix 4C, "Regional Entity" has been revised to "Compliance Enforcement Authority" (CEA in this summary) in numerous places. In addition, since sections have been added and deleted and, as a result, other sections have been renumbered in this Appendix, there are revisions throughout the Appendix to change cross-references.

A. Section 1.0 -- Introduction

Section 1.1 – Definitions – A cross-reference has been added to incorporate definitions in Section 1500 of the ROP.

Section 1.1.2 – Annual Audit Plan – reference to including "Compliance Audit Participant Requirements" in the Annual Audit Plan has been deleted.

Section 1.1.9 – Confirmed Violation – the definition has been expanded to more comprehensively capture the circumstances that constitute a "Confirmed Violation," based on experience, and will include entry into a settlement agreement.

Section 1.12 – ISO/RTO – added new definition that is used in new §5.11 (described below).

Section 1.1.13 (renumbered) – Mitigation Plan – Text not necessary to define the term is being deleted.

Section 1.1.16 (renumbered) – The defined term "Notice of Alleged Violation" is changed to "Notice of Alleged Violation and Proposed Penalty or Sanction," which is the term more commonly used; Notices of Alleged Violation typically include a proposed penalty or sanction.

Section 1.1.18 (renumbered) – Notice of Confirmed Violation – text is deleted that is not necessary to define "Notice of Confirmed Violation." The subject matter of the deleted text is covered (more appropriately) in the definition of "Confirmed Violation."

Section 1.19 (renumbered) – Notice of Penalty – added the phrase Notice "or other notification" of Confirmed Violation to reflect that Regional Entities may sometimes provide notice of a Confirmed Violation through a means of notification other than a Notice of Confirmed Violation.

Section 1.1.22 (renumbered) – Possible Violation – text is deleted that is not necessary to define the term, and potentially inaccurate (a Possible Violation could be identified by a means other than one of the compliance monitoring and enforcement processes enumerated in Section 3.0).

Section 1.1.24 (renumbered) – Preliminary Screen – an additional component is added to the determinations to be made in the Preliminary Screen: "if known, the potential noncompliance is not a duplicate of a Possible Violation or Alleged Violation which is currently being processed."

Section 1.1.24 (renumbered) – Public Notification List – Added new definition that is used in new §5.11 (described below).

Section 1.1.25 (renumbered) – Regional Implementation Plan – revised to reflect that the Regional plans are now to be submitted to NERC by October 1 (rather than November 1) of the preceding year.

Section 1.1.27 (renumbered) – Remedial Action Directive – revised to state that a Remedial Action Directive is immediately necessary to protect the reliability of the Bulk Power System from an imminent or actual threat.

Section 1.1.29 (renumbered) – Self-Certification – Definition is expanded to reflect that additional possible responses to a self-certification request will be allowed, *i.e.*, that the Registered Entity does not own facilities that are subject to the Reliability Standard requirement, or that the Reliability Standard requirement is not applicable to the Registered Entity.

Section 1.1.30 (renumbered) – Self-Report – (1) The defined term is changed from Self-Reporting to Self-Report (this revision is made throughout the document). (2) Definition is revised to provide that the Self-Report may state that the Registered Entity believes it has, or may have, violated a Reliability Standard. This will enable a Registered Entity to submit a Self-Report without having to conclude that it has violated a Reliability Standard. (3) The provision that the Self-Report should state the actions

that have been taken or will be taken to resolve the violation is deleted; this requirement could delay submission of a Self-Report while the Registered Entity determines what actions are to be taken.

Section 1.1.31 (renumbered) – Spot Check – (1) The defined term is changed from Spot Checking to Spot Check (this revision is made throughout the document). (2) In the third basis stated in the definition on which a Spot Check may be initiated, reference to "events, as described in the Reliability Standard" is deleted and "risk-based assessments" is added. The addition is consistent with NERC's developing risk-based assessment approach to determining the frequency with which to conduct compliance monitoring activities.

B. Section 2.0 – Identification of Organizations Responsible for Complying with Reliability Standards

Section 2.0 is revised to specify that a Registered Entity must inform NERC or the applicable Regional Entity promptly of changes to the Registered Entity's compliance information "including planned or completed changes in ownership of Bulk Power System facilities, registration status, address or other contact information, and name of designated compliance contact." Experience has indicated that NERC and the Regional Entities are not receiving timely notification of such information, which may affect registration status, identification of the correct/current Registered Entity, or the ability to contact the Registered Entity.

Detailed text concerning disclosure of confidential compliance information to FERC and other Applicable Governmental Authorities has been deleted here (and in other sections where it was repeated), and replaced with: "Any such provision of information to FERC or to another Applicable Governmental Authority shall be in accordance with Section 8,0, Reporting and Disclosure." The complete text of this provision will now appear in one section (Section 8.0).

C. Section 3.0 – Compliance Monitoring Processes

In the title of Section 3.0, reference to "Enforcement" is deleted; and in the first sentence of the section, "assess and enforce" is deleted. Section 3.0 encompasses only compliance monitoring processes, while Section 5.0 encompasses enforcement.

Throughout Section 3.0, footnotes stating that a particular compliance process normally completes within a specified time period have been deleted; the time required to complete individual compliance processes has varied widely based on particular facts and circumstances.

Text has been added in the first paragraph of the section stating that scheduled compliance monitoring processes will be conducted in accordance with NERC and Regional Annual Implementation Plans and individual entity audit plans; and that compliance monitoring processes can also be initiated on an unscheduled basis as needed, based on factors such as those enumerated in the text, such as the

compliance history of the Registered Entity and the quality of its internal reliability compliance program. This text is consistent with NERC's developing risk-based assessment approach to compliance monitoring.
Text has been added to state that if a potential noncompliance is identified through one of the compliance monitoring processes described in Section 3.0 or through another means, the Compliance Enforcement Authority (CEA) will conduct a Preliminary Screen of the information in accordance with Section 3.8; if the Preliminary Screen results in an affirmative determination with respect to the Preliminary Screen criteria, a Possible Violation exists and the CEA will proceed in accordance with Section 5.0, Enforcement Actions.

Text describing the enforcement actions that may be taken by the CEA is deleted, as this topic is covered in Section 5.0, not in this section.

Text is added to state that the CEA has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security procedures conforming to ROP Section 1500 and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost if the information were placed into the public domain.

This section is revised to state that a Registered Entity that believes a request for documents, data or information is unreasonable may request a determination from the NERC General Counsel (changed from the NERC "compliance program officer").

Section 3.1 – Compliance Audits – Revised to state that Generally Accepted Auditing Standards, Generally Accepted Government Auditing Standards, and standards sanctioned by the Institute of Internal Auditors, are examples of professional auditing standards on which Compliance Audit processes for Compliance Audits in the U.S. should be based.

Section 3.1.1 – Compliance Audit Process Steps – (1) The first step is revised to state that the Annual Audit Plan will be posted, rather than distributed to all Compliance Audit Participants. (2) The second step is revised to provide that the CEA will notify the Registered Entity of the Compliance Audit and the Reliability Standards to be evaluated, 90 days (rather then 2 months) prior to commencement of a regularly scheduled Compliance Audit. (3) The fourth step is revised to delete the statement that the audit team will review the Registered Entity's submitted information "prior to performing the Compliance Audit" – the submitted information may be reviewed before or during the on-site audit activities. Text stating that the audit team "follows NERC audit guidance in the implementation of the Compliance Audit" is also deleted here, as this statement is applicable to all the process steps. (4) The fifth step is revised to state that the audit reported will be completed in accordance with Section 3.1.6,

which addresses the form and contents of the audit report. (5) A step has been added that if the audit team identifies evidence of a potential noncompliance, the CEA will conduct a Preliminary Screen in accordance with Section 3.0. Other process steps describing enforcement actions are deleted here, since enforcement processes are covered in Section 5.0.

Section 3.1.2 – Compliance Enforcement Authority Annual Audit Plan and Schedule – (1) Revised to state that Registered Entities scheduled for Compliance Audits in a year will be notified by October 1 of the preceding year (rather than by January 1 of the year in which the audit is to be conducted). (2) Text is changed to state that the CEA will give due consideration to schedule changes requested by a Registered Entity "for reasonable cause" (rather than "to avoid unnecessary burden") which will allow a broader basis for justification of schedule change requests.

Section 3.1.3 – Frequency of Compliance Audits – The last sentence is deleted because the subject of objections to the composition of the audit team is covered in Section 3.1.5.4.
Section 3.1.4.1 – Reliability Standards – Revised to clarify that a Compliance Audit may include other standards applicable to the Registered Entity, that are not identified in the NERC Implementation Plan, whether or not the other standards are identified in the Regional Entity's Implementation Plan.

Section 3.1.4.2 – Period Covered – (1) Revised to emphasize that the Registered Entity's data and information must show compliance with the standards being audited for the entire period covered by the Compliance Audit. (2) Text is added to state that the CEA will indicate the beginning and End Date of the audit period in its notice of the Compliance Audit. (3) Revised to state that the start of the audit period will be the End Date of the previous Compliance Audit (which may be a different date than the last day of the previous Compliance Audit). (4) The existing second sentence of this section, concerning modification of the audit period, is deleted and replaced with a more straightforward sentence ("The Compliance Enforcement Authority may modify the beginning date of the audit period for any given Reliability Standard requirement based on an intervening compliance monitoring process."). (5) Text is revised to state that the End Date may be a predetermined specific date or may be stated generally as the last day of the Compliance Audit.

Section 3.1.4.3 – Review of Mitigating Activities – The term "Mitigation Plan" is replaced with "mitigating activities." "Mitigating activities" is a broader term, reflecting that actions taken by a registered entity to correct and prevent recurrence of a noncompliance, while they are accepted by the CEA, are not always memorialized in a formal Mitigation Plan.

Section 3.1.5.1 – Composition of Compliance Audit Teams – (1) Revised to state that the audit team will be comprised of members who the CEA has determined to have the requisite knowledge, training, and skills to conduct the Compliance Audit. (2) Revised to clarify who may be included on Compliance Audit teams, in addition to staff of the Regional Entity: (i) contractors and industry subject matter experts, (ii) NERC staff members (which may include contractors to NERC), (iii) compliance staff

members of other Regional Entities, and (iv) representatives of FERC and of other Applicable Governmental Entities that have reliability jurisdiction with respect to the Registered Entity.

Section 3.1.5.2 – Requirements for Compliance Audit Team Members – (1) First bullet is revised to state that audit team members must be free of conflicts of interest "in accordance with Compliance Enforcement Authority policies." (2) Fourth bullet is revised to eliminate the requirement that the CEA provide to the Registered Entity copies of the confidentiality agreements or acknowledgements executed by the audit team members; instead, the CEA will provide confirmation to the Registered Entity that all audit team members have executed confidentiality agreements or acknowledgements.

Section 3.1.5.3 – Compliance Audit Observers and Other Attendees – Revised to clarify the distinctions between audit team members (§3.1.5.1), observes, and attendees. The first paragraph is amended to specify that the following may participate as observers: NERC staff; other members of the Regional Entity's compliance staff; with the Regional Entity's permission, compliance staff members of other Regional Entities; and representatives of FERC and of other Applicable Governmental Entities that have reliability jurisdiction with respect to the Registered Entity. The second paragraph, which is not being revised (and was approved by the Commission in its October 7, 2011 Order) states who may be attendees at the audit. A new third paragraph has been added to state that "Compliance Audit observers and attendees are not audit team members and do not participate in conducting the Compliance Audit or in making audit findings and determinations."

Section 3.1.5.4 – Registered Entity Objections to Compliance Audit Team – (1) Revised to delete "other than a member of NERC or FERC staff" in the sentence "A Registered Entity subject to a Compliance Audit may object to any member of the audit team [deletion] on grounds of a conflict of interest or the existence of other circumstances that could interfere with the team member's impartial performance of his or her duties." NERC (and numerous stakeholders who commented on this provision) believe that while a Registered Entity should not be able to object to participation by NERC staff or FERC staff on a Compliance Audit team (as FERC has indicated in prior orders), a Registered Entity should be allowed to object to the inclusion of a <u>particular individual</u> NERC staff or FERC staff member on the audit team based on conflict of interest, bias or similar specific grounds (*e.g.*, the NERC staff member of FERC staff member is a former employee of the Registered Entity).

Section 3.1.6 – Compliance Audit Reports – (1) In the second line, "evidence of possible noncompliance" is changed to "evidence of potential noncompliance" to avoid confusion with the defined term "Possible Violation." (2) In the first paragraph, the phrase "other mitigating activities" is added to "Mitigation Plan," as not all actions taken by Registered Entities to correct a noncompliance and prevent recurrence are memorialized in formal Mitigation Plans. (3) The first paragraph is also revised to state that the audit report may also state areas of concern and recommendations identified by the audit team (rather than specifying that any recommendations of the audit team be provided in a separate document). (4) In the second paragraph, the first sentence is revised to specify that the CEA will provide the final audit report to the Registered Entity on or before the date the report is provided

to NERC. (5) Text concerning the provision of non-public compliance information to FERC or to another Applicable Governmental Entity is deleted and replaced with a reference to §8.0, where the full text on this topic is provided.

Section 3.2 – Self-Certification – The second paragraph of this section is deleted because its substance has been moved to Appendix 4B, *Sanction Guidelines*, where it is more appropriately placed.

Section 3.2.1 – Self-Certification Process Steps – (1) The first step is revised to specify that the posted reporting schedule should include the applicable reporting periods. (2) The first step is also revised to specify that NERC, along with the CEA, will be responsible to ensure that the appropriate standards, compliance procedures and submittal forms are maintained and available (which may be through a means other than electronic). (3) Consistent with the revised definition of Self-Certification (§1.1.29), the third step is revised to list the four possible responses in a Self-Certification. (4) The fourth step is revised to state that, at a minimum, the CEA will review Self-Certifications of non-compliance and Self-Certifications stating that the Registered Entity does not own facilities that are subject to the Reliability Standard requirement or that the requirement is not applicable to the Registered Entity. (5) The fifth step is revised to state that if the CEA identifies a potential noncompliance, the CEA conducts a Preliminary Screen. (6) A paragraph is added stating that receipt of a Self-Certification by the CEA shall not be construed as a finding by the CEA that the Registered Entity is compliant with, not compliant with, or not subject to, the Reliability Standard requirement. This additional text is intended to negate the assumption that if a CEA makes no further response to a Registered Entity concerning a Self-Certification, the CEA has determined that the Registered Entity is compliant with the Reliability Standard requirement.

Section 3.3 – Spot Check – (1) Revised to state that a Spot Check may be initiated at the discretion of the CEA or as directed by NERC, including on a random schedule. The list of potential reasons is revised to include risk-based assessments based on the Registered Entity's BPS facilities and operations and their significance to the reliability of the BPS and the Registered Entity's compliance history and internal compliance program or other indicators of its culture of compliance. This addition is consistent with NERC's developing program of using risk-based assessments to determine when additional compliance monitoring processes should be initiated, and the scope of the compliance monitoring processes conducted, with respect to a Registered Entity.

Section 3.3.1 – Spot Check Process Steps – (1) The first step is revised to state that a "notification letter" will be issued by the CEA to the Registered Entity, which will include the scope of the Spot Check including the Reliability Standard requirements that will be covered. (2) The second step is revised to state that the notification package will include the names and employment histories of the persons who will perform the Spot Check. It is also revised to state that the CEA shall provide confirmation to the Registered Entity that the Spot Check team members have executed confidentiality agreements or acknowledgements. The second step is also revised to state that the Registered Entity may object to inclusion of any individual on the Spot Check team on the grounds specified in §3.1.5.4,

but that nothing in §3.1 shall be read to limit the participation of NERC staff on a Spot Check team or to limit the participation of FERC staff in a Spot Check of a Registered Entity, or involving a portion of the Bulk Power System, over which FERC has jurisdiction. (3) The third step is revised to specify that the Registered Entity must provide the required information to the CEA by the date specified in the request. (4) The fifth step is revised to state that if the Spot Check team's review of the information submitted indicates a potential noncompliance, the CEA will conduct a Preliminary Screen. (5) The sixth step is revised to state that the Spot Check team will prepare a draft Spot Check report and the Registered Entity will be given ten business days to comment on it. (6) The sixth step is revised to provide that the Spot Check team will consider any corrections based on the Registered Entity's comments, finalize the Spot Check report and provide it to the Registered Entity and to NERC. (7) The step stating that the CEA will send the Registered Entity a Notice of Possible Violation is deleted, as that step will now be covered in Section 5.0, Enforcement Actions.

Section 3.4 – Compliance Investigations – In two places, "possible violation" is replaced with "potential noncompliance" to avoid confusion with the defined term "Possible Violation."

Section 3.4.1 – Compliance Investigation Process Steps – (1) The first step is revised to provide that the CEA will take certain actions within three (rather than within two) business days of the decision to initiate a Compliance Investigation. (2) The second step is revised to provide that within three (rather than two) business days after receiving notice of the decision to initiate a Compliance Investigation, NERC will notify FERC and other Applicable Governmental Authorities. In addition, text concerning the provision of non-public compliance information to FERC or to another Applicable Governmental Entity is deleted and replaced with a reference to Section 8.0, where the full text is provided. (4) The fourth step is revised to provide that the Registered Entity must provide any required information to the CEA by the Required Date as specified in the request. (5) The eighth step is revised to provide that the CEA may review any mitigating activities (in addition to Mitigation Plans), since not all actions taken by a Registered Entity to correct a noncompliance and prevent recurrence are memorialized in a formal Mitigation Plan. (6) The ninth step is revised to provide that if the CEA identifies a potential noncompliance, it will conduct a Preliminary Screen. (7) In the tenth step, text concerning the provision of non-public compliance information to FERC or to another Applicable Governmental Entity is deleted and replaced with a reference to Section 8.0, where the full text is provided.

Section 3.5 – Self-Reports – A sentence is added stating that if possible, and without delaying the Self-Report, a Self-Report may include the actions that have been taken or will be taken to resolve the violation. This addition is consistent with the change to the definition of Self Report (§1.1.30).

Section 3.5.1 – Self-Report Process Steps – (1) The first step is revised to delete reference to the CEA's Web site; the CEA may make the Self-Report submittal forms available through other means. (2) The fourth step is revised to provide that the CEA will conduct a Preliminary Screen of the Self-Report information.

Section 3.6.1 – Periodic Data Submittals Process Steps – (1) The first step is revised to delete reference to the CEA's Web site; the CEA may make the submittal forms available through other means. (2) The third step is revised to provide that the Registered Entity must provide any required information to the CEA by the Required Date as specified in the request. (3) The fifth step is revised to provide that if the CEA's review of the data submittal indicates a potential noncompliance, the CEA will perform a Preliminary Screen. (4) A paragraph is added at the end of this section stating that receipt of a Periodic Data Submittal by the CEA shall not be construed as a finding by the CEA that the Registered Entity is compliant with, not compliant with, or not subject to, the Reliability Standard requirement. This additional text is intended to negate the assumption that if a CEA makes no further response to a Registered Entity concerning a Periodic Data Submittal, the CEA has determined that the Registered Entity is compliant with the Reliability Standard requirement.
Section 3.7 – Exception Reporting – This section is deleted and Exception Reporting will no longer be considered one of the compliance monitoring processes, as exception reports are triggered by requirements of particular Reliability Standard, and not on the initiative of the CEA. However, an exception report containing evidence of a potential noncompliance may still result in performance of a Preliminary Screen and initiation of an enforcement action (see revised Section 2.0).

Section 3.7 (as renumbered) – Complaints – In the first paragraph, text stating that NERC will review any Complaint "that is related to a Regional Entity or its affiliates, divisions, committees or subordinate structures" is deleted. Regional Entities as such are not subject to Reliability Standards; and for those Regional Entities that perform registered functions (FRCC, SPP and WECC), there are in place (or pending before the Commission for approval) agreements by which other Regional Entities, not NERC, perform the CEA responsibilities with respect to the registered functions.

Section 3.8 – Preliminary Screen – (1) The provisions relating to performance of Preliminary Screen are relocated to Section 3.8 from Section 5.1, as the Preliminary Screen is considered a step in the compliance monitoring process (Section 3.0), rather than in the compliance enforcement process (Section 5.0). (2) Section 3.8 states that the Preliminary Screen will be conducted within five business days after the CEA identifies the potential noncompliance, except that (i) if the CEA identifies the potential noncompliance during a Compliance Audit, the Preliminary Screen will be conducted immediately following the exit briefing of the Registered Entity, and (ii) if the CEA identifies the potential noncompliance during a Compliance Investigation, the Preliminary Screen shall be conducted immediately after the Registered Entity is first notified of the potential noncompliance identified by the Compliance Investigation. The two exceptions are necessary so that the Registered Entity does not receive a Notice of Possible Violation before being notified that the Compliance Audit or Compliance Investigation has found a potential noncompliance. (3) Consistent with the change in definition (§1.1.23), the Preliminary Screen will now include a determination of whether, if known, the potential noncompliance is not a duplication of a Possible Violation or Alleged Violation that is currently being processed. (4) The revised section provides that if the Preliminary Screen results in an affirmative determination with respect to the three criteria, a Possible Violation exists and the CEA shall proceed in accordance with Section 5.0.

D. Section 4.0 – Annual Implementation Plans

Section 4.1 – NERC Compliance Monitoring and Enforcement Program Implementation Plans – (1) Revised to provide that the NERC Implementation Plan will be provided to the Regions by on or about September 1 (rather than October 1) of the prior year. (2) Revised to state that NERC may update and revise its Implementation Plan during the course of the year. (3) Revised to state that Regional Entities have discretion to make modifications to the NERC Implementation Plan with respect to individual Registered Entities, based on a determination concerning the Registered Entity's past and current compliance performance.

Section 4.2 – Regional Entity Implementation Plan – (1) Consistent with the revised schedule in §4.1, revised to provide that the Regional Implementation Plans will be submitted on or about October 1 (rather than November 1) of the previous year. (2) Revised to state that a Regional Entity may update and revise its Implementation Plan during the year as necessary, with NERC approval or as directed by NERC. (3) Revised to state that Regional Entities have discretion to make modifications to their Implementation Plans with respect to individual Registered Entities, based on a determination concerning the Registered Entity's past and current compliance performance.

E. Section 5.0 – Enforcement Actions

In the first paragraph of §5.0, "remedial actions" is replaced with "mitigating activities," to avoid possible confusion with the defined term Remedial Action Directive.

A statement is added that imposition and acceptance of penalties and sanctions shall not be considered an acceptable alternative to a Registered Entity's continuing obligations to comply with Reliability Standards.

Text is added to state that the CEA has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security procedures conforming to ROP Section 1500 and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost if the information were placed into the public domain.

This section is revised to state that a Registered Entity that believes a request for documents, data or information is unreasonable may request a determination from the NERC General Counsel (changed from the NERC "compliance program officer").

A statement is added that under the circumstances presented by some Possible Violations, Alleged Violations or Confirmed Violations, absolute adherence to the enforcement process in §5.0, to the exclusion of other approaches, may not be the most appropriate, efficient or desirable means by which to achieve the overall objectives of the Compliance Program for NERC, the CEA and the Registered Entity; in such circumstances, other approaches may be considered and employed. A similar statement is found in current Appendix 4B, but is being deleted there, as it is more appropriately placed in Appendix 4C.

Section 5.1 – Preliminary Screen – This section is deleted and the topic is now covered in Section 3.8 (as discussed above).

Section 5.1 – Notice of Possible Violation – (1) Revised to state that the Notice of Possible Violation will state the dates involved in the Possible Violation "if known." (2) Revised to state that the CEA will report the Possible Violation to NERC (rather than entering it into the compliance reporting and tracking system – it is not necessary to specify the particular reporting mechanism to be used). (3) Revised to state that NERC will report the Possible Violation to other Applicable Governmental Authorities, as applicable (in addition to FERC), in accordance with §8.0, Reporting and Disclosure.

Section 5.3 – Notification to Registered Entity of Alleged Violation – (1) Revised to provide that the CEA will notify the Registered Entity of the determination of an Alleged Violation, even if the CEA and the Registered Entity have entered into settlement negotiations. (2) Revised to state that the CEA will issue a Notice of Alleged Violation and Proposed Penalty or Sanction "or similar notification," to recognize that some Registered Entities' processes may involve providing notification through a different means than a Notice of Alleged Violation and Proposed Penalty or Sanction. Similar revisions are made in other sections. (3) Revised to state that the notification of Alleged Violation will be issued by e-mail and will be effective as of the date of the electronic mail message; this will promote consistency in the methods of delivering notification. Also, the requirements that the notification be signed by an officer or designee of the CEA, and be sent to the CEO of the Registered Entity, are deleted; the notification will be sent to the Registered Entity's compliance contact. (4) Revised to state that the CEA will report the Alleged Violation to NERC (rather than entering it into the compliance reporting and tracking system – it is not necessary to specify the particular reporting mechanism to be used). (5) In item (v) of the list of contents of a notification of Alleged Violation, "or other mitigating activities" is added after "implement a Mitigation Plan," to reflect that some actions taken by Registered Entities to correct and prevent recurrence of a noncompliance, although they are approved by the CEA, are not memorialized in a formal Mitigation Plan. (6) In item (vii) of the list of contents of a notification of alleged violation, "full hearing procedure" is changed to "general hearing procedure" consistent with a revision in the Hearing Procedures. (7) Text concerning the provision of non-public compliance information to FERC or another Applicable Governmental Entity is deleted and replaced with a reference to §8.0, where the full text is provided. (8) The last paragraph of this section is deleted, as completion of the enforcement action and issuance of a Notice of Confirmed Violation is covered in later sections.

Section 5.4 – Registered Entity Response -- (1) Revised to add agreement by the Registered Entity with the notification of Alleged Violation as establishing acceptance of the CEA's determination of violation and penalty or sanction. (2) Revised to provide that the 30 day period runs from the date of notification of Alleged Violation by electronic mail (consistent with a revision to §5.3, above). (3) Revised to state that the CEA will issue a Notice of Confirmed Violation "or similar notification," to recognize that some Registered Entities' processes may involve providing notification through a different means than a Notice of Confirmed Violation. Similar revisions are made in other sections. (4) Revised to state that the CEA will report the Confirmed Violation to NERC (rather than entering it into the compliance reporting and tracking system – it is not necessary to specify the particular reporting mechanism to be used). (5) Revised to state that the Registered Entity will be allowed to provide a written explanatory statement to accompany the filing with FERC and public posting of the Confirmed Violation. (6) Revised to state that if the Registered Entity contests the Alleged Violation or proposed penalty or sanction, it must submit a response within 30 days following the date of notification of the Alleged Violation. (7) Reference to issuing a Notice of Confirmed Violation by the CEA is deleted, as this topic is covered in a subsequent section.

Section 5.6 – Settlement Process -- (1) Revised to provide that the Registered Entity or the CEA may terminate settlement negotiations at any time. Either party should have discretion to terminate settlement negotiations if they are not progressing in a productive manner. (2) Revised to provide that the time for the Registered Entity to respond to the notification of Alleged Violation pursuant to §5.4 is suspended during settlement negotiations. (3) Revised to state that the CEA and the Registered Entity will execute a settlement agreement (rather than that the CEA will issue a letter) setting forth the final settlement terms. (4) Revised to state that within five business days after NERC advises the CEA of NERC's approval, rejection or proposed revisions to a settlement agreement, the CEA will notify the Registered Entity. Notification to the Registered Entity should come from the CEA, not from NERC which has not been in negotiation or other contact with the Registered Entity. (5) Text concerning the provision of non-public compliance information to FERC or another Applicable Governmental Entity is deleted and replaced with a reference to §8.0, where the full text is provided. (6) Text is added to clarify that in the public posting of the settlement agreement or of the terms of the settlement, any Critical Energy Infrastructure Information or Confidential Information will be redacted.

Section 5.7 – NERC Appeal Process – Revised to provide that the CEA, as well as the Regional Entity, may appeal the decision of the Regional Entity hearing body, in accordance with amended Section 409 of the ROP.

Section 5.9 – Notice of Penalty – (1) Revised to provide that the Registered Entity shall be informed that the Notice of Penalty is pending public filing at least five business days prior to the public filing and posting. (2) Text concerning the provision of non-public compliance information to FERC or another Applicable Governmental Entity is deleted and replaced with a reference to §8.0, where the full text is provided.

Section 5.10 – Completion of Enforcement Action – The title of this section is revised from "Closure of Enforcement Action."

Section 5.11 -- Special Procedures for an Enforcement Action Against an ISO/RTO Where the Monetary Penalty May be Allocated by the ISO/RTO to Other Entities – This is a new section to establish procedures pursuant to which (1) an ISO/RTO can request the CEA to make a determination, during the enforcement process for a Notice of Possible Violation issued to the ISO/RTO, that one or more specified other entities were responsible, in whole or on part, for actions or omissions that caused or contributed to the violation (if approved), and (2) the specified other entity(ies) can request and be allowed to participate in the enforcement process.

Section 5.11.1 specifies that NERC will maintain on its website, based on information to be provided by the ISO/RTO, a Public Notification List of Entities that an ISO/RTO contends it has authority to allocate to, pursuant to a proceeding under §205 of the Federal Power Act, some or all of a monetary penalty imposed on the ISO/RTO for a violation of a Reliability Standard. Pursuant to §5.11.3, the ISO/RTO will not be allowed to invoke the procedures of §5.11, and the CEA will not make the requested determination, with respect to another Entity that was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation to the ISO/RTO, unless the ISO/RTO demonstrates and the CEA concludes that there are extraordinary circumstances that warrant the CEA making the requested determination with respect to the specified other Entity(ies).

Section 5.11.2 specifies that in order to request the CEA to make a determination in an enforcement action that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to a violation (if confirmed) of a Reliability Standard for which the ISO/RTO has received a Notice of Possible Violation, the ISO/RTO shall, no later than five business days after receiving the Notice of Possible Violation (i) submit a written request to the CEA and (ii) issue a notice to the specified other Regional Entity(ies). Section 5.11.2 contains the content and delivery requirements for the ISO/RTO's request and notice. Pursuant to §5.11.3, upon verifying that the specified other entity(ies) were on the Public Notification List as of the date of issuance of the Notice of Possible Violation, that the ISO/RTO has authority to allocate all or a portion of any monetary penalty to the other entity(ies), and that the other entity(ies) received a timely notice from the ISO/RTO in accordance with §5.11.2, the CEA will contact the other entity(ies) to provide further information concerning their right to participate in the enforcement process for the Notice of Possible Violation. In order to participate in the enforcement process, the other entity(ies) will be required to submit a written request to participate and to execute a nondisclosure agreement. The specified other entity(ies) must request to participate in the enforcement process prior to, as applicable (i) the date of execution of a settlement agreement between the CEA and the ISO/RTO, and (ii) the date that the CEA issues a Notice of Confirmed Violation to the ISO/RTO. Pursuant to §5.11.5, upon receiving notice from the CEA that it is allowed to participate in the enforcement action, the specified other entity may

participate in the same manner as the ISO/RTO and shall be subject to all applicable requirements and deadlines specified in the Compliance Program.

Section 5.11.6 provides that, assuming all the precedent conditions described above have been met, and if the enforcement action is not resolved by a settlement agreement stating whether or not the specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, the CEA shall make, and include in its proposed Notice of Penalty, its determination of whether or not the specified other entity(ies) were responsible, in whole or in part, for actions or omissions that caused or contributed to the violation.

Section 5.11.7 provides that if an ISO/RTO's tariffs, agreement or other relevant governance documents establish procedures, that have been approved by FERC, that allow members of the ISO/RTO to directly assign to the ISO/RTO monetary penalties imposed on the ISO/RTO member(s) for violations of Reliability Standards, then the ISO/RTO members may follow the same requirements of §5.11.2, 511.3 and 511.5 as are applicable to an ISO/RTO under those sections, and the ISO/RTO shall be afforded the same rights to participate in the enforcement action as a specified other entity under §5.11.2, 5.11.3, 5.11.5 and 5.11.6, subject to the same requirements and conditions specified in those sections.

Section 5.11.8 specifies that the ISO/RTO shall be obligated and responsible to pay any monetary penalty imposed by the CEA on the ISO/RTO for violation of a Reliability Standard, in accordance with §5.10 of Appendix 4C, (i) regardless of whether the CEA has made a determination that a specified other entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation, (ii) without regard to the timing of any separate proceeding(s) in which the ISO/RTO seeks to allocate some or all of the monetary penalty to a specified other entity(ies), and (iii) without regard to whether or when the ISO/RTO receives payment from the specified other entity(ies). This provision obligates the ISO/RTO to pay any penalty imposed on it for violation of a Reliability Standard within the time period specified in §5.10, without regard to whether or when the ISO/RTO has received payment from any other entity to which the ISO/RTO is seeking to allocate all or a portion of the penalty.

F. Section 6.0 – Mitigation of Violations of Reliability Standards

Text is added to state that the CEA has authority to collect documents, data and information in the manner it deems most appropriate, including removing copies of documents, data and information from the Registered Entity's location in accordance with appropriate security procedures conforming to ROP Section 1500 and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost if the

information were placed into the public domain.

This section is revised to state that a Registered Entity that believes a request for documents, data or information is unreasonable may request a determination from the NERC General Counsel (changed from the NERC "compliance program officer").

Section 6.2 – Contents of Mitigation Plans – Revised to eliminate the requirement that the representative of the Registered Entity who signs the Mitigation Plan shall be (if applicable) the person that signed the Self-Certification or Self-Report submittal. The Mitigation Plan must be signed by an officer, employee, attorney or other authorized representative of the Registered Entity.

Section 6.3 – Timetable for Completion of Mitigation Plans – (1) Detailed text concerning the timing by which a Mitigation Plan should be completed is deleted and replaced with "shall be completed in accordance with its terms." (2) Examples of grounds on which the completion deadline may be extended are revised to include specific operational issues such as the ability to schedule an outage to complete mitigating activities and construction requirements that require longer to complete than originally anticipated.

Section 6.4 – Submission of Mitigation Plans – Revised to provide that a Mitigation Plan may be reflected in a settlement agreement or Notice of Penalty (in addition to the option of being submitted as a separate document). This is consistent with longstanding practice, *e.g.*, that the terms of the Mitigation Plan are often included in the settlement agreement rather than in a separate "Mitigation Plan" document.

Section 6.6 – Completion/Confirmation of Implementation of Mitigation Plans – (1) Revised to delete reference to the CEA verifying that the Registered Entity is in compliance with the requirements of the Reliability Standard a noncompliance with which led to the Mitigation Plan. The CEA will only be required to verify that all required actions in the Mitigation Plan have been completed. (2) Revised to state that the Regional Entity will provide to NERC the quarterly status reports from Registered Entities on progress in completing Mitigation Plans, "upon request by NERC" (rather than as a matter of course).

G. Section 7.0 – Remedial Action Directives

Consistent with the revision to the definition of Remedial Action Directive (§1.1.27), this section is revised to state that a Remedial Action Directive is issued when the action is immediately necessary to protect the reliability of the BPS from an imminent or actual threat.

The third paragraph is revised to remove the text that the CEA shall consult the Reliability Coordinator for the Registered Entity "to ensure that the Remedial Action Directive is not in conflict with directives issued by the Reliability Coordinator," *i.e.*, the consultation will not be limited to this topic.

The fourth paragraph is revised to expand the information to be included in a notice of Remedial Action Directive, including the requirement the CEA is imposing to remove the threat to reliability of the BPS; a schedule for specific periodic updates to the CEA on progress to achieving compliance; and a statement that the Registered Entity is in a state of noncompliance with the Reliability Standard until the requirements of the Remedial Action Directive are completed and certified complete by an officer of the Registered Entity.

The fifth paragraph is revised to provide that the notice of the Remedial Action Directive that is delivered by electronic mail shall be sent to both the Registered Entity's CEO and its designated contact person for reliability matters; and that the notice will be deemed received on the earlier of the actual date of receipt of the electronic submission or receipt of the express courier delivery of the notice as specified by the courier service's verification of delivery.

The sixth paragraph is revised to specify that the CEA will copy NERC on all correspondence sent to the Registered Entity.

H. Section 8.0 – Reporting and Disclosure

This section is revised to contain two subsections, as described below.

Section 8.1 – Information to be Reported -- This section lists the information to be provided by Regional Entities to NERC via electronic reports. A sentence is added that NERC will work with Regional Entities to specify form, content, timing and method of submitting reports and notices. The revised list of information to be reported includes the status of the review and assessment of all Possible Violations, Alleged Violations and Confirmed Violation; the potential impact of any Alleged Violation of Confirmed Violation on the reliability of the BPS; and the name of a Regional Entity staff person knowledgeable about the information to serve as a point of contact, as well as other information specific in current §8.0.

Section 8.2 – Reporting to Applicable Governmental Authorities and Public Disclosure -- Text concerning procedures for the disclosure of non-public U.S. compliance information to Applicable Governmental Authorities other than FERC, and disclosure of non-public non-U.S. compliance information to FERC, which is currently found in several sections of Appendix 4C, has been placed into §8.2 and deleted from all other sections. As described above with respect to the revisions to other sections in which this text is being deleted, it is replaced with a reference to §8.0. This section is also revised to state that NERC will publicly post on its web site each Notice of Penalty, with any Critical Energy Infrastructure Information or Confidential Information redacted, when NERC files the Notice of Penalty with FERC pursuant to §5.9.

I. Section 9.0 – Data Retention and Confidentiality

There are no changes to Section 9.0 other than changes in capitalization of terms and changes in certain terms to be consistent with the changes to those terms elsewhere in Appendix 4C.

V. Attachment 1 to Appendix 4C – Process for Non-Submittal of Requested Data

In Attachment 1 to Appendix 4C, the process steps that the CEA will follow for non-submittal of requested or required data have been revised. The revised text more clearly sets forth the three steps that will be followed, including the two additional notifications that will be issued and to whom they will be issued, if the Registered Entity fails to provide data, information or reports requested in a compliance monitoring or enforcement process by the Required Date.

VI. Attachment 2 to Appendix 4C – Hearing Procedures

Throughout Appendix 2, (1) references to "[HEARING BODY]" (which were originally intended to allow each Regional Entity to insert the name of its Hearing Body) have been replaced with "Hearing Body;" and (2) references to provisions within Attachment 2 have been changed from "Paragraph" to "Section." Additionally, in numerous sections, the text has been divided into lettered subsections ((a), (b), (c), etc.).

A. Section 1.1 -- Applicability, Definitions and Interpretation

Section 1.1.1 – Procedure Governed – (1) Subsection (b) is revised to provide that where the Hearing Body is comprised, in whole or in part, of industry stakeholders, the composition of the hearing body shall be such that no two industry segments may control, and no single industry segment may veto, any decision by the Hearing Body; and where the Hearing Body is comprised solely of independent members and an independent Hearing Officer, decisions shall require a majority vote. This revision is intended to accommodate NPCC's new Hearing Body composition which was recently approved by the Commission. (2) A new subsection (d) has been added providing that if a final order has been entered by the Hearing Body, or the Hearing Body has issued a ruling determining that there are no issues to be decided regarding the Alleged Violation, proposed Penalty amount, proposed Mitigation Plan or proposed Remedial Action Directive, or the Registered Entity and the CEA have entered into a settlement agreement resolving the matters that are the subject of the hearing, the hearing shall be terminated by the Hearing Body and no further proceedings shall be conducted.

Section 1.1.2 – Deviation -- A reference to the Hearing Officer "as defined in Paragraph [now Section] 1.1.5 has been deleted as unnecessary.

Section 1.1.4 – Interpretation – A new subsection (b) is added to provide that "Any ruling, order or decision of the Hearing Officer referenced in these Hearing Procedures shall be made by the Hearing Body where the composition of the Hearing Body consists of independent members and an

independent Hearing Officer." This additional text is intended to accommodate NPCC's new Hearing Body composition which the Commission has recently approved; it avoids a situation in which the Hearing Officer, as a member of the Hearing Body, would be required to review his or her own decisions.

Section 1.1.5 – Definitions – (1) The definition of "Clerk" is expanded to identify his/her duties ("perform administrative tasks relating to the conduct of hearings as described in these Hearing Procedures"). (2) The definition of "Director of Compliance" is expanded to include an individual designated by the CEA (regardless of title) who is responsible for management and direction of the Compliance Staff. (3) Two new definitions are added, "Evidentiary Hearing" and "Testimonial Hearing." An Evidentiary Hearing is a hearing at which one or more Participants submit evidence for the record, while a Testimonial Hearing is an Evidentiary Hearing at which one or more witnesses appear in person to present testimony and be subject to cross-examination. (Corresponding revisions are made throughout the Hearing Procedures as necessary to identify references to hearings as "Evidentiary" or "Testimonial".) (4) A definition of "Hearing Body" is added, consistent with the revision of this term from "[HEARING BODY]" as described above. (5) The definition of "Participant" is revised consistent with the revisions to Section 1.2.12 (described below) that provide for the Hearing Body to be able to grant intervention into the hearing in specific, limited circumstances.

B. Section 1.2 – General Provisions including Filing, Service, Transcription and Participation

Section 1.2.1 – Contents of Filing – In subsection (d) a reference to "documents" is changed to the broader term "evidence."

Section 1.2.3 – Submission of Documents – (1) In subsection (a), the placeholder for insertion of the CEA's regular business hour is deleted and replaced with "during the Compliance Enforcement Authority's regular business hours." (2) In subsection (b), the placeholder for insertion of the CEA's time of close of business is deleted and replaced with "5:00 P.M." (3) In subsection (e), the statement "The signature on a filing constitutes a certificate that the signer has read the filing and knows its contents, and that the contents are true to the best of the signer's knowledge and belief" is deleted, since this topic is now covered in new §1.2.15.

Section 1.2.4 – Service – (1) In subsection (a), the statement that the Registered Entity's "designated agent for service" shall automatically be included on the service list is changed to "compliance contact." (2) In subsection (b), a proviso "subject to the provisions of Section 1.5.10" is added. Section 1.5.10 is the section of the Hearing Procedures on Protective Orders. (3) Subsection (c) is revised to state that the Clerk shall transmit a copy of the record to the ERO at the time the CEA transmits (rather than "serves") to the ERO a Notice of Penalty or a Hearing Body final order that includes a Notice of Penalty.

Section 1.2.8 – Transcripts – (1) The text in subsection (a) is amended to provide that the court reporter shall file a copy of each transcript with the Clerk, and that upon receipt of a transcript from the court reporter, the Clerk shall send notice to the Participants stating that a transcript has been filed by the court reporter, the date or dates of the hearing that the transcript records, and the date the transcript was filed with the Clerk. This filing and notice initiate the time period within which the Participants may file transcript corrections. (2) In subsection (b), the time within which a Participant may file suggested transcript corrections is changed to within 14 days from the date of the Clerk's notice that the transcript has been filed with the Clerk. In addition, this subsection is revised to provide that the Hearing Officer shall only allow changes that conform the transcript to "the statements being transcribed" (rather than suggesting that the testimony given could be revisited).

Section 1.2.11 – Participant Participation – the statement that witnesses shall personally appear at the evidentiary hearing if required by Paragraph 1.6.6 is deleted and replaced with "except as required by Section 1.6.6" (§1.6.6 addresses the requirements for witness attendance at Testimonial Hearings).

Section 1.2.12 – Interventions – (1) The title of this section is changed from "Interventions Are Not Permitted," as the revised section will authorize the Hearing Body to allow intervention under limited, specific circumstances. (2) The section is revised as necessary throughout to reflect that the Hearing Body (as well as FERC) will be allowed to permit interventions. (3) New subsection (b) provides that the Hearing Body may allow a Person to intervene only if the Hearing Body determines that the Person seeking intervention has a direct and substantial interest in the outcome of the Alleged Violation, proposed penalty or sanction, Mitigation Plan, or Remedial Action Directive that is the subject of the proceeding. Two examples of a "direct and substantial interest in the outcome" are provided in the text. Two examples of situations that will not constitute "a direct and substantial interest in the outcome" and will not be grounds on which intervention may be allowed, are also provided in the text (including "seek[ing] to intervene to advocate an interpretation of the Reliability Standard requirement(s) or provision(s) of the *Sanction Guidelines* that are at issue"). (3) Subsections (c), (d) and (e) set forth the procedures and timing requirements for submission of a motion to intervene (including the required contents), responses by other Participants, issuance of a recommendation by the Hearing Officer, and the Hearing Body's decision on the motion to intervene. (4) Subsection (f) authorizes the Hearing Officer or the Hearing Body to stay or suspend the proceedings while a request to intervene filed with the Hearing Body or with FERC, or any appeal of the ruling on the request to intervene, is being resolved. (5) Subsection (g) provides that a Person allowed to intervene shall be deemed to be aligned with the Respondent(s), unless the Hearing Body specifies that the Person intervening shall be aligned with another Participant. (6) Subsection (h) provides that a Person allowed to intervene must take the record and procedural status of the proceeding as it stands on the date the motion to intervene is granted by the Hearing Body. (7) Subsection (i) provides that appeals of decisions of the Hearing Body granting or denying requests to intervene may be appealed to NERC in accordance with ROP §414, and that the notice of appeal must be filed with the NERC director of enforcement no later than seven days following the date of the decision of the Hearing Body granting or denying the intervention.

Section 1.2.14 – Docketing System – Revised to state that a docketed proceeding shall be created upon the filing of a request for hearing (rather than upon issuance of a Notice of Alleged Violation). Docketed hearing proceedings need to be created by the Regional Entity Hearing Body only when a request for a hearing on a matter is filed.

Section 1.2.15 – Representation Deemed to be Made in All Pleadings – This is a new section. It provides that a Participant presenting any pleading to the Hearing Officer or Hearing Body shall be deemed to certify to the best of the Participant's knowledge, information and belief, formed after and based on an inquiry that is reasonable under the circumstances, certain specified matters as to the factual allegations in the pleading, the denials in the pleading of factual allegations made by another Participant, the claims, defenses and other contentions set forth in the pleading, and that the pleading is not being presented for any improper purpose such as to harass, cause unnecessary delay, or needlessly increase the cost incurred by any Participant.

C. Section 1.3 – Initiation of the Hearing Process

Section 1.3.1 – Registered Entity's Option to Request a Hearing – (1) This section has been divided into subsections. (2) In subsection (d), concerning notification in a Notice of Alleged Violation of hearing options, a reference to Section 5.3 of the Compliance Monitoring and Enforcement Program is added. (3) Subsection (e) sets forth the required contents of a Registered Entity's request for hearing, and provides that the Registered Entity may state two or more alternative grounds for its position. (4) Subsection (f) contains the provisions for determining if the general hearing procedure (referred to in the current Hearing Procedures as the "full" hearing procedures) or the shortened hearing procedure will be used, based on the Registered Entity's request and the response by the Compliance Staff and any other Participants (there are no substantive changes to this provision).

Section 1.3.2 – Compliance Staff's Response to Request for Hearing – This section specifies that the Compliance Staff must file a response to the request for hearing (i) if the request for hearing requests use of the shortened hearing procedure or (ii) the request for hearing requests that the Registered Entity's proposed revised Mitigation Plan be approved. In all other situations, the Compliance Staff may, but is not required to, file a response to the request for hearing. Any response by the Compliance Staff must be filed within 15 days after the date the request for hearing was filed, unless the Hearing Officer or Hearing Body allows a longer time.

Section 1.3.3 – Notice of Hearing – This new section provides that the Clerk shall issue a notice of hearing not less than 16 days nor more than 21 days after the request for hearing is filed, stating whether the shortened hearing procedure or the general hearing procedure will be used; and identifying the Hearing Officer and the date, time and place for the initial prehearing conference (which shall be set for seven days following the date of the notice if the shortened hearing procedure is to be used, and 14 days following the date of the notice if the general hearing procedure is to be used).

Section 1.3.4 – Shortened Hearing Procedure – There are a number of revisions to this section to conform to terminology changes elsewhere in the revised Hearing Procedures; however, the following two revisions are substantive: (1) Compliance Staff is to make Documents available to the Registered Entity for inspection and copying pursuant to §1.5.7 within ten days (rather than five days) after the issuance of the notice of hearing; and (2) it shall be the objective of the Hearing Body to issue its final order within 120 days (rather than 90 days) after the notice of hearing. Completing the hearing process within 90 days was viewed as unrealistic in light of the various intermediate time periods for activities specified in the Hearing Procedures.

D. General Hearing Procedure

Section 1.4.1 – [Currently] Notice of Hearing – The text of this section, which in the current Hearing Procedures covers issuance of the initial notice of hearing, is deleted (this topic will be covered in new §1.3.3), and the section is intentionally left blank to avoid the need to renumber all the following subsections in §1.4.

Section 1.4.2 – Hearing Officer – (1) In subsection (a), text is revised to provide that the CEA shall (rather than may) utilize a Hearing Officer to preside over the hearing. (2) Correspondingly, subsection (b) is revised to provide that the Hearing Officer is responsible (rather than may be delegated authority) for the conduct of the hearing. (3) In subsection (b), the list of the Hearing Officer's responsibilities is modified to include to "hear argument on all objections, motions and other requests."

Section 1.4.3 – Hearing Body – (1) New subsection (a) provides that the composition of the Hearing Body, after any recusals or disqualifications, shall be such that no two industry segments may control, and no single industry segment may veto, any decision of the Hearing Body. (2) The text in subsection (b) is revised to specify that upon receiving a filing by a Participant, the Clerk shall promptly send a notice to the members of the Hearing Body identifying the date of the filing and the Participant making the filing and briefly describing the nature of the filing, and that any member of the Hearing Body may request from the Clerk a copy of any filing made by a Participant. (3) Subsection (b) is also revised to specify that the Clerk shall send all issuances of the Hearing Officer to the Hearing Body members. (4) Text is added to subsection (b) to specify that at any prehearing conference or hearing attended by a member of the Hearing Body, the Hearing Body member may ask questions directly of any Participant or witness.

Section 1.4.4 – Interlocutory Review – Revised to provide that a petition for interlocutory review shall be supported by either references to the record or by affidavit if based on facts that do not appear in the record.

Section 1.4.5 – Disqualification – Revised to provide that where a replacement Hearing Officer is appointed after the hearing has commenced, the replacement Hearing Officer may recall any witness or may take other steps necessary to ensure familiarity with the record.

Section 1.4.7 – No Ex Parte Communications – (1) Text is added to specify that the proscription against ex parte communications does not prohibit (i) communications between the Hearing Officer or members of the Hearing Body to the Clerk for the purpose of transmitting documents, giving instructions to the Clerk, or discussing scheduling or other procedural matters, or (ii) communications between or among the Clerk, the Hearing Body and representatives of the CEA for purposes of establishing the hearing forum. (2) In subsection (c), text is revised to require that a report of a prohibited communication be made by any member of the Hearing Body, the Hearing Officer or a Technical Advisor who receives or makes or knowingly allows (currently "knowingly causes to be made") a prohibited communication.

Section 1.4.8 – Appearances – Text is added to specify that all representatives appearing before the Hearing Body or Hearing Officer shall conform to the standards of ethical conduct required of practitioners before the courts of the United States.

Section 1.4.10 – Consolidation of Proceedings – (1) Revised to provide that consolidation may be considered on motion of a Participant (in addition to by the Hearing Body on its own motion). (2) References to "transaction" are changed to "occurrence," as more descriptive of the types of events that might result in an Alleged Violation, proposed penalty or proposed Mitigation Plan and ultimately result in a hearing before a Regional Entity Hearing Body.

E. Section 1.5 – Prehearing Procedure

Section 1.5.2 – Prehearing Conferences – (1) Revised to require the Hearing Officer to hold at least one prehearing conference. (2) Topics are added to the topics to be discussed at the initial prehearing conference. (3) Text is added to specify that the scheduled date for the Evidentiary Hearing shall be within 90 days of the initial prehearing conference, unless a different date is specified by the Hearing Officer or the Hearing Body with the consent of all Participants or for good cause shown. (4) Text is added to require the Hearing Officer to hold a final prehearing conference prior to the Evidentiary Hearing, to discuss specified topics and other topics suggested by the Participants.

Section 1.5.3 – Summary Disposition – (1) The basis for granting summary disposition is revised to state that there are no issues of material fact and a Participant is entitled to issuance of a final order in its favor. (2) More detailed requirements are added for the contents of a motion requesting summary disposition and the responses in opposition.

Section 1.5.4 – Status Hearing – (1) Text is added to expand the reasons for a status hearing to include "other matters relevant to the conduct of the hearing." (2) Text is added to require that a Participant

requesting a status hearing to resolve a dispute shall include in its request a certification that it has made a good faith effort to resolve the dispute with the other Participant(s) before requesting the status hearing.

Section 1.5.7 – Inspection and Copying of Documents in Possession of Staff – (1) Revised to specify that Staff is to make Documents available for inspection and copying by other Participants (rather than by just the Respondent) within 25 days after the request for hearing is filed (rather than within 5 days after the notice of hearing is issued). Corresponding revisions of "Respondent" to "Participants" are made throughout this section. (2) The requirements for production of later-received Documents are tied to the scheduled date of the Evidentiary Hearing (rather than "the hearing"). (3) The provision concerning privileged and work product Documents that may be withheld by Compliance Staff is revised to Documents that are privileged to, or work product of counsel to, the CEA (rather than the Compliance Staff). (4) Text is revised to provide that inspection reports, internal memoranda or other notes or writings prepared by Compliance Staff may be withheld if they will not be offered in evidence "or otherwise relied on by Staff in the hearing." (5) The provision concerning Documents that may be withheld by Compliance Staff because they would disclose an examination, investigatory or enforcement technique or guideline is revised to specify that the protected information must not otherwise be made public. (6) Subsection (c) is revised to require that the Compliance Staff's withheld Documents list must include a statement of the grounds that support withholding the Documents. (7) Subsection (c) is also revised to specify that the Hearing Officer, for good cause shown, may order Compliance Staff to make available any withheld Document other than a Document that is subject to attorney-client privilege. (8) Subsection (e) is revised to make it clear that a Participant may remove from the CEA's offices copies of the Documents made available by the CEA.

Section 1.5.8 – Other Discovery Procedures – (1) Text is revised to provide that the Hearing Officer, for good cause shown, may order a Participant to make a withheld Document available to other Participants, for inspection or copying. (2) The time period during which discovery should be completed is revised to 6 months following the date the request for hearing was filed (changed from 6 months from the date of the initial prehearing conference).

Section 1.5.9 – Pre-Evidentiary Hearing Submission of Testimony and Evidence – Revised to clarify that all Participant witness direct testimony to be submitted in an Evidentiary Hearing must be prepared in written form.

Section 1.5.11 – Pre-Evidentiary Hearing Memorandum – (1) Revised to eliminate the need for the Hearing Officer or Hearing Body to have grounds for requesting submission of pre-Evidentiary Hearing memoranda. (2) Revised to provide that the topics directed to be included in the pre-Evidentiary Hearing Memoranda may include "such other matters as may be directed by the Hearing Officer or the Hearing Body."

Section 1.5.12 – Certification of Questions to the NERC Board of Trustees – This new section provides for certification by the Hearing Body to the NERC Board of Trustees, for decision, a significant question of law, policy or procedure the resolution of which may be determinative of the issues in the proceeding in whole or in part, or as to which there are other extraordinary circumstances that make prompt consideration of the question by the Board of Trustees appropriate, pursuant to ROP §412. The section specifies that questions of fact presented by the particular matter in dispute in a hearing shall not be the subject of a certification. The section provides the procedures for requesting certification of a question or considering whether a question should be certified. The Hearing Body shall determine whether any proposed question shall be certified to the NERC Board for decision. The Hearing Body shall also determine whether or not the hearing should be stayed or suspended while a certified question is pending before the NERC Board.

F. Section 1.6 – Procedure at Evidentiary Hearing

Section 1.6.1 – Purpose of Evidentiary Hearing – Revised to delete the provision that the evidentiary hearing also may be used to address any other issue pending between the Participants.

Section 1.6.6 – Witness Attendance at Testimonial Hearing – A provision is added to specify that a person compelled to appear, voluntarily testifying, or making a statement may be accompanied, represented and advised by an attorney.

Section 1.6.14 – Cross-Examination – (1) Revised to provide that leading questions are permitted on cross-examination. (2) Text is added to state that the credibility of a witness may be attacked by any Participant, including the Participant calling the witness. (3) Revised to delete the requirement that if a member of the Hearing Body seeks to ask a witness questions, the Hearing Body member shall do so by submitting the questions in writing to the Hearing Officer to ask the witness (in other words, Hearing Body members can question witnesses directly).

Section 1.6.15 – Redirect Examination – Revised to delete the requirement that if a member of the Hearing Body seeks to ask a witness questions, the Hearing Body member shall do so by submitting the questions in writing to the Hearing Officer to ask the witness.

Section 1.6.17 – Close of the Evidentiary Record – (1) Revised to state that the Hearing Officer may reopen the evidentiary record for good cause shown prior to issuance of the Hearing Body's final order. (2) A statement is added that for purposes of reopening the evidentiary record, newly discovered evidence that is material to the issues in dispute and could not, by due diligence, have been discovered prior to or during the Evidentiary Hearing, shall constitute good cause.

G. Section 1.7 – Post-Evidentiary Hearing Procedure

Section 1.7.1 – Briefs – (1) Revised to allow the Hearing Officer to allow oral closing statements in addition to (not just in lieu of) briefs, and to delete the requirement that there must be agreement of the Participants in order for the Hearing Officer allow oral closing statements in addition to or in lieu of briefs (thereby leaving it to the Hearing Officer's discretion as to whether or not to allow or request closing statements). (2) Revised to allow the Hearing Officer to impose reasonable word limits (rather than page limits) on briefs. The use of word limits is consistent with current practice in many courts and agencies.

Section 1.7.4 – Hearing Officer's Initial Opinion – Revised to eliminate the provision that if the initial opinion proposes a Penalty, the initial opinion shall include a proposed Notice of Penalty. Notices of Penalty are prepared by NERC. Corresponding revisions are made in other sections of the Hearing Procedures to delete references to Notices of Penalty prepared by the Hearing Officer or the Hearing Body.

Section 1.7.5 – Exceptions – Revised to allow the Hearing Officer to impose reasonable word limits (rather than page limits) on briefs.

Section 1.7.7 – Additional Hearings – Revised to state that the Hearing Officer may reopen the record and hold additional hearings before issuance of the Hearing Body's final order (rather than before issuance of the Hearing Officer's initial decision).

Section 1.7.10 – Appeal – (1) Revised to state that a Participant or a Regional Entity acting as the CEA may appeal a final order of the Hearing Body to NERC in accordance with NERC ROP §409. (2) The statement that the Clerk shall transmit the record to NERC for any proceeding that appealed is deleted, as the procedures governing appeals are set forth in ROP §409.

H. Section 1.8 -- Settlement

Consistent with revisions in Section 5.6 of the Compliance Monitoring and Enforcement Program, this section is revised to provide that the CEA may terminate settlement negotiations at any time.

I. Section 1.9 – Remedial Action Directives

Section 1.9.1 – Initiation of Remedial Action Directive Hearing – Revised to specify that the CEA will notify NERC within two business days after issuance of a Remedial Action Directive.

Section 1.9.2 – Remedial Action Directive Hearing Procedure – (1) Revised to state that the hearing shall (rather than may) be presided over by a Hearing Officer. (2) Revised to state that the Hearing Body shall issue its summary written decision within 10 days following submission of the last brief (rather than within 10 days following the hearing). (3) Text is added to clarify that "upon issuance of the summary written decision, the Registered Entity is required to comply with the Remedial Action

Directive as specified in the summary written decision;" that is, the obligation to comply is not postponed until the Hearing Body issues its full written decision.

VII. Appendix 5A – Organization Registration and Certification Manual

A. Section I – Executive Summary

A number of revisions have been made throughout Appendix 4A for more consistent use of terms and acronyms, such as "BPS," "RC," "TOP" and BA," and "user, owner or operator" (of the BPS).

The section captioned "Where to Access and Submit Form(s)?" is revised to specify that completed registration and certification forms should be sent to the website location and/or individual(s) responsible for registration and/or certification at the Regional Entity.

In the section captioned "Roles and Responsibilities," the descriptions of the roles and responsibilities of NERC and the Regional Entities in the registration and certification processes have been revised in accordance with current practice.

B. Section II – Introduction to Organization Registration and Organization Certification Processes

In the section captioned "Organization Certification," text has been revised to specify that all entities registered in the NERC Compliance Registry for the RC, TOP and BA functions, and entities that perform some or all of the reliability functions for or with the RC, TOP or BA, shall be certified.

C. Section III – Organization Registration Process

The section captioned "Organization Registration Process," including Figure 1, Organization Registration Process Overview, has been revised consistent with current practice as to the respective responsibilities of NERC and the Regional Entities in the organization registration process.

D. Section IV – Organization Certification Process

In the section captioned "Purpose and Scope," the reference to certification of a new entity that will become NERC certified and registered as a BA, TOP or RC has been expanded to include those entities that perform some or all of the reliability functions of an RC, BA or TOP.

In the section captioned "Organization Certification Process," the text describing the Provisional Certification Process has been deleted, since the Provisional Certification Process is no longer needed. In subsection 8c of that section, the reference to the Regional Entity as the entity to which an entity

undergoing certification may express its objections to a member of the Certification Team (CT), has been changed to the Certification Team Lead. A new subsection 8e has been added to describe the composition of the CT where an existing certified entity is seeking to expand its footprint. In subsection 13, an exception has been added to the requirement that the CT shall conduct at least one on-site visit to the entity's facilities, specifically, where only a minor change in the existing footprint of an existing certified entity is under review, in which case the CT may determine that an on-site visit is not necessary. In Section 21, the provision that NERC shall update the Compliance Registry (for a new certification) "prior to the entity going operational" is changed to "in accordance with the registration rules."

E. Section V – NERC Organization Registration Appeals Process

The title and address of the NERC employee with whom registration appeals must be filed is revised. Registration appeals should now be submitted to the NERC Director of Compliance Operations.

F. Section VI – NERC Organization Certification Appeals Process

In the section captioned "Organization Certification Appeals Procedure," the title of the NERC employee with whom registration appeals must be filed is revised. Registration appeals should now be submitted to the NERC Director of Compliance Operations. Subsection 5d has been revised to more clearly describe the actions to be taken by NERC based on the Board of Trustees Compliance Committee's decision on the registration dispute.

VIII. Appendix 6 – System Operator Program Certification Manual

Appendix 6 is being deleted from the ROP, and, as described above in the summary of the revisions to ROP Section 600, the substantive provisions of Appendix 6 are being moved into Section 600. It was determined that Appendix 6 contained a significant amount of administrative detail about the System Operator Certification Program that does not need to be in the ROP.

IX. Appendix 8 – NERC Event Response Procedures

Appendix 8 is being comprehensively revised. The title of this Appendix is changed to "NERC Event Response Procedures." Consistent with the proposed revisions to ROP Sections 807 and 808 (described above), Appendix 8 has been revised to provide for a more consistent use of terms including "major event" and "occurrences."

Some material has been deleted from Appendix 8 because it will be covered in NERC's Event Analysis Process document, or is otherwise administrative detail concerning event analysis that does not need to be included in the ROP. For example, current Attachments A (Typical Team Assignments for Analysis of Blackouts or Disturbances), B (Guidelines for Analysis Team Scopes), C (NERC Confidentiality

Agreement for Analysis of Blackouts and Disturbances), and E (Guidelines for NERC Reports on Blackouts and Disturbances) are deleted. Current Attachment D (retitled "NERC Major Event Analysis Objectives, Analysis Approach, Schedule, and Status") is retained, but with sections added for Personnel, Procedures and Communications; System Restoration; System Planning and Design; and Conclusions and Recommendations.

The "Introduction" section of revised Appendix 8 provides an overview of the event response and analysis procedures, including the critical components of an effective event analysis effort.

The section "Categorization of Events" provides a description of the categorization of events, both as Category 1 (least significant) to Category 5 (most significant) events, and by level of significance: "Significant," "Conditionally Significant," "Consequential and Noteworthy," "Non-Consequential but Noteworthy," and "Not Consequential." Descriptions of the levels of significance are provided. As used in revised Appendix 8, the term "major event" is generally intended to refer to a Category 4 or 5, or a Significant or Conditionally Significant, event; and the term "other event" is generally intended to refer to a Category 1, 2 or 3, or a Consequential and Noteworthy, Non-Consequential but Noteworthy, or Not Consequential, event.

The section "Responsibility for Event Analysis Based on Category or Significance of Event" describes NERC's role in event analysis in the case of a major event and in the case of another event (*i.e.*, an event that is not a major event)..

The section "Response to and Analysis of Major Events" describes the activities that will occur or be performed by the involved participants in the case of a major event. This section describes the four phases of responding to a major event: (1) Situation Assessment and Communications, (2) Situation Tracking and Communications, (3) Data Collection, Investigation, Analysis, and Reporting (which is the event analysis phase), and (4) Publishing of Recommendations (lessons learned, best practices, and alerts, if applicable). In the Data Collection, Investigation, Analysis, and Reporting phase (*i.e.*, event analysis), based on the scope, magnitude and impact of a major event, NERC may (1) perform an overview analysis of BPS and generator response, (2) rely on a Regional Entity to conduct the analysis and monitor the analysis results, (3) work with a Regional Entity in its analysis, or (4) conduct a NERC-level analysis. Appendix 8 describes the following steps for the Data Collection, Investigation, Analysis, and Reporting phase: (a) collecting pertinent data on the major event, (b) detailed sequence of events leading to and triggering the major event, (c) detailed BPS analysis, (d) cause analysis, and (e) findings, conclusions and recommendations.

The section "Event Analysis of Other Events" describes the process steps for an event analysis of another event (*i.e.*, a non-major event).

A table is included in the revised Appendix 8 listing, by Category of event, the reports that Registered Entities involved in the event are expected to prepare and submit and the timing requirements for each report.

The section "Development of Lessons Learned from Events" describes the process for developing lessons learned from an event, to be disseminated to the industry.

The section "Reporting and Analysis Requirements for Registered Entities in Connection with Events" specifies that Registered Entities are required to report the occurrence of defined BPS disturbances and unusual occurrences to the applicable Regional Entity and to NERC in accordance with NERC and Regional Reliability Standards and other requirements.

The section "Event Analysis Interface with Compliance" states that to support a strong culture of compliance, Registered Entities are expected to conduct a rigorous self-analysis of events to determine if there have been Possible Violation(s) of a NERC Reliability Standard(s). Registered Entities are also strongly encouraged to submit a compliance self-assessment report to the applicable Regional Entity compliance liaison. This section states that, as provided in Appendix 4B, *Sanction Guidelines*, if the Registered Entity is fully cooperative in the event analysis process, conducts a self-analysis of the event and submits a timely compliance self-assessment report, and submits Self-Reports of any Possible Violations of Reliability Standards and implements corrective and mitigating actions, then in any subsequent enforcement actions, the Registered Entities' actions will be considered as mitigating factors in the determination of any penalties or sanctions for violations of Reliability Standards in connection with the event.

From:	Alex Zak
To:	Alex Zak
Subject:	NERC: Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011
Date:	Tuesday, November 22, 2011 7:21:22 PM

Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011

November 22, 2011

Click Here for access to the proposed changes: (NERC Rules of Procedure webpage)

The North American Electric Reliability Corporation (NERC) is posting revised versions of proposed new Section 5.11, and associated new Section 1.1.24 (definition of "Public Notification List") of Appendix 4C of the NERC Rules of Procedure. Proposed revisions to Appendix 4C, and to other sections and Appendices of the NERC Rules of Procedure, were originally posted on November 7, 2011, for a 45-day comment period ending December 22, 2011 and are available at: http://www.nerc.com/page.php?cid=1|8|169.

Section 5.11 of Appendix 4C is a proposed new section to establish procedures pursuant to which (1) an ISO/RTO can request the Compliance Enforcement Authority to make a determination, during the enforcement process for a Notice of Possible Violation issued to the ISO/RTO, that one or more specified other entities were responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if approved), and (2) the specified other entity or entities can request and be allowed to participate in the enforcement process against the ISO/RTO. The "Summary of Proposed Rules of Procedure Revisions" posted with the original November 7, 2011 posting correctly indicated that Section 5.11 would be applicable where the ISO/RTO seeks to allocate all or a portion of the penalty to "one or more specified other entity(ies)." However, the posted text of Section 5.11 (and the associated definition in Section 1.1.24) incorrectly provided that the Section 5.11 procedures would be available only where the ISO/RTO seeks to allocate all or a portion of the penalty to "one or more specified other Registered Entity(ies)" (emphasis added). NERC intended for the posted version of proposed Section 5.11 to specify that the procedures would be available where the ISO/RTO seeks to allocate all or a portion of the penalty to one or more specified other entity(ies); however, in the version of Appendix 4C that was posted for comment, the references to "other Registered Entity(ies)" that appeared in a prior internal draft were not revised to "other entity(ies)." In the revised versions of Sections 5.11 and 1.1.24 that are included with this notice, references throughout these sections to "specified other Registered

Entity(ies)" and "other Registered Entity(ies)" have been changed to "specified other entity(ies)" and "other entity(ies)."

NERC emphasizes that whether the procedures specified in proposed new Section 5.11 should be available only where the ISO/RTO seeks to allocate all or a portion of the penalty to one or more specified other Registered Entity(ies), or should be available where the ISO/RTO seeks to allocate all or a portion of the penalty to one or more specified other entity(ies) (whether Registered Entity(ies) or not), remains an open issue. Entities planning to submit comments on proposed Section 5.11 of Appendix 4C are urged to address this point in their comments.

The closing date for submitting comments on the proposed revisions to Appendix 4C and the other posted revisions to the Rules of Procedure remains December 22, 2011, and must be submitted electronically to ROPcomments@nerc.net.

For further information, please contact Rebecca Michael at rebecca.michael@nerc.net.

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

Ms. Alex Zak
alex.zak@nerc.net
NERC -North American Electric Reliability Corporation
Legal Dept.
1120 G Street. NW, Suite 990
Washington, DC 20005
Tel: (202) 393-3998; Fax: (202) 393-3955

This e-mail and any of its attachments may contain NERC proprietary information that is privileged, confidential, or subject to copyright belonging to NERC. This e-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this e-mail is strictly prohibited and may be unlawful. If you receive this e-mail in error, please notify the sender immediately and permanently delete the original and any copy of this e-mail and any printout.

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1276800-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011

November 22, 2011

Comments Due: December 22, 2011

The North American Electric Reliability Corporation (NERC) is posting revised versions of proposed new Section 5.11, and associated new Section 1.1.24 (definition of "Public Notification List") of Appendix 4C of the NERC Rules of Procedure. Proposed revisions to Appendix 4C, and to other sections and Appendices of the NERC Rules of Procedure, were originally posted on November 7, 2011, for a 45-day comment period ending December 22, 2011 and are available at: http://www.nerc.com/page.php?cid=1|8|169.

Section 5.11 of Appendix 4C is a proposed new section to establish procedures pursuant to which (1) an ISO/RTO can request the Compliance Enforcement Authority to make a determination, during the enforcement process for a Notice of Possible Violation issued to the ISO/RTO, that one or more specified other entities were responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if approved), and (2) the specified other entity or entities can request and be allowed to participate in the enforcement process against the ISO/RTO. The "Summary of Proposed Rules of Procedure Revisions" posted with the original November 7, 2011 posting correctly indicated that Section 5.11 would be applicable where the ISO/RTO seeks to allocate all or a portion of the penalty to "one or more specified other entity(ies)." However, the posted text of Section 5.11 (and the associated definition in Section 1.1.24) incorrectly provided that the Section 5.11 procedures would be available only where the ISO/RTO seeks to allocate all or a portion of the penalty to "one or more specified other Registered Entity(ies)" (emphasis added). NERC intended for the posted version of proposed Section 5.11 to specify that the procedures would be available where the ISO/RTO seeks to allocate all or a portion of the penalty to one or more specified other entity(ies); however, in the version of Appendix 4C that was posted for comment, the references to "other Registered Entity(ies)" that appeared in a prior internal draft were not revised to "other entity(ies)." In the revised versions of Sections 5.11 and 1.1.24 that are included with this notice, references throughout these sections to "specified other Registered Entity(ies)" and "other Registered Entity(ies)" have been changed to "specified other entity(ies)" and "other entity(ies)."

NERC emphasizes that whether the procedures specified in proposed new Section 5.11 should be available only where the ISO/RTO seeks to allocate all or a portion of the penalty to one or more specified other Registered Entity(ies), or should be available where the ISO/RTO seeks to allocate all or

a portion of the penalty to one or more specified other entity(ies) (whether Registered Entity(ies) or not), remains an open issue. Entities planning to submit comments on proposed Section 5.11 of Appendix 4C are urged to address this point in their comments.

The closing date for submitting comments on the proposed revisions to Appendix 4C and the other posted revisions to the Rules of Procedure remains December 22, 2011, and must be submitted electronically to ROPcomments@nerc.net.

For further information, please contact Rebecca Michael at rebecca.michael@nerc.net.

Revised Versions of Proposed New Sections 1.1.24 and 5.11 of Appendix 4C to the NERC Rules of Procedure

1.1.24 Public Notification List: A list posted on the NERC website, pursuant to Section 5.11 of this Appendix, of the names of the entities that an ISO/RTO contends it has authority to allocate to, pursuant to a proceeding under section 205 of the Federal Power Act, some or all of a monetary penalty imposed on the ISO/RTO for a violation of a Reliability Standard.

5.11 Special Procedures for an Enforcement Action Against an ISO/RTO Where the Monetary Penalty May be Allocated by the ISO/RTO to Other Entities

A Registered Entity that is an ISO/RTO may have authority to allocate, pursuant to a proceeding under section 205 of the Federal Power Act, some or all of a monetary penalty imposed on the ISO/RTO for violation of a Reliability Standard, to another entity(ies) that the Compliance Enforcement Authority, NERC or FERC determines was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation of the Reliability Standard. In such circumstances, the ISO/RTO may request the Compliance Enforcement Authority to make a determination, during the enforcement process for a Notice of Possible Violation issued to the ISO/RTO, that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. This Section sets forth the procedures to be followed when an ISO/RTO that has received a Notice of Possible Violation requests a determination by the Compliance Enforcement Authority that another entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation.

The procedures in this section apply only where an ISO/RTO requests a determination that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in a Notice of Possible Violation issued to the ISO/RTO, and shall not apply where the ISO/RTO anticipates or is entitled to allocate or assign a monetary penalty among all, or an identified segment of, its members, customers or users, pursuant to general cost recovery provisions in the ISO/RTO's tariffs, agreements or governance documents and regardless of actual fault or responsibility of the entities to whom the monetary penalty is issued for the violation for which the penalty is imposed.

5.11.1 Public Notification List

NERC shall maintain on its website a Public Notification List for each ISO/RTO. The Public Notification Lists shall be based solely on information provided to NERC by each ISO/RTO, and NERC shall have no responsibility to correct errors and omissions on a Public Notification List or in information provided by the ISO/RTO to NERC for inclusion in the Public Notification List. Inclusion of an entity on the Public Notification List shall not constitute or be construed as a determination by NERC that the ISO/RTO has the authority to allocate to the entity all or a part of any monetary penalty that may be imposed on the ISO/RTO for violation of a Reliability

Standard. The Public Notification List for an ISO/RTO shall be developed and maintained in accordance with the following steps:

(1) The ISO/RTO shall provide to NERC a list of the entities to which the ISO/RTO contends it has authority to allocate all or a part of any monetary penalty that is imposed on the ISO/RTO for violation of a Reliability Standard.

(2) The ISO/RTO shall provide revisions to the information for the Public Notification List to NERC from time to time as changes occur, and shall notify NERC of any errors, omissions, corrections or additions needed to the Public Notification List.

(3) NERC shall post and maintain the Public Notification List based on the information provided to NERC by the ISO/RTO. The posted Public Notification List shall consist of the names of the other entities and the date each entity was placed on the Public Notification List.

(4) Each ISO/RTO shall also provide on its website a link to the ISO/RTO's Public Notification List on the NERC website.

5.11.2 ISO/RTO's Request for Determination and Notice to Other Entity or Entities

In order to request the Compliance Enforcement Authority to make a determination in an enforcement action that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to a violation (if confirmed) of a Reliability Standard for which the ISO/RTO has received a Notice of Possible Violation, the ISO/RTO shall, no later than five (5) business days after receiving the Notice of Possible Violation (i) submit a written request to the Compliance Enforcement Authority and (ii) issue a notice to the specified other entity(ies), each conforming to the requirements of the following two paragraphs of this Section.

The ISO/RTO's written request to the Compliance Enforcement Authority shall contain:

(1) the Compliance Enforcement Authority's identification number for the Notice of Possible Violation;

(2) a statement that the ISO/RTO is requesting that the Compliance Enforcement Authority make a determination that a specified other entity(ies) was responsible, in whole or in part, for actions and omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation;

(3) the name(s) of, and contact information for, the specified other entity(ies), including name(s) and address(es) of the entity(ies) and name(s), telephone number(s) and e-mail address(es) of the contact person(s) for the other entity(ies);

(4) a statement of the basis for the ISO/RTO's authority to allocate some or all of the monetary penalty to the specified other entity(ies), including copies of any supporting tariffs, agreements, orders, or governance documents;

(5) a brief statement of the factual basis on which the ISO/RTO contends in good faith that the specified other entity(ies) was responsible for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. As the enforcement action proceeds, the ISO/RTO shall not be limited by the statement in its written request of the factual basis on which it contends the specified other entity(ies) was responsible for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation, but rather may supplement, expand or modify this explanation as additional information becomes available during the course of the enforcement action; and

(6) If the specified other entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, a statement demonstrating that there are extraordinary circumstances warranting that the Compliance Enforcement Authority make the requested determination with respect to the specified other entity despite the specified other entity's absence from the Public Notification List.

The ISO/RTO's notice to the specified other entity(ies) shall contain the following information:

(1) The name of the specified other entity, and the name, telephone number and e-mail address of the specified other entity's contact person (person to whom the notice is being sent);

(2) A statement that the ISO/RTO has received a Notice of Possible Violation from the Compliance Enforcement Authority, the Compliance Enforcement Authority's identification number for the Notice of Possible Violation, and contact information for the Compliance Enforcement Authority;

(3) A statement that the ISO/RTO has requested the Compliance Enforcement Authority to make a determination that the specified other entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, and that the ISO/RTO intends to seek to allocate to the specified other entity all or a portion of any monetary penalty that is imposed on the ISO/RTO for the violation (if confirmed), if the Compliance Enforcement Authority determines the specified other entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation.

(4) A statement that the specified other entity should contact the Compliance Enforcement Authority as soon as possible for further information and to request

to participate in the enforcement action relating to the Notice of Possible Violation.

The ISO/RTO shall cause its notice to the specified other entity(ies) to be delivered to the other entity(ies) by next-business-day delivery using a delivery service that provides verification of delivery. The ISO/RTO shall provide the Compliance Enforcement Authority with (i) a copy of the notice sent to each specified other entity, and (ii) a copy of the delivery service's verification of delivery of the notice to each specified other entity.

5.11.3 Responses of the Compliance Enforcement Authority and the Specified Other Entity or Entities to ISO/RTO's Request for Determination and Notice

Upon (i) verifying that the specified other entity(ies) was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, or, if the specified other entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determining that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the specified other entity(ies), (ii) verifying, based on the written request from the ISO/RTO, that the ISO/RTO has authority to allocate to the specified other entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, and (iii) receiving the copy of the notice and of the verification of delivery to the specified other entity(ies) showing timely delivery of the notice to the specified other entity(ies) in accordance with Section 5.11.2, the Compliance Enforcement Authority shall provide the specified other entity(ies) with a copy of a non-disclosure agreement (which shall include the specified other entity's agreement to comply with the confidentiality requirements of the Compliance Program and of Section 1500 of the NERC Rules of Procedure) that must be executed to obtain a copy of the Notice of Possible Violation and a copy of the ISO/RTO's written request to the Compliance Enforcement Authority for a determination that the specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation (if confirmed) identified in the Notice of Possible Violation. In addition to transmitting the non-disclosure agreement, the Compliance Enforcement Authority shall advise the specified other entity(ies) that: (i) the specified other entity(ies) may elect not to participate in the enforcement action, and may submit a written statement to the Compliance Enforcement Authority stating why the specified other entity is not participating and providing any facts or information the other entity wishes to provide concerning the occurrence(s) that are the subject of the Notice of Possible Violation, and (ii) whether or not the specified other entity elects to participate in the enforcement action, the Compliance Enforcement Authority may make a determination that the specified other entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation.

If the Compliance Enforcement Authority has (i) verified that the specified other entity(ies) was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation or, if the specified other entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determined that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the

specified other entity(ies), and (ii) verified that the ISO/RTO has authority to allocate to the specified other entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, then a specified other entity that has received a timely notice from the ISO/RTO as described in Section 5.11.2 shall be permitted to participate in the enforcement action concerning the Notice of Possible Violation if the other entity submits a written request to participate to the Compliance Enforcement Authority and executes a non-disclosure agreement in the form provided by the Compliance Enforcement Authority as described above. The specified other entity must submit its written request to participate prior to, as applicable (i) the date of execution of a settlement agreement between the Compliance Enforcement Authority and the ISO/RTO, or (ii) the date that the Compliance Enforcement Authority issues a Notice of Confirmed Violation to the ISO/RTO. The Compliance Enforcement Authority is not required to suspend or delay the enforcement process pending receipt of a request to participate from the specified other entity(ies), nor to revisit or redo any aspect of the enforcement process that has already occurred prior to receipt of the specified other entity(ies)'s written request to participate; however, upon receipt of a written request to participate and executed nondisclosure agreement from the specified other entity(ies), the Compliance Enforcement Authority shall suspend activity in the enforcement action until it has acted on the request to participate.

Upon receiving the specified other entity's written request to participate in the enforcement action and the other entity's executed nondisclosure agreement, the Compliance Enforcement Authority shall issue a notice to the ISO/RTO and to the specified other entity stating that the specified other entity is allowed to participate in the enforcement action. The Compliance Enforcement Authority's notice that the specified other entity is allowed to participate in the enforcement action shall include a copy of the Notice of Possible Violation originally issued to the ISO/RTO and, if a Notice of Alleged Violation and Proposed Penalty or Sanction or similar notification has been issued to the ISO/RTO, a copy of the latter Notice or notification.

If the Compliance Enforcement Authority determines (i) that the specified other entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation and that there are not extraordinary circumstances that warrant making the requested determination with respect to the specified other entity, or (ii) that the ISO/RTO does not have authority to allocate to the specified other entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, or (ii) that the ISO/RTO did not provide a timely notice to the specified other entity in accordance with Section 5.11.2, the Compliance Enforcement Authority shall issue a notice to the ISO/RTO and to the specified other entity stating that the Compliance Enforcement Authority will not make the determination requested by the ISO/RTO and that the specified other entity will not be allowed to participate in the enforcement action relating to the Notice of Possible Violation.

5.11.4 Compliance Enforcement Authority's Notices to NERC

(a) Within five (5) business days after receiving an ISO/RTO's written request for a determination that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to a violation identified in the Notice of Possible Violation

issued to the ISO/RTO, the Compliance Enforcement Authority shall provide to NERC (i) a copy of the ISO/RTO's written request for a determination that a specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, and (ii) the ISO/RTO's notice to the specified other entity(ies).

(b) On the same day that the Compliance Enforcement Authority issues a notice pursuant to Section 5.11.3 stating, as applicable, that (i) it will or will not make the determination requested by the ISO/RTO or (ii) the specified other entity(ies) are or are not allowed to participate in the enforcement action, the Compliance Enforcement Authority shall provide a copy of the notice to NERC and shall send a copy of the notice to any other entities that have been allowed to participate in the enforcement action.

5.11.5 Participation by the Specified Other Entity or Entities in the Enforcement Action Against the ISO/RTO

Upon receiving notice from the Compliance Enforcement Authority that it is allowed to participate in the enforcement action, the specified other entity may participate in the same manner as the ISO/RTO and shall be subject to all applicable requirements and deadlines specified in the NERC Compliance Program.

5.11.6 Compliance Enforcement Authority's Determination

If the Compliance Enforcement Authority has (i) verified that the specified other entity was listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, or, if the specified other entity(ies) was not listed on the Public Notification List as of the date of issuance of the Notice of Possible Violation, determined that there are nonetheless extraordinary circumstances that warrant making the requested determination with respect to the specified other entity(ies), (ii) verified that the ISO/RTO has authority to allocate to the specified other entity(ies) all or a portion of any monetary penalty imposed on the ISO/RTO for the violation (if confirmed) identified in the Notice of Possible Violation, and (iii) verified that the specified other entity(ies) received a timely notice(s) from the ISO/RTO as described in Section 5.11.2, then, if the enforcement action is not resolved by a settlement agreement stating whether or not the specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation, the Compliance Enforcement Authority shall make, and include in its proposed Notice of Penalty, its determination of whether or not the specified other entity(ies) were responsible, in whole or in part, for actions or omissions that caused or contributed to the violation. The Compliance Enforcement Authority's determination shall only address whether or not the specified other entity(ies) was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation, and shall not address whether all or a part of any monetary penalty imposed on the ISO/RTO for the violation should be allocated or assigned to the specified other entity(ies).

If the specified other entity(ies) has requested permission, and been allowed, to participate in the enforcement action, any settlement agreement specifying that the specified other entity(ies) was

responsible, in whole or in part, for actions or omissions that caused or contributed to the violation identified in the Notice of Possible Violation must be agreed to by the specified other entity(ies).

5.11.7 Procedure Where ISO/RTO Members Are Allowed to Directly Assign Monetary Penalties for Violations of Reliability Standards to the ISO/RTO

If an ISO/RTO's tariffs, agreement or other relevant governance documents establish procedures, that have been approved by FERC, that allow members of the ISO/RTO to directly assign to the ISO/RTO monetary penalties imposed on the ISO/RTO member(s) for violations of Reliability Standards, then the ISO/RTO members may follow the same requirements of Sections 5.11.2, 511.3 and 511.5 as are applicable to an ISO/RTO under those sections, and the ISO/RTO shall be afforded the same rights to participate in the enforcement action as a specified other entity under Sections 5.11.2, 5.11.3, 5.11.5 and 5.11.6, subject to the same requirements and conditions specified in those sections. In such circumstances, the ISO/RTO shall be deemed to be a "specified other entity" for purposes of this Section.

5.11.8 Obligation to Pay Monetary Penalty

(a) The ISO/RTO shall be obligated and responsible to pay any monetary penalty imposed by the Compliance Enforcement Authority on the ISO/RTO for violation of a Reliability Standard, in accordance with Section 5.10 of this Appendix, (i) regardless of whether the Compliance Enforcement Authority has made a determination that a specified other entity was responsible, in whole or in part, for actions or omissions that caused or contributed to the violation, (ii) without regard to the timing of any separate proceeding(s) in which the ISO/RTO seeks to allocate some or all of the monetary penalty to a specified other entity(ies), and (iii) without regard to whether or when the ISO/RTO receives payment from the specified other entity(ies).

(b) In an enforcement action subject to Section 5.11.7, the ISO/RTO member(s) shall be obligated and responsible to pay any monetary penalty imposed by the Compliance Enforcement Authority on the ISO/RTO member(s) for violation of a Reliability Standard, regardless of whether or when the ISO/RTO members receive payment or reimbursement from the ISO/RTO.

Standard Development Roadmap

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

Development Steps Completed:

1. NPCC Regional Standards Committee (RSC) authorized posting UFLS RSAR development on August 20, 2008.
2. UFLS RSAR posted on NPCC website on August 25, 2008.
3. NPCC Reliability Coordinating Committee (RCC) approved the Task Force on System Studies (TFSS) as the lead task force to initiate drafting a UFLS Regional Standards on September 4, 2008.
4. NPCC UFLS Regional Standard Drafting Team initial meeting on January 27, 2009.
5. First draft posted on the NPCC Website July 13, 2009 for a 45 day comment period.
6. Second draft posted on the NPCC Website May 26, 2010 for a 45 day comment period.
7. Third draft posted on the NPCC Website May 6, 2011 for a 45 day comment period.

Description of Current Draft:

This is the third draft of the proposed standard.

Future Development Plan:

Anticipated Action	Anticipated Date
1. Post the initial draft of the standard for 45 day comment period.	July 13, 2009 to August 27, 2009
2. Respond to comments on the first posting and post revised standard and implementation plan for a 45 day comment period.	September 2009 to May 2010 May 26, 2010 to July 9th, 2010
3. Respond to comments on the 2nd posting.	July 2010 to October 2010
4. Obtain RSC approval to move the standard forward to balloting.	November 2010
5. Post the standard and implementation plan for a 30 day pre ballot review.	December 2010

6. Conduct a ten day ballot.	December 2010
7. Respond to ballot comments and post revised standard and implementation plan for a 45 day comment period.	May, 2011.
8. Respond to comments on the 3rd posting.	July 2011
9. Obtain RSC approval to move the standard forward to balloting.	August 2011
10. Post the standard and implementation plan for a 30 day pre ballot review.	August 2011
11. Conduct a ten day ballot.	September 2011
12. Membership Approval.	September 2011.

Definitions of Terms Used in Standard

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

In the standards, defined terms are indicated with its first letter capitalized.

A. Introduction

1. **Title:** **Automatic Underfrequency Load Shedding**

2. **Number:** PRC-006-NPCC-1

3. **Purpose:** To provide a regional reliability standard that ensures the development of an effective automatic underfrequency load shedding (UFLS) program in order to preserve the security and integrity of the bulk power system during declining system frequency events in coordination with the NERC UFLS reliability standard characteristics.

4. **Applicability:**

   4.1. Generator Owner

   4.2. Planning Coordinator

   4.3. Distribution Provider

   4.4. Transmission Owner

5. **(Proposed) Effective Date:** To be established.

B. Requirements

R1 Each Planning Coordinator shall establish requirements for entities aggregating their UFLS programs for each anticipated island and requirements for compensatory load shedding based on islanding criteria (required by the NERC PRC Standard on UFLS). [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]

R2 Each Planning Coordinator shall, within 30 days of completion of its system studies required by the NERC PRC Standard on UFLS, identify to the Regional Entity the generation facilities within its Planning Coordinator Area necessary to support the UFLS program performance characteristics. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]

R3 Each Planning Coordinator shall provide to the Transmission Owner, Distribution Provider, and Generator Owner within 30 days upon written request the requirements for entities aggregating the UFLS programs and requirements for compensatory load shedding program derived from each Planning Coordinator's system studies as determined by Requirement R1. [Violation Risk Factor: Low] [Time Horizon: Long Term Planning]

R4 Each Distribution Provider and Transmission Owner in the Eastern Interconnection portion of NPCC shall implement an automatic UFLS program reflecting normal operating conditions excluding outages for its Facilities based on frequency thresholds, total nominal operating time and amounts specified in Attachment C, Tables 1 through 3, or shall collectively implement by mutual agreement with one or more Distribution Providers and Transmission Owners within the same island identified in Requirement R1 and acting as a single entity, provide an aggregated automatic UFLS program that sheds their coincident peak aggregated net Load, based on frequency thresholds, total nominal operating time and amounts specified in Attachment C, Tables 1 through 3. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R5 Each Distribution Provider or Transmission Owner that must arm its load to trip on underfrequency in order to meet its requirements as specified and by doing so exceeds the tolerances and/or deviates from the number of stages and frequency set points of the UFLS program as specified in the tables contained in Requirement R4 above, as applicable depending on its total peak net Load shall: [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

5.1 Inform its Planning Coordinator of the need to exceed the stated tolerances or the number of stages as shown in UFLS Attachment C, Table 1 if applicable and

5.2 Provide its Planning Coordinator with a technical study that demonstrates that the Distribution Providers or Transmission Owners specific deviations from the requirements of UFLS Attachment C, Table 1 will not have a significant adverse impact on the bulk power system.

5.3 Inform its Planning Coordinator of the need to exceed the stated tolerances of UFLS Attachment C, Table 2 or Table 3, and in the case of Attachment C, Table 2 only, the need to deviate from providing two stages of UFLS, if applicable, and

5.4 Provide its Planning Coordinator with an analysis demonstrating that no alternative load shedding solution is available that would allow the Distribution Provider or Transmission Owner to comply with UFLS Attachment C Table 2 or Attachment C Table 3.

R6 Each Distribution Provider and Transmission Owner in the Québec Interconnection portion of NPCC shall implement an automatic UFLS program for its Facilities based on the frequency thresholds, slopes, total nominal operating time and amounts specified in Attachment C, Table 4 or shall collectively implement by mutual agreement with one or more Distribution Providers and Transmission Owners within the same island, identified in Requirement R1, an aggregated automatic UFLS program that sheds Load based on the frequency thresholds, slopes, total nominal operating time and amounts specified in Attachment C, Table 4. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R7 Each Distribution Provider and Transmission Owner shall set each underfrequency relay that is part of its region's UFLS program with the following minimum time delay:

7.1 Eastern Interconnection – 100 ms

7.2 Québec Interconnection – 200 ms

[Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R8 Each Planning Coordinator shall develop and review once per calendar year settings for inhibit thresholds (such as but not limited to voltage, current and time) to be utilized within its region's UFLS program. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]

R9 Each Planning Coordinator shall provide each Transmission Owner and Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds within 30 days of the initial determination of those inhibit thresholds and within 30 days of any changes to those thresholds. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

R10 Each Distribution Provider and Transmission Owner shall implement the inhibit threshold settings based on the notification provided by the Planning Coordinator in accordance with Requirement R9. [Violation Risk Factor: High] [Time Horizon: Operations Planning]

R11 Each Distribution Provider and Transmission Owner shall develop and submit an implementation plan within 90 days of the request from the Planning Coordinator for approval by the Planning Coordinator in accordance with R9. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

R12 Each Transmission Owner and Distribution Provider shall annually provide documentation, with no more than 15 months between updates, to its Planning Coordinator of the actual net Load that would have been shed by the UFLS relays at each UFLS stage coincident with their integrated hourly peak net Load during the previous year, as determined by measuring actual metered Load through the switches that would be opened by the UFLS relays. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]

R13 Each Generator Owner shall set each generator underfrequency trip relay, if so equipped, below the appropriate generator underfrequency trip protection settings threshold curve in Figure 1, except as otherwise exempted in Requirements R16 and R19. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R14 Each Generator Owner shall transmit the generator underfrequency trip setting and time delay to its Planning Coordinator within 45 days of the Planning Coordinator's request. [Violation Risk Factor: High] [Time Horizon: Operations Planning]

R15 Each Generator Owner with a new generating unit, scheduled to be in service on or after the effective date of this Standard, or an existing generator increasing its net capability by greater than 10% shall: [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

15.1 Design measures to prevent the generating unit from tripping directly or indirectly for underfrequency conditions above the appropriate generator tripping threshold curve in Figure 1.

15.2 Design auxiliary system(s) or devices used for the control and protection of auxiliary system(s), necessary for the generating unit operation such that they will not trip the generating unit during underfrequency conditions above the appropriate generator underfrequency trip protection settings threshold curve in Figure 1.

R16 Each Generator Owner of existing non-nuclear units in service prior to the effective date of this standard that have underfrequency protections set to trip above the appropriate curve in Figure 1 shall: [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

16.1 Set the underfrequency protection to operate at the lowest frequency allowed by the plant design and licensing limitations.

16.2 Transmit the existing underfrequency settings and any changes to the underfrequency settings along with the technical basis for the settings to the Planning Coordinator.

16.3 Have compensatory load shedding, as provided by a Distribution Provider or Transmission Owner that is adequate to compensate for the loss of their generator due to early tripping.

R17 Each Planning Coordinator in Ontario, Quebec and the Maritime provinces shall apply the criteria described in Attachment A to determine the compensatory load shedding that is required in Requirement R16.3 for generating units in its respective NPCC area. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R18 Each Generator Owner, Distribution Provider or Transmission Owner within the Planning Coordinator area of ISO-NE or the New York ISO shall apply the criteria described in Attachment B to determine the compensatory load shedding that is required in Requirement R16.3 for generating units in its respective NPCC area. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R19 Each Generator Owner of existing nuclear generating plants with units that have underfrequency relay threshold settings above the Eastern Interconnection generator tripping curve in Figure 1, based on their licensing design basis, shall: [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

19.1 Set the underfrequency protection to operate at as low a frequency as possible in accordance with the plant design and licensing limitations but not greater than 57.8Hz.

19.2 Set the frequency trip setting upper tolerance to no greater than + 0.1 Hz.

19.3 Transmit the initial frequency trip setting and any changes to the setting and the technical basis for the settings to the Planning Coordinator.

R20 The Planning Coordinator shall update its UFLS program database as specified by the NERC PRC Standard on UFLS. This database shall include the following information: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

20.1 For each UFLS relay, including those used for compensatory load shedding, the amount and location of load shed at peak, the corresponding frequency threshold and time delay settings.

20.2 The buses at which the Load is modeled in the NPCC library power flow case.

20.3 A list of all generating units that may be tripped for underfrequency conditions above the appropriate generator underfrequency trip protection settings threshold curve in Figure 1, including the frequency trip threshold and time delay for each protection system.

20.4 The location and amount of additional elements to be switched for voltage control that are coordinated with UFLS program tripping.

20.5 A list of all UFLS relay inhibit functions along with the corresponding settings and locations of these relays.

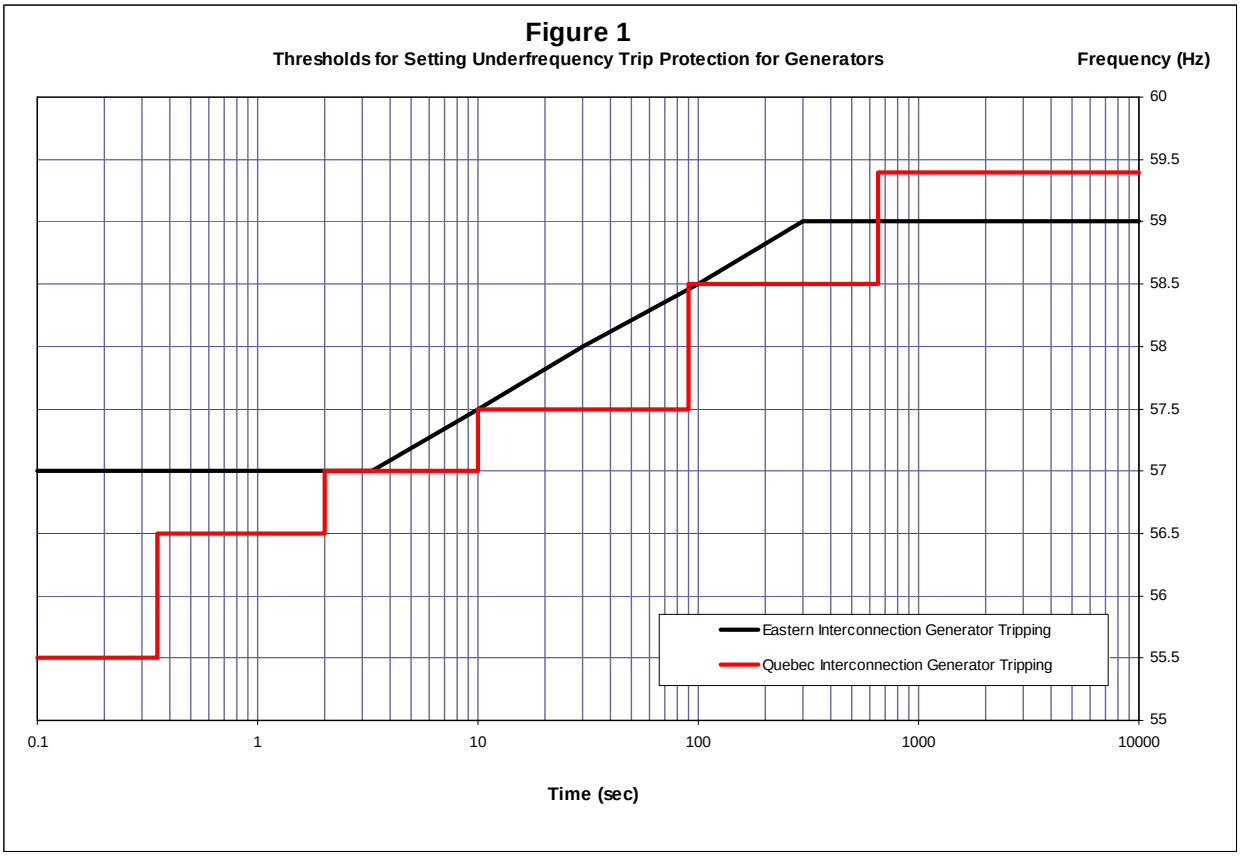
R21 Each Planning Coordinator shall notify each Distribution Provider, Transmission Owner, and Generator Owner within its Planning Coordinator area of changes to load distribution needed to satisfy UFLS program performance characteristics as specified by the NERC PRC Standard on UFLS.[Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R22 Each Distribution Provider, Transmission Owner and Generator Owner shall implement the load distribution changes based on the notification provided by the Planning Coordinator in accordance with Requirement R21. [Violation Risk Factor: High] [Time Horizon: Long Term Planning]

R23 Each Distribution Provider, Transmission Owner and Generator Owner shall develop and submit an implementation plan within 90 days of the request from the Planning Coordinator for approval by the Planning Coordinator in accordance with Requirement R21. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

Figure 1

Thresholds for Setting Underfrequency Trip Protection for Generators



C. Measures

M1 Each Planning Coordinator shall have evidence such as reports, system studies and/or real time power flow data captured from actual system events and other dated documentation that demonstrates it meets Requirement R1.

M2. Each Planning Coordinator shall have evidence such as dated documentation that demonstrates that it meets requirement R2.

M3 Each Planning Coordinator shall have evidence such as dated documentation that demonstrates that it meets Requirement R3.

M4 Each Distribution Provider and Transmission Owner in the Eastern Interconnection portion of NPCC shall have evidence such as documentation or reports containing the location and amount of load to be tripped, and the corresponding frequency thresholds, on those circuits included in its UFLS program to achieve the individual and cumulative percentages identified in Requirement R4. (Attachment C Tables 1-3).

M5 Each Distribution Provider or Transmission Owner shall have evidence such as reports, analysis, system studies and dated documentation that demonstrates that it meets Requirement R5.

M6 Each Distribution Provider and Transmission Owner in the Québec Interconnection shall have evidence such as documentation or reports containing the location and amount of load to be tripped and the corresponding frequency thresholds on those circuits included in its UFLS program to achieve the load values identified in Table 4 of Requirement R6. (Attachment C Table 4).

M7 Each Distribution Provider and Transmission Owner shall have evidence such as documentation or reports that their underfrequency relays have been set with the minimum time delay, in accordance with Requirement R7.

M8 Each Planning Coordinator shall have evidence such as reports, system studies or analysis that demonstrates that it meets Requirement R8.

M9 Each Planning Coordinator shall provide evidence such as letters, emails, or other dated documentation that demonstrates that it meets Requirement R9.

M10 Each Distribution Provider and Transmission Owner shall provide evidence such as test reports, data sheets or other documentation that demonstrates that it meets Requirement R10.

M11 Each Distribution Provider and Transmission Owner shall provide evidence such as letters, emails or other dated documentation that demonstrates that it meets Requirement R11.

M12 Each Distribution Provider and Transmission Owner shall provide evidence such as reports, spreadsheets or other dated documentation submitted to its Planning Coordinator that indicates the frequency set point, the net amount of load shed and the percentage of its peak load at each stage of its UFLS program coincident with the integrated hourly peak of the previous year that demonstrates that it meets Requirement R12.

M13 Each Generator Owner shall provide evidence such as reports, data sheets, spreadsheets or other documentation that demonstrates that it meets Requirement R13.

M14 Each Generator Owner shall provide evidence such as emails, letters or other dated documentation that demonstrates that it meets Requirement R14.

M15 Each Generator Owner shall provide evidence such as reports, data sheets, specifications, memorandum or other documentation that demonstrates that it meets Requirement R15.

M16 Each Generator Owner with existing non-nuclear units in service prior to the effective date of this Standard which have underfrequency tripping that is not compliant with Requirement R13 shall provide evidence such as reports, spreadsheets, memorandum or dated documentation demonstrating that it meets Requirement R16.

M17 Each Planning Coordinator in Ontario, Quebec and the Maritime provinces shall provide evidence such as emails, memorandum or other documentation that demonstrates that it followed the methodology described in Attachment A and meets Requirement R17.

M18 Each Generator Owner, Distribution Provider or Transmission Owner within the Planning Coordinator area of ISO-NE or the New York ISO shall provide evidence such as emails, memorandum, or other documentation that demonstrates that it followed the methodology described in Attachment B and meets Requirement R18.

M19 Each Generator Owner of nuclear units that have been specifically identified by NPCC as having generator trip settings above the generator trip curve in Figure 1 shall provide evidence such as letters, reports and dated documentation that demonstrates that it meets Requirement R19.

M20 Each Planning Coordinator shall provide evidence such as spreadsheets, system studies, or other documentation that demonstrates that it meets the requirements of Requirement R20.

M21 Each Planning Coordinator shall provide evidence such as emails, memorandum or other dated documentation that it meets Requirement R21.

M22 Each Distribution Provider, Transmission Owner and Generator Owner shall provide evidence such as reports, spreadsheets or other documentation that demonstrates that it meets Requirement R22.

M23 Each Distribution Provider, Transmission Owner and Generator Owner shall provide evidence such as letters, emails or other dated documentation that demonstrates it meets Requirement 23.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

NPCC Compliance Committee

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable

1.3. Data Retention

The Distribution Provider and Transmission Owner shall keep evidences for three calendar years for Measures 4, 5, 6,7,10, 11, and 12.

The Planning Coordinator shall keep evidence for three calendar years for Measures 1, 2, 3, 8, 9, 20, and 21.

The Planning Coordinator in Ontario, Quebec, and the Maritime Provinces shall keep evidence for three calendar years for Measure 17.

The Distribution Provider, Transmission Owner, and Generator Owner shall keep evidences for three calendar years for Measures 18, 22, and 23.

The Generator Owner shall keep evidence for three calendar years for Measures 13, 14, 15, 16, and 19.

1.4. Compliance Monitoring and Assessment Processes

Self -Certifications.

Spot Checking.

Compliance Audits.

Self- Reporting.

Compliance Violation Investigations.

Complaints.

1.5. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	**N/A**	Planning Coordinator did not establish requirements for entities aggregating their UFLS programs. or Did not establish requirements for compensatory load shedding.	Planning Coordinator did not establish requirements for entities aggregating their UFLS programs and did not establish requirements for compensatory load shedding.
R2	The Planning Coordinator identified the generation facilities within its Planning Coordinator Area necessary to support the UFLS program, but did so more than 30 days but less than 41 days after completion of the system studies.	The Planning Coordinator identified the generation facilities within its Planning Coordinator Area necessary to support the UFLS program, but did so more than 40 days but less than 51 days after completion of the system studies.	The Planning Coordinator identified the generation facilities within its Planning Coordinator Area necessary to support the UFLS program, but did so more than 50 days but less than 61 days after completion of the system studies.	The Planning Coordinator identified the generation facilities within its Planning Coordinator Area necessary to support the UFLS program, but did so more than 60 days after completion of the system studies. or The Planning Coordinator did not identify the generation facilities within its Planning Coordinator Area necessary to support the UFLS program.
R3	The Planning Coordinator provided the requested information, but did so more than 30 days but less than 41 days to the requesting entity.	The Planning Coordinator provided the requested information, but did so more than 40 days but less than 51 days to the requesting entity.	The Planning Coordinator provided the requested information, but did so more than 50 days but less than 61 days to the requesting entity.	The Planning Coordinator provided the requested information, but did so more than 60 days after the request. or The Planning Coordinator failed to provide the requested information.

R4	N/A	N/A	N/A	The Distribution Provider or Transmission Owner failed to implement an automatic UFLS program reflecting normal operating conditions excluding outages, for its Facilities or collectively implemented by mutual agreement with one or more Distribution Providers and Transmission Owners within the same island identified in Requirement R1, an aggregated automatic UFLS program that sheds Load based on frequency thresholds, total nominal operating time, and amounts specified in the appropriate included tables.
R5	N/A	The Distribution Provider or Transmission Owner armed its load to trip on underfrequency in order to meet its minimum obligations and by doing so exceeded the tolerances and/or deviated from the number of stages and frequency set points of the UFLS program as specified in the tables contained in Attachment C, as applicable depending on their total peak net Load, but did not inform the Planning Coordinator of the need to exceed the stated tolerances of UFLS Table 2 or Table 3, and in the case of Table	The Distribution Provider or Transmission Owner armed its load to trip on underfrequency in order to meet its minimum obligations and by doing so exceeded the tolerances and/or deviated from the number of stages and frequency set points of the UFLS program as specified in the tables contained in Attachment C, as applicable depending on their total peak net Load, but did not provide the Planning Coordinator with an analysis demonstrating that no alternative load shedding solution is available that would allow the Distribution Provider or	The Distribution Provider or Transmission Owner did not arm its load to trip on underfrequency in order to meet its minimum obligations and in doing so exceeded the tolerances and/or deviated from the number of stages and frequency set points of the UFLS program as specified in the tables contained in Attachment C, as applicable depending on their total peak net Load.

		2 only, the need to deviate from providing two stages of UFLS.	Transmission Owner to comply with the appropriate table.	
R6	N/A	N/A	T	The Distribution Provider or Transmission Owner in the Québec Interconnection portion of NPCC did not implement an automatic UFLS program for its Facilities based on the frequency thresholds, slopes, total nominal operating time and amounts specified in Attachment C, Table 4 or did not collectively implement by mutual agreement with one or more Distribution Providers and Transmission Owners within the same island, identified in Requirement R1, an aggregated automatic UFLS program that sheds Load based on the frequency thresholds, slopes, total nominal operating time and amounts specified in Attachment C, Table 4.
R7	N/A	N/A	N/A	The Distribution Provider or Transmission Owner failed to set

				an underfrequency relay that is part of its region's UFLS program as specified in Requirement R7.
R8		N/A	The Planning Coordinator developed inhibit thresholds as specified in Requirement R8 but did not perform the review once per calendar year.	The Planning Coordinator did not develop inhibit thresholds as specified in Requirement R8.
R9	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 30 days but less than 41 days of the initial determination or any subsequent change to the inhibit thresholds.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 40 days but less than 51 days of the initial determination or any subsequent change to the inhibit thresholds.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 50 days but less than 61 days of the initial determination or any subsequent change to the inhibit thresholds.	The Planning Coordinator provided to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds more than 60 days after the initial determination or any subsequent change to the inhibit thresholds. or The Planning Coordinator did not provide to a Transmission Owner or Distribution Provider within its Planning Coordinator area the applicable inhibit thresholds.
R10	N/A	N/A	N/A	The Distribution Provider or Transmission Owner did not implement the inhibit threshold based on the notification provided by the Planning Coordinator in accordance with Requirement R9.

R11	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 90 days but less than 101 days after the request from the Planning Coordinator.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 100 days but less than 111 days after the request from the Planning Coordinator.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 110 days but less than 121 days after the request from the Planning Coordinator.	The Distribution Provider or Transmission Owner developed and submitted its implementation plan more than 120 days after the request from the Planning Coordinator. or The Distribution Provider or Transmission Owner did not develop its implementation plan.
R12				The Transmission Owner or Distribution Provider did not provide documentation to its Planning Coordinator of actual net load data or updates to the data that would be shed by the UFLS relays, as determined by measuring actual metered load through the switches that would be opened by the UFLS relays, that were armed to shed at each UFLS stage coincident with their integrated hourly peak during the previous year.
R13	N/A	N/A	N/A	The Generator Owner did not set each generator underfrequency trip relay, if so equipped, below the appropriate generator underfrequency trip protection settings threshold curve in Figure 1, except as otherwise exempted.

R14	The Generator Owner transmitted the generator underfrequency trip setting and time delay to its Planning Coordinator more than 45 days and less than 56 days of the Planning Coordinator's request.	The Generator Owner transmitted the generator underfrequency trip setting and time delay to its Planning Coordinator more than 55 days and less than 66 days of the Planning Coordinator's request.	The Generator Owner transmitted the generator underfrequency trip setting and time delay to its Planning Coordinator more than 65 days and less than 76 days of the Planning Coordinator's request.	The Generator Owner transmitted the generator underfrequency trip setting and time delay to its Planning Coordinator more than 75days after the Planning Coordinator's request. or The Generator Owner did not transmit the generator underfrequency trip setting and time delay to its Planning Coordinator.
R15	N/A	N/A	The Generator Owner did not fulfill the obligation of Requirement R15; Part 15.1 OR did not fulfill the obligation of Requirement R15, Part 15.2.	The Generator Owner did not fulfill the obligation of Requirement R15, Part 15.1 and did not fulfill the obligation of Requirement R15, Part 15.2.
R16	N/A	The Generator Owner did not fulfill the obligation of Requirement R16, Part 16.2.	The Generator Owner did not fulfill the obligation of Requirement R16; Part 16.1 OR did not fulfill the obligation of Requirement R16, Part 16.3.	The Generator Owner did not fulfill the obligation of Requirement R16, Part 16.1 and did not fulfill the obligation of Requirement R16, Part 16.3.

R17	N/A	N/A	N/A	The Planning Coordinator did not apply the methodology described in Attachment A to determine the compensatory load shedding that is required.
R18	N/A	N/A	N/A	The Generator Owner, Distribution Provider, or Transmission Owner did not apply the methodology described in Attachment B to determine the compensatory load shedding that is required.
R19	N/A	The Generator Owner did not fulfill the obligation of Requirement R19, Part 19.3.	The Generator Owner did not fulfill the obligation of Requirement R19; Part 19.1 OR did not fulfill the obligation of Requirement R19, Part 19.2.	The Generator Owner did not fulfill the obligation of Requirement R19, Part 19.1 and did not fulfill the obligation of Requirement R19, Part 19.2.
R20	The Planning Coordinator did not have data in its database for one of the parameters listed in Requirement 20, Parts 20.1 through 20.5.	The Planning Coordinator did not have data in its database for two of the parameters listed in Requirement 20, Parts 20.1 through 20.5.	The Planning Coordinator did not have data in its database for three of the parameters listed in Requirement 20, Parts 20.1 through 20.5.	The Planning Coordinator did not have data in its database for four or more of the parameters listed in Requirement 20, Parts 20.1 through 20.5.

R21	N/A	N/A	N/A	The Planning Coordinator did not notify a Distribution Provider, Transmission Owner, or Generator Owner within its Planning Coordinator area of changes to load distribution needed to satisfy UFLS program requirements.
R22	N/A	N/A	N/A	The Distribution Provider, Transmission Owner, or Generator Owner did not implement the load distribution changes based on the notification provided by the Planning Coordinator.
R23	The Distribution Provider. Transmission Owner or Generator Owner developed and submitted its implementation plan more than 90 days but less than 101 days after the request from the Planning Coordinator.	The Distribution Provider. Transmission Owner or Generator Owner developed and submitted its implementation plan more than 100 days but less than 111 days after the request from the Planning Coordinator.	The Distribution Provider. Transmission Owner or Generator Owner developed and submitted its implementation plan more than 110 days but less than 121 days after the request from the Planning Coordinator.	The Distribution Provider. Transmission Owner or Generator Owner developed and submitted its implementation plan more than 120 days after the request from the Planning Coordinator. or The Distribution Provider. Transmission Owner or Generator Owner did not develop its implementation plan.

PRC-006-NPCC-1 Attachment A

Compensatory Load Shedding Criteria for Ontario, Quebec, and the Maritime Provinces:

The Planning Coordinator in Ontario, Quebec and the Maritime provinces is responsible for establishing the compensatory load shedding requirements for all existing non-nuclear units in its NPCC area with underfrequency protections set to trip above the appropriate curve in Figure 1. In addition, it is the Planning Coordinator's responsibility to communicate these requirements to the appropriate Distribution Provider or Transmission Owner and to ensure that adequate compensatory load shedding is provided in all islands identified in Requirement R1 in which the unit may operate.

The methodology below provides a set of criteria for the Planning Coordinator to follow for determining compensatory load shedding requirements:

1. The Planning Coordinator shall identify, compile and maintain an updated list of all existing non-nuclear generating units in service prior to the effective date of this standard that have underfrequency protections set to trip above the appropriate curve in Figure 1. The list shall include the following information for each unit:

    1.1 Generator name and generating capacity
    1.2 Underfrequency protection trip settings, including frequency trip set points and time delays
    1.3 Physical and electrical location of the unit
    1.4 All islands within which the unit may operate, as identified in Requirement R1

2. For each generating unit identified in (1) above, the Planning Coordinator shall establish the requirements for compensatory load shedding based on criteria outlined below:

    2.1 Arrange for a Distribution Provider or Transmission Owner that owns UFLS relays within the island(s) identified by the Planning Coordinator in Requirement R1 within which the generator may operate to provide compensatory load shedding.

    2.2 The compensatory load shedding that is provided by the Distribution Provider or Transmission Owner shall be in addition to the amount that the Distribution Provider or Transmission Owner is required to shed as specified in Requirement R4..

    2.3 The compensatory load shedding shall be provided at the UFLS program stage (or threshold stage for Quebec) with a frequency threshold setting that corresponds to the highest frequency at which the subject generator will trip above the appropriate curve in Figure 1 during an underfrequency event. If the highest

frequency at which the subject generator will trip above the appropriate curve in Figure 1 does not correspond to a specific UFLS program stage threshold setting, the compensatory load shedding shall be provided at the UFLS program stage with a frequency threshold setting that is higher than the highest frequency at which the subject generator will trip above the appropriate curve in Figure 1.

2.4 The amount of compensatory load shedding shall be equivalent (±5%) to the average net generator megawatt output for the prior two calendar years, as specified by the Planning Coordinator, plus expected station loads to be transferred to the system upon loss of the facility. The net generation output should only include those hours when the unit was a net generator to the electric system.

In the specific instance of a generating unit that has been interconnected to the electric system for less than two calendar years, the amount of compensatory load shedding shall be equivalent (±5%) to the maximum claimed seasonal capability of the generator over two calendar years, plus expected station loads to be transferred to the system upon loss of the facility.

PRC-006-NPCC-1 Attachment B

Compensatory Load Shedding Criteria for ISO-NE and NYISO:

The Generator Owner in the New England states or New York State are responsible for establishing a compensatory load shedding program for all existing non-nuclear units with underfrequency protection set to trip above the appropriate curve in Figure 1 of this standard. The Generator Owner shall follow the methodology below to determine compensatory load shedding requirements:

1. The Generator Owner shall identify and compile a list of all existing non-nuclear generating units in service prior to the effective date of this standard that has underfrequency protection set to trip above the appropriate curve in Figure 1. The list shall include the following information associated with each unit:

    1.1 Generator name and generating capacity
    1.2 Underfrequency protection trip settings, including frequency trip set points and time delays
    1.3 Physical and electrical location of the unit
    1.4 Smallest island within which the unit may operate as identified by the Planning Coordinator in Requirement R1 of this Standard.

2. For each generating unit identified in (1) above, the Generator Owner shall establish the requirements for compensatory load shedding based on criteria outlined below:

    2.1 In cases where a Distribution Provider or Transmission Owner has coordinated protection settings with the Generator Owner to cause the generator to trip above the appropriate curve in Figure 1, the Distribution Provider or Transmission Owner is responsible to provide the appropriate amount of compensatory load to be shed within the smallest island identified by the Planning Coordinator in Requirement R1 of this standard.

    2.2 In cases where a Generator Owner has a generator that cannot physically meet the set points defined by the appropriate curve in Figure 1, the Generator Owner shall arrange for a Distribution Provider or Transmission Owner to provide the appropriate amount of compensatory load to be shed within the smallest island identified by the Planning Coordinator in Requirement R1 of this standard.

    2.3 The compensatory load shedding that is provided by the Distribution Provider or Transmission Owner shall be in addition to the amount that the Distribution Provider or Transmission Owner is required to shed as specified in Requirement R4.

2.4 The compensatory load shedding shall be provided at the UFLS program stage with the frequency threshold setting at or closest to but above the frequency at which the subject generator will trip.

2.5 The amount of compensatory load shedding shall be equivalent (±5%) to the average net generator megawatt output for the prior two calendar years, as specified by the Planning Coordinator, plus expected station loads to be transferred to the system upon loss of the facility. The net generation output should only include those hours when the unit was a net generator to the electric system.

In the specific instance of a generating unit that has been interconnected to the electric system for less than two calendar years, the amount of compensatory load shedding shall be equivalent (±5%) to the maximum claimed seasonal capability of the generator over two calendar years, plus expected station loads to be transferred to the system upon loss of the facility.

PRC-006-NPCC-1 Attachment C

UFLS Table 1: Eastern Interconnection

Distribution Providers and Transmission Owners with 100 MW or more of peak net Load shall implement a UFLS program with the following attributes:

Frequency Threshold (Hz)	Total Nominal Operating Time (s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
59.5	0.30	6.5 – 7.5	6.5 – 7.5
59.3	0.30	6.5 – 7.5	13.5 – 14.5
59.1	0.30	6.5 – 7.5	20.5 – 21.5
58.9	0.30	6.5 – 7.5	27.5 – 28.5
59.5	10.0	2 – 3	29.5 – 31.5

UFLS Table 2: Eastern Interconnection

Distribution Providers and Transmission Owners with 50 MW or more and less than 100 MW of peak net Load shall implement a UFLS program with the following attributes:

UFLS Stage	Frequency Threshold (Hz)	Total Nominal Operating Time(s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
1	59.5	0.30	14-25	14-25
2	59.1	0.30	14-25	28-50

1. The total nominal operating time includes the underfrequency relay operating time plus any interposing auxiliary relay operating times, communication times, and the rated breaker interrupting time. The underfrequency relay operating time is measured from the time when frequency passes through the frequency threshold setpoint, using a test rate of frequency decay of 0.2 Hz per second. If the relay operating time is dependent on the rate of frequency decay, the underfrequency relay operating time and any subsequent testing of the UFLS relays shall utilize a test rate of linear frequency decay of 0.2 Hz per second.

UFLS Table 3: Eastern Interconnection

Distribution Providers and Transmission Owners with 25 MW or more and less than 50 MW of peak net Load shall implement a UFLS program with the following attributes:

UFLS Stage	Frequency Threshold (Hz)	Total Nominal Operating Time (s)[1]	Load Shed at Stage as % of TO or DP Load	Cumulative Load Shed as % of TO or DP Load
1	59.5	0.30	28-50	28-50

1. The total nominal operating time includes the underfrequency relay operating time plus any interposing auxiliary relay operating times, communication times, and the rated breaker interrupting time. The underfrequency relay operating time is measured from the time when frequency passes through the frequency threshold setpoint, using a test rate of frequency decay of 0.2 Hz per second. If the relay operating time is dependent on the rate of frequency decay, the underfrequency relay operating time and any subsequent testing of the UFLS relays shall utilize a test rate of linear frequency decay of 0.2 Hz per second.

UFLS Table 4: Quebec Interconnection

	Rate	Frequency (Hz)	MW at peak (*Load must be fixed at all times when above 60% of peak load..)	Mvar at peak	Total Nominal Operating Time (s) [2]
Threshold Stage 1	——	58.5	1000*	1000	0.30
Threshold Stage 2	——	58.0	800*	800	0.30
Threshold Stage 3	——	57.5	800	800	0.30
Threshold Stage 4	——	57.0	800	800	0.30
Threshold Stage 5 (anti-stall)	——	59.0	500	500	20.0
Slope Stage 1	-0.3 Hz/s	58.5	400	400	0.30
Slope Stage 2	-0.4 Hz/s	59.8	800*	800	0.30
Slope Stage 3	-0.6 Hz/s	59.8	800*	800	0.30
Slope Stage 4	-0.9 Hz/s	59.8	800	800	0.30

2. The total nominal operating time includes the underfrequency relay operating time plus any interposing auxiliary relay operating times, communications time, and the rated breaker interrupting time. The underfrequency relay operating time shall be measured from the time when the frequency passes through the frequency threshold set point.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Regional Reliability Standards Announcement

Comment Period Open for PRC-006-NPCC-1
November 22, 2011–December 22, 2011

Regional Project: Now Available

Proposed Standard for the Northeast Power Coordinating Council (NPCC)

NPCC has requested NERC to post regional reliability standard PRC-006-NPCC-1 — Automatic Underfrequency Load Shedding for a 30-day industry review as permitted by the NERC Rules of Procedure.

Instructions
Please use this **electronic form** to submit comments. If you experience any difficulties in using the electronic form, please contact Eleanor Crouch at **eleanor.crouch@nerc.net**. An off-line, unofficial copy of the comment form is posted on the **regional standards development page**:

Background
PRC-006-NPCC-1 ensures the development of an effective Automatic Underfrequency Load Shedding (UFLS) program in order to preserve the security and integrity of the bulk power system during declining system frequency events.

Regional Reliability Standards Development Process
Section 300 of the ***Rules of Procedure for the Electric Reliability Organization*** governs the regional reliability standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Eleanor Crouch at **eleanor.courch@nerc.net** (via email) or at 404.446.2572.

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

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

PRC-006-NPCC-1 Automatic Underfrequency Load Shedding

Implementation Plan

Background:

The purpose of this draft Regional Standard is to ensure the development and maintenance of an effective and coordinated Automatic Underfrequency Load Shedding program in order to preserve the reliability and integrity of the bulk power system during declining system frequency events.

In the developing the Implementation Plan for PRC-006-NPCC-01 the Standard Drafting Team considered the following:

1. The requirements listed in this Regional Standard are intended to cover all aspects of the UFLS program. The Regional Standard Drafting Team (RSDT) coordinated its development with the draft NERC UFLS Standard PRC-006. The intent of this Regional Standard is to be more stringent than the continent wide standard while incorporating specific program characteristics into the requirements.
2. The Implementation Plan for this standard is based, in part, on the timelines reflected in the existing and ongoing Implementation Plan for NPCC Directory #12 absent the annual milestones required by Directory #12.

Effective Dates:

Eastern Interconnection & Québec Interconnection Portions of NPCC Excluding the Independent Electricity System Operator (IESO) Planning Coordinator Area of NPCC in Ontario, Canada.

1. The effective date for requirements R1, R2, R3, R4, R5, R6, and R7 is the first day of the first calendar quarter following applicable regulatory approval but no earlier than Jan 1, 2016 to allow for the existing implementation plan to be completed.

2. The effective date for requirements R8 through R23 is the first day of the first calendar quarter two years following applicable governmental and regulatory approval.

Independent Electricity System Operator (IESO) Planning Coordinator's Area of NPCC in Ontario, Canada

1. Effective the first day of the first calendar quarter following applicable governmental and regulatory approval but no earlier than April 1, 2017.

References:

- 2006 Assessment of UFLS Adequacy Part 3 Assessment of Program Modifications.
- SS38 Underfrequency Load Shedding Support Studies

NPCC Criteria:

- Directory #12 Underfrequency Load Shedding Program Requirements.
- A-7 NPCC Glossary of Terms.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Application Notice — 0027

TOP-003 R2 Coordination of Scheduled Outages

DRAFT

Posted [DATE]

Primary Interest Groups
Compliance Enforcement Authority (CEA)[1]
NERC
Regional Entity
Balancing Authority (BA)
Generator Operator (GOP)
Transmission Operator (TOP)
Reliability Coordinator (RC)

Issue: What is the responsibility of the BA under TOP-003 R2?
For the purpose of aiding a CEA, this CAN provides instruction to assess whether the BA fulfilled its responsibility to communicate and coordinate under TOP-003 R2.

Background
TOP-003 R2 *Planned Outage Coordination* requires that each TOP, BA and GOP plan and coordinate scheduled outages of system voltage regulating equipment with affected BAs and TOPs as required.

The BA has knowledge of the generating unit commitment and planned dispatch which defines the dynamic reactive support available. This information is necessary for TOPs, BAs, and GOPs to coordinate scheduled outages of other system voltage regulating equipment. This information enables the TOP to determine the need for any additional generating units that must be committed to provide additional dynamic reactive capability.

Compliance Application
TOP-003 R2 provides:

> *R2. Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.*

[1] Compliance Enforcement Authorities include ERO auditors, investigators, enforcement personnel or any person authorized to assess issues of concern, potential non-compliance, and possible, alleged or confirmed violations of NERC Reliability Standard requirements.

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

Coordination, as required by R2, involves two or more registered entities working together to achieve a desired result. While coordination among BAs, TOPs and GOPs is interwoven, each function provides key information. Although not all-inclusive, a simplified example of how the three functions coordinate is as follows:

- The BA has knowledge of generation unit commitment and planned dispatch, which it must communicate to the TOP. Additionally, the BA provides dispatch orders for generation to the GOP based on requests for dispatch changes from the TOP.
- The GOP provides information on the availability, status, real and reactive capability, and real and reactive de-ratings of generating units to both the BA and the TOP.
- The TOP is responsible for the system configuration, managing the required must-run units for voltage and reactive control, and determining needs for system support. It provides voltage and reactive schedules to the GOP and requests that the BA dispatch additional capacity for system support as necessary, including reactive support.

A CEA is to verify that the BA coordinated with the GOP and the TOP pursuant to TOP-003 R2.

Effective Period for CAN

This CAN is effective upon posting as final on the NERC Web site, and is to be used by CEAs to assess compliance from the posting date forward, regardless of the start date of any non-compliance or Possible Violation. It supersedes all prior communications and will remain in effect until such time that a future version of a FERC or other applicable government authority approved standard or interpretation becomes effective and addresses the specific issue contained in this CAN.

For any enforcement action in process and for audits that have been initiated,[2] a CEA will apply the appropriate discretion, including consideration of the specific facts and circumstances of the non-compliance, in determining whether to assess compliance pursuant to this CAN.

Evidence of Compliance

A CEA is to verify that a BA provided dispatch information to the TOP including generating unit commitment. The CEA is to verify the BA coordinated generation related outages.

Since the BA only has knowledge of generation related resources, and is not responsible for knowing the status of other reactive resources, the CEA should not hold the BA accountable for the planning and coordination of scheduled outages for reactive resources such as static var compensators (SVCs), static synchronous compensators (STATCOMs), or shunt and series capacitors, and reactors.

Additionally, a CEA is to verify that the BA responded to any requests from the TOP, including but not limited to requests to dispatch additional units for reactive capacity.

The CEA is to verify these activities regardless of whether the BA operates under a vertically-integrated company or an unbundled, full-service market structure.

[2] "Initiated" means that a registered entity has received notification of the upcoming audit.

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

For more information please contact:

Michael Moon
Director of Compliance Operations
michael.moon@nerc.net
404-446-2567

Valerie Agnew
Manager of Interface and Outreach
valerie.agnew@nerc.net
404-446-2566

Caroline Clouse
Interface and Outreach Specialist
caroline.clouse@nerc.net
404-446-2588

This document is designed to convey compliance monitoring instruction to achieve a measure of consistency among auditors and Compliance Enforcement Authorities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing NERC Reliability Standard. Compliance will continue to be assessed based on language in the currently enforceable NERC Reliability Standards. This document is not intended to define the exclusive method an entity must use to comply with a particular standard or requirement, or foreclose a registered entity's demonstration by alternative means that it has complied with the language and intent of the standard or requirement, taking into account the facts and circumstances of a particular registered entity. Implementation of information in this document is not a substitute for compliance with requirements in NERC's Reliability Standards.

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

From: Jordan Erwin
To: canonly
Subject: NERC Announcement: Activity on the Compliance Application Notice (CAN) Website
Date: Tuesday, November 22, 2011 2:24:09 PM

NERC Compliance Announcement:

DRAFT CAN Posted for Industry Review

DRAFT CAN Industry Comment Materials Posted

Updated CAN Status Spreadsheet

The following draft CAN has been posted on the NERC Web site for industry review:

- **DRAFT CAN-0027**: TOP-003 R2 Coordination of Scheduled Outages
  This CAN will be posted for industry comment until **December 14, 2011**. Please email comments using the CAN Comment Form to cancomments@nerc.net.

The following DRAFT CAN Industry Comment materials are posted on the NERC Web site:

- **DRAFT CAN-0030**: Attestations
  - Comment Analysis Summary
  - Industry Comment Analysis Spreadsheet
  - Industry Comments Received

The CAN Status spreadsheet has been posted as final under the Complete List of CANs and Status section on the NERC Web site:

- The CAN Status spreadsheet has been updated to reflect the recent changes to Compliance Application Notices. This spreadsheet indicates where each CAN currently resides in the CAN development process.

For more information regarding Compliance Application Notices, please contact Valerie Agnew at (404) 446-2566, Ben Engelby at (404) 446-2578 or Caroline Clouse at (404) 446-2588.

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

Y