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

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #14-5
December 4th, 2014, 8:00 a.m. – 5:00 p.m. AST
Halifax Marriott Harbourfront Hotel
1919 Upper Water Street
Halifax, Nova Scotia B3J 3J5 Canada
Attire: Business Casual

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

For Reference: Glossary of Terms Used in NERC Reliability Standards, dated October 1, 2014
NPCC Glossary of Terms, dated January 18, 2012

Introductions and Chair's Remarks

NPCC Antitrust Compliance Guidelines

Agenda Items:

1.0 Review of Agenda

2.0 RSC Meeting Minutes

2.1 Approval of Minutes: September 17-18, 2014 RSC Meeting #14-4*

3.0 Drafting Team Members and Executive Tracking Summary

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

4.0 Open Action Items*

4.1 Open Action Items List

5.0 Items Requiring RSC Discussion / Approval

5.1 NERC Weekly Standards Bulletin
5.2 NERC RAPA Meeting
5.3 NPCC RCC Meeting Minutes
5.4 NERC Bulk Electric System Update
5.5 Canadian Provincial Summaries

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

6.1 Currently Posted Projects

Project	Comment Period	Ballot Period	Standards Developer	12/4/14 Call-In

	End Date	End Date		
Project 2014-01 Standards Applicability for Dispersed Generation Resources	12/10/14	12/19/14	Katherine Street	
Project 2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions	1/8/15	1/8/15	Ryan Stewart	
Comments: (I) – Informal; (F) – Formal **Ballots:** (I) – Initial; (A) – Additional; (F) – Final				

6.1.1 NERC Projects Comment Period Guidelines

6.2 Ballot History (Since last RSC Meeting)*

6.3 Comment Form History (Since last RSC Meeting)*

7.0 NERC Drafting Team Nominations

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

7.1 Currently Posted Drafting Team Vacancies

7.1.1 None at this time

7.2 Closed Drafting Team Nominations (Since last RSC Meeting)

7.2.1 None at this time

7.3 Solicitation For Informal Development Teams

7.3.1 None at this time

8.0 NPCC Regional Reliability Standards*

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

8.1 Current Activities: Regional Standards Process Manual

8.2 Current Activities: Regional Standard BAL-002-NPCC-01: Regional Reserve Sharing

9.0 NPCC Non-Standards*

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

9.1 Directories:

9.1.1 Directory #1 Design and Operation of the Bulk Power System

9.1.2 Directory#3 Maintenance Criteria BPS – (Retirement Approved on 10/15/2014 effective April 1st, 2015).

9.2 Directory Clarifications

9.2.1 TFSP Clarification for the IESO- Market Assessment and Compliance Division (MACD).

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

9.4 Directory Manual (Revisions Approved by the RSC on 10/03/2014)

10.0 RSC Member Items of Interest

10.1 RSC Roster*

11.0 Standards Activity Post NERC BOT Approval*

(Since last RSC Meeting)

11.1 NERC Filings to FERC

http://www.nerc.com/FilingsOrders/Pages/default.aspx

11.2 FERC Orders / Rules
http://www.nerc.com/FilingsOrders/Pages/default.aspx
11.3 Federal Register
https://www.federalregister.gov/
11.4 FERC Sunshine Act Meeting Notice
11.5 FERC Open Meeting Summaries

12.0 NERC Meetings

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

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

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

February 6th & 7th	March 12th & 13th	April 23rd Call
June 10th & 11th	July 29th	October 1st
October 28th	December 9th	

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

February 21st - Call	February 28th - Meeting	April 17th - Meeting
June 10th	September 30th	October 16th - Call
November 6th - Call		

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

January 8th	February 5th	April 9th
May 6th	July 16th	August 13th
October 15th	November 12th & 13th	

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

February 6th	April 23rd	May 7th
August 14th	October 29th	November 13th

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

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

13.0 NERC Compliance Tools (Since last RSC Meeting)

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

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

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

13.2.1 There are five RSAWs have been posted for comment since the last RSC meeting.

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

13.3.1 There have not been any new CANs posted since the last RSC meeting

14.0 NERC Items of Interest (Since last RSC Meeting)

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

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

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

14.2.1 There has been no new NERC Alert released since the last RSC meeting.

14.3 Five Year ERO Performance Assessment

15.0 Other Items of Interest

15.1 2015 Regional Entity Business Plans and Budgets

15.2 Quality Review of NERC Standards

16.0 Future RSC Meetings and Conference Calls

16.1 RSC 2014/2015 Meeting Dates

Feb. 19th – 20th, NextEra Energy Offices
April 10th & 11th, NPCC Offices

June 18th & 19th, Saratoga, NY
September 17th & 18th, Montreal, Quebec
December 4th, Halifax, Nova Scotia
February 18-19, 2015, NextEra Energy Offices

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

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

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 participants 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 Assistant Secretary, Andrew Fawbush at 904-598-6133.

NPCC, Inc.

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

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #14-4
September 17, 2014, 10:00 a.m. - 5:00 p.m. EST
September 18, 2014, 8:00 a.m. - 3:00 p.m. EST
Marriott Spring Hill Suites Old Montreal Hotel
445 Rue Saint-Jean-Baptiste
Montreal, Canada
Attire: Business Casual

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

For Reference: Glossary of Terms Used in NERC Reliability Standards, dated August 20, 2014
NPCC Glossary of Terms, dated January 18, 2012

MEETING MINUTES

Attendees:

	Name	Organization	Sector (s)	Day(s)	Comment
1.	Kal Ayoub	FERC	Guest	1 & 2	
2.	Guy Zito	Northeast Power Coordinating Council		1 & 2	
3.	Lee Pedowicz	Northeast Power Coordinating Council		1 & 2	
4.	Gerry Dunbar	Northeast Power Coordinating Council		1 & 2	Via Phone
5.	RuiDa Shu	Northeast Power Coordinating Council		1 & 2	
6.	Herb Schrayshuen	Power Advisors, LLC – Proxy for NextEra Energy, LLC	4	1 & 2	Via Phone
7.	Jim Grant Proxy for Greg Campoli	New York Independent System Operator	2	1 & 2	Via Phone
8.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	2	1 & 2	
9.	Michael Jones	National Grid	3	1 & 2	Via Phone
10.	Vijay Puran	NYS Department of Public Service	6	1	Via Phone
11.	Kathleen Goodman	ISO-NE	2	1 & 2	
12.	Helen Lainis	IESO	2	1	

* Item in Meeting Materials

13.	Alan MacNaughton	New Brunswick Power Corporation	1	1 & 2	
14.	Don Weaver	New Brunswick Power Corporation	Guest	1 & 2	
15.	Bruce Metruck Sector 4 Proxy for Wayne Sipperly	New York Power Authority	4/5	1 & 2	
16.	Greg Goodrich	New York Power Authority	Guest	1	Via Phone
17.	Si-Truc Phan Sector 1 Proxy for Sylvain Clermont	Hydro-Québec TransÉnergie	1/2	1 & 2	
18.	Brian Robinson	Utility Services	5	1	
19.	Brian Shanahan	National Grid	1	1 & 2	
20.	Chantal Mazza	Hydro-Québec TransÉnergie	Guest	1 & 2	
21.	Muhammed Ali	Hydro One Networks	Guest	1 & 2	
22.	Ayesha Sabouba	Hydro One Networks	1	2	Via Phone
23.	Ben Wu	Orange and Rockland Utilities	1	1 & 2	
24.	Tom Neglia	Orange and Rockland Utilities	Guest	1 & 2	Via Phone
25.	Mike Garton	Dominion Resources Services	4	1 & 2	
26.	Connie Lowe	Dominion Resources Services	Guest	1 & 2	
27.	Don Nelson	Massachusetts Department of Public Utilities	Guest	1	Via Phone
28.	Ron Falsetti	AESI	Guest	1 & 2	Via Phone
29.	Dave Kiguel	David Kiguel Consulting	Guest	1 & 2	

Introductions and Chair's Remarks

Guy Zito called the meeting to order at 9:59AM on Wednesday September 17, 2014.

NPCC Antitrust Compliance Guidelines

The NPCC Antitrust Compliance Guidelines were read by Lee Pedowicz.

Agenda Items:

1.0 <u>Review of Agenda</u>

The RSC Draft Meeting Agenda was reviewed by Guy Zito.

* Item in Meeting Materials

2.0 RSC Meeting Minutes

2.1 Approval of Minutes: June 18-19, 2014 RSC Meeting #14-3*

The RSC Meeting Minutes for June 18-19, 2014 RSC Meeting #14-3 was reviewed.

Mike Garton made a motion for approval.

Kathleen Goodman seconded the motion.

The Meeting Minutes were approved as read.

3.0 Drafting Team Members and Executive Tracking Summary

3.1 NPCC Members on NERC Drafting Teams*

The spreadsheet of NPCC Members on NERC Drafting Teams March, 2014 was reviewed. It was noted that the spreadsheet was unchanged since the last RSC meeting.

3.2 Executive Tracking Summary*

Additional information was provided for RSC members to look at. The Executive tracking summary has been actively updated for over seven years.

3.3 NERC Project Tracking Spreadsheet (*link*)

This is NERC's version of the Executive Tracking Summary.

4.0 Open Action Items*

4.1 Open Action Items List

Item	Description	Owner	Due	Status
4.1.1	Coordination with the Compliance Committee to develop Joint Activity Action List	Greg Campoli/Guy Zito	RSC Meeting	Update: RSC decided that it was not necessary to have a joint meeting with CC at the December, 2014 meeting in Halifax.
4.1.2	New York Adoption of More Stringent/Specific NPCC Criteria – determine more stringent criteria and submit filing	Gerry Dunbar	October, 2014	Update: NPCC Executive Staff is providing additional comments. NPCC expects the document to be filed with the NYSPSC by late September pending final NPCC legal review. RSC Members will

* Item in Meeting Materials

				be notified when the document is filed.
4.1.3	NPCC outreach program development – discussion item: members provide input and opportunities for development of an outreach program	RSC	RSC Meeting	Update: Ongoing, two outreaches have been done with NYPA.
4.1.4	Project 2010-17, BES - Follow up with Drafting Team to identify established set of criteria for when an entity can request an exclusion and what should be provided	Guy Zito		Update: Because this has been addressed, this will be removed from the Open Action Item List.
4.1.5	Revise the Directory Development Manual to address cost effectiveness	G. Dunbar		Update: Revisions to the Directory Manual posted to the NPCC Open Process from May, 2014 to July, 2014. Draft RSC responses to Open Process comments and final approval of Directory Manual revisions pending final RSC review and approval.
4.1.6	Project 2007-06 - System Protection Coordination – share concerns raised at the RSC meeting with the	Guy Zito		Update: This will be removed from the Open Action Item List as suggested by

* Item in Meeting Materials

	Standard Drafting Team *[At the February RSC meeting there were concerns regarding: coordination between entities; tracking and notification of 10% or greater change in fault current at an interconnecting bus; need for a common tool to facilitate data exchange.]*			Guy Zito, agreed to by Si-Truc Phan who had been following it.
4.1.7	Follow up with NERC on current RSAW development process	Guy Zito		Update: After discussion the RSC members decided to not immediately address this, but wait for new items to be published.
4.1.8	Update NPCC Members on NERC Drafting Teams based on feedback received at the April, 2014 RSC meeting			Update: This item will be removed from the Open Action Item list because the task is completed
4.1.9	Update executive tracking summary. • Project 2007-02 Operating Personnel Communications Protocols: COM-002-4 Final Ballot Project 2010-05.1 was updated under the Reliability Standards tab but was missing from summary of changes. The summary of changes should be corrected.			Update: This item will be removed from the Open Action Item List. RuiDa Shu is keeping it current.
4.1.10	Update the RSCMembers email list to include both Primary and Alternate RSC members			Update: This item was done, and will be removed.

* Item in Meeting Materials

4.1.11	Project 2010-02, the use of the term "Facilities" rather than entities defined by the functional model was not supported by the RSC. Provide alternate language for consideration	Helen Lainis		Update: This item will be removed from the Open Action Item List since Project 2010-02 is approved, as suggested by Guy Zito and approved by Helen Lainis.

5.0 Items Requiring RSC Discussion / Approval

5.1 NERC Weekly Standards Bulletin

This is additional information for the RSC and is available on the NERC website.

5.2 NERC RAPA Meeting

Guy Zito suggested that for future RSC meetings only provide a link to these materials instead of downloading them into the meeting package.

5.3 NPCC RCC Meeting Minutes

Guy Zito suggested that for future RSC meetings only provide a link to these materials instead of downloading them into the meeting package.

5.4 NERC Bulk Electric System Update

Guy Zito suggested that for future RSC meetings only provide a link to these materials instead of downloading them into the meeting package.

5.5 Enhancing and Expanding RSC Standards Activities

Comments should be reviewed more closely. Guy Zito asked the RSC members to consider and provide suggestions/comments if necessary.

5.6 Impact of New SPS Definition – Gerry Dunbar

Currently NERC has posted a project for comment and ballot (Project 2010-05.2 – Special Protection Systems) that would establish a new NERC Glossary definition for a RAS (Remedial Action Scheme) and retire the term SPS, in addition to replacing references to SPS with RAS in all ERO standards.

NPCC and its Task Forces will be required to evaluate the revised definition to ensure that its criteria remain not inconsistent with the new definition.

While the RSC is responsible for coordinating the NPCC Directory project and monitoring the impact of revised ERO standards on its criteria, ultimately any changes to the NPCC criteria or other documents fall under the jurisdiction of the NPCC Task Force responsible for the document and the RCC.

* Item in Meeting Materials

The RSC will continue to monitor the progress of this project in order to ensure that its criteria remain not inconsistent with the ERO standards.

6.0 NERC Reliability Standards

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

6.1 Currently Posted Projects

Project	Comment Period End Date	Ballot Period End Date	Standards Developer	9/17/14 Call-In
Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	10/17/14 (F)	10/17/14 (A)	Greg Goodrich from NYISO	11:30AM
Project 2014-03 Revisions to TOP and IRO Standards	9/19/14 (F)	9/19/14 (A)	Wendy Muller	NA
Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	10/2/14 (F)	10/2/14 (A)	Darrel Richardson	1:15PM
Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings	10/6/14 (F)	10/6/14 (A)	Scott Barfield-McGinnis	1:30PM
Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	10/8/14 (F)	10/8/14 (I)	Lacey Ourso	1:45PM
Project 2013-03 Geomagnetic Disturbance Mitigation	10/10/14 (F)	10/10/14 (A)	Mark Olson	2:00PM
Project 2014-01 Applicability for Dispersed Generation Resources Standards	10/16/14 (F)	10/16/14 (A)	Ryan Stewart	2:15PM
Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions	10/17/14 (F)	10/17/14 (A)	Ryan Stewart	2:30PM
Project 2009-03 Emergency Operations	10/20/14 (F)	10/20/14 (A)	Laura Anderson	2:45PM
Project 2007-11 Disturbance Monitoring	10/21/14 (F)	10/21/14 (A)	Stephen Crutchfield	3:00PM
Project 2014-01 Applicability for Dispersed Generation Resources Standards	10/22/14 (F)	10/22/14 (A)	Ryan Stewart	3:15PM
Comments: (I) – Informal; (F) – Formal **Ballots:** (I) – Initial; (A) – Additional; (F) – Final				

* Item in Meeting Materials

1. Project 2014-02 CIP version 5: The communication systems deadline is in December, 2015. Two elements did not pass. The SDT has made adjustments to the standards' language to satisfy concerns from entities. One area of concern is the effort from the low risk entities. The sense is generally a positive response from the entities with minor changes to the standards. There is a concern with the industry in terms of underestimating the amount of time/effort required for the new standards. The goal is to have the TFIST group come up with the consensus votes during the meeting tomorrow September 18th, 2014 and turn it in by next Tuesday September 23rd, 2014 to RSC. The internal control program is completely separate from the RSAWs. CIP-003 low impact assets and CIP-010 are the two areas of concern and an update from TFIST is needed in terms of consensus for those two standards. These two issues will be the main focus for RSC, and the CIP-003 low impact assets will be the biggest challenge. Greg Goodrich is recommending we abstain on the recommendation for CIP-003. All other standards were approved.
2. Project 2014-03: Standard developer Wendy Muller called in.
   TOP-001-3:
   R1 should revert back to the original language. Use maintain instead of ensure. Operations planning is not real-time operations. It was suggested to keep real-time operations. R2 has the same issue as R1.
   R3 has the same issues with the time horizons.
   R4--all time horizons should be reviewed especially where operating instruction is used to review the time horizons to be done. Check the wording for this.
   R5 is acceptable as is.
   R6 is acceptable as is.
   R7 capitalize Emergency procedures since Emergency is a defined term. Comparable should be added in front of Emergency procedures.
   R8 is acceptable as is.
   R9--need to remove interconnect NERC registered to be consistent with TOP-002-4 requirement R3.
   R10--repeat the comments submitted for the previous posting.
   R11 make a comment on the word "ensure". Reference PRC-001-1.1 against R11.
   R12 is acceptable as is.
   R13 remove the word "ensure".
   R14 is acceptable as is.
   R15-- "System" should be capitalized.
   R16--remove telecommunication and replace it with telemetering equipment. There is inconsistency between R9 and R16.
   R17--remove telecommunication and replace it with telemetering equipment. There is inconsistency between R9 and R16.
   R18--remove the word "always".
   R19--remove the word "Balancing Authority Area", and replace it with Transmission Operator area.
   R20--remove the Transmission Operator Area and replace it with "Balancing Authority Area".
   RSC will be voting "No" for this standard.
   TOP-002-4: RSC will be voting "Yes".

* Item in Meeting Materials

TOP-003-3: RSC will be voting "Yes".
IRO-001-4: Voting status is divided among the members.
IRO-002-4: Telecommunication should be removed from R3 and replaced with telemetering equipment. The goal is to make it consistent. R4--remove the comma between facilities and identify. RSC will be voting "No".
IRO-008-2: Remove "Wide" from R6 on Reliability Coordinator Wide Area so it is consistent. There are no positive votes, all votes were abstain or negative.
IRO-010-2: Dominion is voting "No" because of the sub-100KV requirement. Voting status is divided among the members.
IRO-014-3: Use the old wording instead of adjacent Reliability Coordinator Areas, RSC will be voting "No".
IRO-017-1: RSC will be voting "Yes".
RSC voted "Yes" to the Implementation plan.

3. Project 2010-14.1: Some language was removed from the standard because it clouded the issue. The SDT tried to make it stand-alone versus the EOP standards. BAL-002 and EOP standards are conflicting with each other. Additional language was added, such as contingency reserves that can be used, but you are required to restore the contingency reserve within 90 minutes. Darrel Richardson called in.
4. Project 2010-13.3: Re-evaluation of the relays every three years. Three years allows the entities to plan out their relay maintenance. There was a 17 percent approval and 83 percent disapproval. Scott Barfield-McGinnis called in.
5. Project 2008-02: Very minimal changes, modified R9 and R10 for the new requirement. Identified the deficiency in the UFLS program. Lacey Ourso called in.
6. Project 2013-03 GMD: The main objectives are historical measurements, reports, and an understanding of HQ's findings. There are three types of GIC (Geomagnetic Induced Current): Electrojet, Simulation and Hypothesis. Study is based on the blackout of March, 1989. Volts/km is an issue. E-field is another issue. Transformer thermal assessment is proving to be a challenge. GMDTF has provided a training model. Mark Olson called in.
7. Project 2014-01: A NERC Webinar outreach will be in a few weeks. Ryan Stewart called in.
8. Project 2014-02: CIP version 5 has a webinar on Friday September 19th, 2014. Ryan Stewart called in.
9. Project 2009-03: The manual load shedding plan has been minimized. Major change was taking out the "approval" language to "review". Review, identify and notify the BA for any emergency operations. The goal is to make sure the RC, BA and TOP do not have overlapping responsibilities. Contingency reserves should be part of operating reserves. Laura Anderson called in.
10. Project 2007-11: Standard is posted for another comment and ballot. The standard has been revised to address common concerns of the industry. The standard is trying to capture the data, not focus on the equipment to capture the data. The standard is there because data capture is not consistent across the continent. Dynamic disturbance recording data has been revised, the fault recording section of the standard (record length) has been reduced. Best business practice is to have these data available for your power system for real time operations and analysis afterwards. Lee Pedowicz discussed the standard.

* Item in Meeting Materials

11. Project 2014-01: Ryan Stewart called into the meeting, provided a brief update on PRC-004-2.1a(X) and PRC-004-4. The goal is to complete this project (including regulatory approval) prior to BES Phase 2 implementation 7/1/2016.

6.1.1 NERC Projects Comment Period Guidelines

Lee Pedowicz gets comments from TFSP and TFIST only.

Lee Pedowicz proposed to provide comments (generated by the Standards Staff) before sending it to the appropriate Task Force.

Chris de Graffenried suggested to have a weekly conference call with the Task Force to discuss comments on posted standards.

Lee Pedowicz suggested to meet with the NPCC Staff who is in charge of the Task Forces and explain to them the work necessary for the comments, Guy Zito approved.

6.2 Ballot History (Since last RSC Meeting)*

Guy Zito reviewed the Ballot History in the meeting.

6.3 Comment Form History (Since last RSC Meeting)*

Guy Zito reviewed the Comment Form History document in the meeting.

7.0 NERC Drafting Team Nominations

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

7.1 Currently Posted Drafting Team Vacancies

7.1.1 None at this time

7.2 Closed Drafting Team Nominations (Since last RSC Meeting)

7.2.1 None at this time

7.3 Solicitation For Informal Development Teams

7.3.1 None at this time

8.0 NPCC Regional Reliability Standards*

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

8.1 Current Activities: Regional Standards Process Manual

8.2 Current Activities: Regional Standard BAL-002-NPCC-01: Regional Reserve Sharing

9.0 NPCC Non-Standards*

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

9.1 Directories:

9.1.1 Directory #1 Design and Operation of the Bulk Power System

Directory #1 has been posted to the Open Process for two 45 day comment periods with the most recent posting concluding on July 7th, 2014.

CO7/CP11 was currently reconvened to address comments, develop draft responses and revise the draft of Directory #1as necessary.

9.1.2 Directory #3 Maintenance Criteria BPS

The TFSP has completed a technical comparison of the criteria within Directory #3 with the FERC approved PRC-005-2 Protection System Maintenance standard and has recommended that the criteria in Directory #3 can be retired.

* Item in Meeting Materials

The TFSP recommendation was posted to the NPCC Open Process and all comments on the TFSP proposal have been addressed.
The RCC approved the TFSP recommendation at its September, 2014 meeting and pending a final ballot of the NPCC Full Members Directory#3 will be retired effective April 1st, 2015.

9.2 Directory Interpretations

TFSP is considering 4 separate clarification requests from the IESO on Directory #3. Clarification Requests now subject to an Open Process posting and RCC approval, in accordance with 2013 RSC approved revisions to the Directory Manual. TFSP expects to post responses to criteria clarification requests in late October.

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

9.3.1 TFCO Retirement of 'C' Documents: C05, C07, C17, C21, C36, C42 and C44

9.4 Directory Manual Revisions (Posting concluded 8-8-2014)

9.4.1 Comment Review and Proposed Responses for RSC Approval

9.4.2 Approval of Directory Manual Revisions

Bruce Metruck made a motion to approve the Directory Manual.
Brian Robinson seconded the motion.
Bruce Metruck withdrew his motion because many members of RSC did not review the manual.
The goal is to have the RSC Members review it on their own first and then have the conference call on September 26th, 2014 (conference call moved to Oct. 3, 2014) so it can be approved.
Gerry Dunbar circulated agenda items to RSC Members in advance of a scheduled October 3rd Conference Call to finalize draft Open Process comment responses and obtain RSC approval of the Directory Manual revisions.

10.0 RSC Member Items of Interest

10.1 RSC Roster*

11.0 Standards Activity Post NERC BOT Approval*

(Since last RSC Meeting)

11.1 NERC Filings to FERC
http://www.nerc.com/FilingsOrders/Pages/default.aspx
Guy Zito provided regulatory updates to the RSC members.

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

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

11.3.1 June 25th, 2014 Geomagnetic Disturbance Operations

11.3.2 June 26th, 2014 Modeling, Data and Analysis Reliability Standards

11.3.3 June 26th, 2014 Reliability Standards Approvals

11.3.4 July 7th, 2014 Generator Relay Loadability and Revised Transmission Relay Loadability Reliability Standards

* Item in Meeting Materials

11.3.5 July 7th, 2014 Physical Security Reliability Standards
11.3.6 July 31st, 2014 Protection System Maintenance Reliability Standards

11.4 FERC Sunshine Act Meeting Notice

11.5 FERC June Open Meeting Summaries

12.0 NERC Meetings

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

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

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

NERC has decided to redo the cost effectiveness document. It is a quality control review as part of the quality review process.

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

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

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

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

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

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

The NPCC Regional Standard Processes Manual (RSPM) was approved at the BOT meeting.

* Item in Meeting Materials

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

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

Fourteen risk profiles were presented at the meeting.

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

13.0 NERC Compliance Tools (Since last RSC Meeting)

Chris de Graffenried suggested to keep this section, but only review when necessary or upon request.

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

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

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

13.2.1 There are seven individual RSAWs and one group RSAWs have been posted for comment since the last RSC meeting:

After discussion around the table regarding a question raised by Lee Pedowicz with regard to whether it's necessary to keep the RSAWs on our Agenda, the final decision is to leave the RSAWs on the Agenda and keep and maintain it. However, the RSC does not need to go over these as a group. The RSC determined that Compliance Committee is the appropriate group to be reviewing the RSAWs.

- Project 2013-03 Geomagnetic Disturbance (GMD) TPL-007-1 issued on 6/27/14 and issued on 9/11/14
- Project 2009-03 Emergency Operations EOP-011-1 issued on 7/18/14
- Project 2014-01 Applicability for Dispersed Generation Resources Standards issued on 7/25/14
- Project 2014-03 Revisions to TOP and IRO Standards issued on 8/26/14
- Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings and Lens Characteristic Tool issued on 9/10/14
- Project 2008-02 Underfrequency Load Shedding (UFLS) PRC-006-2 issued on 9/10/14
- Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves BAL-002-2 issued on 9/11/14

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

13.3.1 There have not been any new CANs posted since the last RSC meeting

* Item in Meeting Materials

14.0 NERC Items of Interest (Since last RSC Meeting)

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

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

- LL20140601 - Relay and Protection System - Generation Relaying - Underfrequency Protection Coordination

  Issued 6/19/2014

  Primary Interest Groups: Generator Owners (GOs)

- LL20140602 - Relay and Protection System - Generation Relaying - Overexcitation

  Issued 6/19/2014

  Primary Interest Groups: Generator Owners (GOs)

- LL20140603 - Bulk-Power System Operations - Verify That Actions Called for in Operating Guides Can Be Implemented Within Required Time Frames

  Issued 6/19/2014

  Primary Interest Groups: Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), Transmission Owner (TO)

- LL20140604 - Communications - Loss of SCADA Due to Memory Resources Being Fully Utilized

  Issued 6/19/2014

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

- LL20140801 - Bulk-Power System Operations - Load-Shedding Plans for Localized Events

  Issued 8/5/2014

  Primary Interest Groups: Transmission Operator (TOP), Transmission Owner (TO), Balancing Authority (BA), Load Serving Entity (LSE), Generator Operator (GOP)

- LL20140802 - Communications - Loss of EMS Monitoring and Control Functionality for More Than 30 Minutes

  Issued 8/5/2014

  Primary Interest Groups: Reliability Coordinator (RC), Transmission Operator (TOP), Transmission Owner (TO), Generator Operator (GOP)

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

14.2.1 There has been no new NERC Alert released since the last RSC meeting.

14.3 Five Year ERO Performance Assessment

15.0 Other Items of Interest

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

15.2 2015 Regional Entity Business Plans and Budgets

15.3 Quality Review of NERC Standards

October 15th, and 16th, Risk Base Registration Workshop for TOs and TOPs.

16.0 Future RSC Meetings and Conference Calls

16.1 RSC 2014/2015 Meeting Dates

RSC members agreed on the dates for the next meeting at NextEra Energy Office in Juno Beach, Florida Wednesday-Thursday, February 18th-19th, 2015.

Guy proposed the following dates for 2015 RSC meetings:

April 15th and 16th at Dominion's Offices in Richmond VA.

June 23rd and 24th in Saratoga Spring NY.

October 7th and 8th in Montreal Canada.

December 3rd and 4th in Albany NY.

Set up a conference call schedule with Lee Pedowicz based on this tentative face-to-face meeting schedule.

Feb. 19th – 20th, 2014 NextEra Energy Offices
April 10th & 11th, 2014 NPCC Offices
June 18th & 19th, 2014 Saratoga, NY
September 17th & 18th, 2014Montreal, Quebec
December 4th & 5th, 2014 Halifax, Nova Scotia
February 18-19, 2015, NextEra Energy Offices

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

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

* Item in Meeting Materials

The meeting adjourned at 10:46AM on Thursday, September 18, 2014.

Respectfully Submitted,

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

* Item in Meeting Materials

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 212-335-4765.

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

Source = NERC Standard Drafting Team Rosters - March 2014

Change Control: Changes Since March 2014:

Projects Removed:

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

Projects Added:

1. Project 2014-04, Physical Security

NPCC Representative Changes:

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

Revised: #REF!

Tab Name	Last Revised	Summary of Changes
NERC RS Exec Tracking Summary	11/26/2014	
NERC RSAWs	11/26/2014	
NPCC RRS Tracking Summary	#REF!	- Regional Standard Processes Manual; Following NPCC BOD approval, NERC posted the proposed NPCC Regional Standard Processes Manual for a 45-day industry review through 8 p.m. Eastern on Wednesday, May 7, 2014
NPCC Doc Tracking Summary	#REF!	- C-00 (Discontinued) - C-05 (Retired) - C-07 (Retired) - C-21 (Retired) - C-44 (Retired)
NPCC Directory Tracking Summary	#REF!	- Directory #1, Design and Operation of the Bulk Power System posted in Open Process - Directory Development and Revision Manual - Comment Response Document posted
NPCC Directory Interpretations	#REF!	- Directory #3 Interpretation on behalf of Hydro One Networks included
Quarterly Filing to NSUARB	#REF!	Annotated worksheet to indicate that "Revisions to D#7 and D#12 approved by the Full Members on 7/9/2013. "

Prior Revision

Tab Name	Last Revised	Summary of Changes

NERC Reliability Standards Executive Tracking Summary

Revised: 11/26/2014

Line No.	Project No. / Title	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status	
2	2012-INT-07 - Interpretation of CIP-005 for AEP									This interpretation is being prepared for an initial 30-day formal comment period.		
6	Project 2007-06 — System Protection Coordination	PRC-001-3, PRC-027-1	Yes 1st (Thru 7/10/07)	Yes (PRC-027-1 Thru 12/31/13)	Yes (PRC-027-1 Additional Thru 12/31/13)						Under Development	
8	Project 2007-11 — Disturbance Monitoring	PRC-002-2	Yes 1st (Thru 4/20/07)	NA	Yes (Final 11/6/14)	Yes (11/6/14)	Yes (11/13/14)	Pending for Approval			Under Development	x
12	Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays)	PRC-005-4	Yes (Informal Thru 3/14/14)	Yes (Formal Thru 6/2/14)	Yes (Inital Thru 6/2/14)							
13	Project 2008-01 — Voltage and Reactive planning and control (Informal Development Project)	VAR-001 and VAR-002	Yes 2nd (Thru 3/26/10)								Under Development	
14	Project 2008-02 — Undervoltage Load Shedding	PRC-006-2	Yes (Thru 10/9/13)	N/A	Yes (Final Thru 10/31/14)	Yes (10/31/14)	Yes (11/13/14)	Pending for Approval			Under Development	x
18	Project 2009-02 — Real-time Reliability Monitoring and Analysis Capabilities	"New"	Yes 2nd (Thru 2/18/10)	Yes 1st (Informal Thru 4/4/11)						Concept White Paper posted for informal comment period	Under Development	x
19	Project 2009-03 — Five-Year Review of Emergency Operations EOP-001, EOP-002, EOP-003, and IRO-001	EOP-001-2b, EOP-002-3, EOP-003-1, EOP-004-2 (P81, RBS), EOP-005-2 (P81, RBS), EOP-006-2 (RBS), EOP-008-1 (RBS), EOP-009-1, IRO-001-5	Yes (Thru 12/5/13)	NA	EOP-011-1 Yes (Final Thru 11/6/14)					Project initiated as a 5-year review to clarify scope, avoid potential concurrent revisions to EOP standards (Cold weather SAR)	Under Development	
20	Project 2009-04 — Phasor Measurement Units										Project has not started	
21	Project 2009-05 — Resource Adequacy Assessments	"New"	Yes 2nd (Thru 3/30/06)								Under Consideration for Development	
22	Project 2009-07 — Reliability of Protection Systems	"New"	Yes 1st (Thru 2/18/09)							Pending prioritization - may be postponed	Under Consideration for Development	
24	Project 2009-20 — Interpretation of BAL-003-0 R2 and R5 by Energy Mark, Inc.	BAL-003-0.1b	x	x	Yes (Recirc Thru 2/26/10)	Yes (2/26/10)					Under Development	
27	Project 2010-02 — Connecting New Facilities to the Grid	FAC-001, FAC-002, FAC-003-3, FAC-008-3, FAC-010-2.1, FAC-011-2, FAC-013-2, FAC-014-2	Yes (Informal Thru 1/17/14)	Yes (Formal Thru 5/15/14)	Yes (Final Thru 6/23/14)	Yes (6/23/14)	Yes (8/14/14)	Yes (8/22/14)		Two projects (FAC Review, Project 2010-02) were consolidated and are being initiated as a 5-year review		
30	Project 2010-05.1 — Protection Systems: Phase 1 (Misoperations)	PRC-004-3	Yes 1st (Informal Thru 7/11/11)	Yes (Formal Thru 7/9/14)	Yes (Final Thru 8/7/14)	Yes (8/7/14)	Yes (8/14/14)	Pending for Approval		Ballot will be extended one day at a time to achieve a quorum.	Under Development	
31	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)	RAS Definition	Yes (Informal Thru 3/19/14)	NA	Yes (Final Thru 11/6/14)	Yes (11/6/14)	Yes (11/13/14)	Pending for Approval				
32	Project 2010-06 — Results-based Reliability Standards	Results-based Reliability Standards Transistion Plan								Transistion Plan posted 7/26/10		
36	Project 2010-13.3 Relay Loadability: Stable Power Swings	PRC-026-1	For Comment (Thru 9/19/10)	Yes (Formal Thru 12/24/14)	Yes (Additional Thru 12/24/14)							
38	Project 2010-14.1 — Phase 1 of Balancing Authority Reliability-based Control: Reserves	BAL-002-2	NA	Yes (Formal Thru 12/11/14)	Yes (Additional Thru 12/12/14)					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		
39	Project 2010-14.2 Periodic Review of BAL Standards	BAL-004, BAL-005-0.1b, BAL-006-2	Yes (Thru 8/14/14)							A 30-day informal comment period for BAL standards (SAR) is now open through 8/14/14.	Under Development	
40	Project 2010-16 — Definition of System Operator	NERC Glossary Of Terms	Yes 1st (Thru 12/3/10)	Yes 1st (Thru 12/3/10)							Under Consideration for Development	
43	Project 2010-INT-03 Interpretation of TOP-002-2a R2, R8, and R19 for FMPP	TOP-002-2a, R2, R8 and R19								Standards Committee curtailed work in April 2011 - revived in January 2012 to see if a Rapid Revision was feasible. Overtaken by filing of TOP standards.		
45	Project 2012-01 Equipment Monitoring and Diagnostic Devices	FUTURE										
46	Project 2012-02 Physical Protection	FUTURE										
49	Project 2012-08.2 — Phase 2 of Glossary Updates	NERC Glossary Of Terms								Modify existing definition of Transmission Operator and Generator Operator		
50	Project 2012-09 IRO Five-Year Review	Various IRO standards	x	Yes (Thru 9/20/13)						Five year review	Under Development	
51	Project 2012-13 NUC - Nuclear Plant Interface Coordination	NUC-001-2.1	Yes (Informal Thru 3/13/14)	Yes (Formal Thru 5/22/14)	Yes (Final Thru 7/3/14)	Yes (Final Thru 7/3/14)	Yes (8/14/14)	Pending for Approval		Five year review		
52	Project 2012-INT-03 Interpretation of CIP-007 for TECO									This interpretation is on hold pending finalization of Project 2012-INT-04 (Interpretation of CIP-007 for ITC).		
55	Project 2013-01 — Cold Weather Preparedness	"TBD"	Draft for Comment (Thru 10/24/12)									
57	Project 2013-03 Geomagnetic Disturbance Mitigation, Stage 2	TPL-007-1	NA	Yes (Formal Thru 11/21/14)	Yes (Additional Thru 11/21/14)							
59	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	PRC-001-1x1(X), PRC-019-2 and PRC-024-1(X)	Yes (Thru 12/19/13	Yes (Formal Thru 12/19/14)	Yes (Initial Thru 12/19/14)							
60	Project 2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions	CIP	Yes (Thru 2/18/14)	Yes (Formal Thru 1/8/15)	Yes (Additional Thru 1/8/15)							
61	Project 2014-03 Revisions to TOP and IRO Standards	TOP-001-3	Yes (Formal Thru 3/24/14)	Yes (Formal Thru 11/10/14)	Yes (Additional Thru 11/10/14)							
62	Project 2014-04 Physical Security		Yes (Informal Thru 3/28/14)	Yes (Formal Thru 4/24/14)	Yes (Initial Thru 4/24/14)							

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 Reliability Standard Audit Worksheet (RSAW) Executive Tracking Summary

Revised: **11/26/2014**

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

RSAW#	Title	Posted for Comment?	RSAW Issued?	Comments
BAL-001-1	Real Power Balancing Control Performance	x	3/28/2014	New RSAW Posted
BAL-00202	Contingency Reserve for Recovery from Balancing Contingency Event	x	8/19/2014	Draft RSAW Posted
BAL-003-0.1b	Frequency Response and Bias	x	3/20/2014	
BAL-005-0.2b	Automatic Generation Control	x	5/20/2013	Revised RSAWs Posted
CIP-001-2a	Sabotage Reporting	x	10/13/2012	
CIP-002-5.1	Cyber Security - BES Cyber System Categorization	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-003-6	Cyber Security - Security Management Controls	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-004-6	Cyber Security - Personnel & Training	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-007-6	Cyber Security - System Security Management	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-009-6	Cyber Security - Security Management Controls	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-011-2	Cyber Security - Information Protection	Yes (Thru 10/17/14)	9/17/2014	Draft RSAW Posted
CIP-014-1		Yes (thru 4/24/14)		
COM-002-2a	Communication and Coordination	x	11/14/2012	
COM-002-4	Operating Personnel Communications Protocols	Yes (Thru 1/31/14)		
COM-003-1	Operating Personnel Communications Protocols	Yes (Thru 4/5/13)		
EOP-001-2.1b	Emergency Operations Planning	x	8/9/2013	Revised RSAWs Posted
EOP-002-3.1	Capacity and Energy Emergencies	x	3/20/2014	Revised RSAWs Posted
EOP-003-2	Load Shedding Plans	x	10/13/2012	
EOP-004-2	Event Reporting	N/A	10/15/2013	New RSAW
EOP-005-2	System Restoration from Blackstart Resources	x	7/17/2013	Revised RSAWs Posted
EOP-006-2	System Restoration Coordination	x	7/17/2013	Revised RSAWs Posted
EOP-008-1	Loss of Control Center Functionality	x	6/28/2013	Revised RSAWs Posted
EOP-011-1	Emergency Operations	Yes (Thru 9/25/14)	1-/20/2014	Draft RSAW Posted
FAC-001-2	Facility Interconnection Requirements	Yes (Thru 6/25/2014)		The draft RSAW is posted for feeback through June 25, 2014.
FAC-002-2	Facility Interconnection Studies	Yes (Thru 6/25/2014)		The draft RSAW is posted for feeback through June 25, 2014.
FAC-003-3	Transmission Vegetation Management	N/A	4/24/2014	Revision serves to clarify guidance for Requirement R6 regarding initial inspections for calendar year 2014 by expanding the Note to Auditor section
FAC-008-3	Facility Ratings	x	3/20/2014	Revised RSAWs Posted
FAC-013-2	Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon	x	10/13/2012	
IRO-001-4	Reliability Coordination- Responsibilities	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
IRO-002-2	Reliability Coordination - Facilities	x	3/20/2014	
IRO-002-4	Reliability Coordination - Monitoring and Analysis	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
IRO-003-2	Reliability Coordination - Wide-Area View	x	3/20/2014	
IRO-005-3.1a	Reliability Coordination - Current-Day Operations	x	5/20/2013	Revised RSAWs Posted
IRO-008-2	Reliability Coordinator Operational Analyses and Real-time Assessments	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
IRO-010-2	Reliability Coordinator Data Specification and Collection	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
IRO-014-1	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators	x	10/13/2012	
IRO-014-3	Coordination Among Reliability Coordinators	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
IRO-017-1	Outage Coordination	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
MOD-028-2	Area Interchange Methodology	N/A	10/10/2013	New RSAW

RSAW#	Title	Posted for Comment?	RSAW Issued?	Comments
MOD-031-1	Demand and Energy Data	Yes (Thru 11/22/13)		Draft RSAW posted along with Draft Standard
NUC-001-2		N/A	4/24/2014	Revised RSAW represent the initial release for the errata versions of the Reliability Standard
PER-001-0.2	Operating Personnel Responsibility and Authority	x	5/20/2013	Revised RSAWs Posted
PER-003-1	Operating Personnel Credentials	x	1/23/2013	
PER-005-1	System Personnel Training	N/A	10/15/2013	Revised RSAWs Posted
PRC-001-1	System Protection Coordination	N/A	4/24/2014	Revised RSAW represent the initial release for the errata versions of the Reliability Standard
PRC-002-NPCC-01	Disturbance Monitoring	Yes (Thru 10/21/2014)	9/19/2014	Revised RSAWs Posted
PRC-004-2.1a	Analysis and Mitigation of Transmission and Generation Protection System Misoperations	x	3/28/2014	Revised RSAWs Posted
PRC-004-3	Protection System Misoperation Identification and Correction	Yes (Thru 3/19/14)		Draft RSAW posted along with Draft Standard
PRC-005-1.1b	Transmission and Generation Protection System Maintenance and Testing	x	3/28/2014	Revised RSAWs Posted
PRC-006-2	Automatic Underfrequency Load Shedding	Yes (Thru 10/8/14)	9/10/2014	Revised RSAWs Posted
PRC-010-1	Undervoltage Load Shedding	Yes (Thru 8/7/2014)		
PRC-023-2	Transmission Relay Loadability	N/A	10/10/2013	Revised RSAWs Posted
PRC-025-1	Generator Relay Loadability	Yes (Thru 3/11/13)		
PRC-026-1	Relay Peformance During Stable Power Swings	Yes (Thru 12/2/2014)	11/12/2014	Draft RSAW Posted
TOP-001-1a	Reliability Responsibilities and Authorities	x	5/20/2013	Revised RSAWs Posted
TOP-001-3	Transmission Operations	Yes (Thru 11/10/2014)	10/16/2014	Revised RSAWs Posted
TOP-002-2.1b	Normal Operations Planning	x	3/20/2014	Revised RSAWs Posted

NPCC Regional Reliability Standards Executive Tracking Summary

Revised: 3/24/2014

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 (11/18/11)	Yes (11/30/11)	Yes (2/9/12)	Yes (5/4/12)	Yes (2/21/13)		Completed
4	PRC-002-NPCC-02										- Regional Standard Authorization Request (RSAR) has been submitted and approved - Drafting Team Nomination period ended March 25, 2013 - Draft Team kick-off conference call was Monday April 8, 2013	Under Development
5	PRC-002-NPCC-01, Interpretation R1.1		x	x	x	Yes (TFSP 10/19/12)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
6	PRC-002-NPCC-01, Interpretation R1.2.2		x	x	x	Yes (TFSP 4/8/13)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
7	PRC-002-NPCC-01, Interpretation R4, R5, and R6		x	x	x	Yes (TFSP 5/16/13)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
8	BAL-002-NPCC-01	Regional Reserve Sharing	Yes (Thru 11/2/10)	Yes (Thru 12/16/11)	Yes (Thru 1/6/10)						Nomination Form posted - nominations due by 11/10/11	Under Development
9	PRC-012-NPCC-01	Special Protection Systems	Yes (thru 8/18/08)									On Hold
10	Regional Standard Processes Manual	Regional Standard Processes Manual (RSPM)	N/A	Yes (Thru 10/20/13)	Yes (Thru 1/27/14)	Yes (1/27/14)	Yes (3/11/14)				NERC posted the proposed NPCC Regional Standard Processes Manual for a 45-day industry review through 8 p.m. Eastern on Wednesday, May 7, 2014	

x

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: 11/25/2014

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

Line No.	Type	Document	Description	Latest Revision	Comments	Status
1	Criteria	A-01	Criteria for Review and Approval of Documents	Mar-05		
2	Criteria	A-10	Classification of BPS Elements	Dec-09		
3	Criteria	A-15	Disturbance Monitoring Equipment Criteria	Aug-07		
4	Guideline	B-01	NPCC Guide for the Application of Autoreclosing to the Bulk Power System	Feb-13		
5	Guideline	B-12	Guidelines for On Line Computer System Performance During Disturbances	Nov-07		
6	Guideline	B-25	Guide to Time Synchronization Substation Equipment	Nov-08		
7	Guideline	B-26	Guide for Application of Disturbance Recording Equipement	Sep-06		
8	Guideline	B-27	Regional Critical Asset Identification Methodology	Feb-08		
9	Guideline	B-28	Guide for Generator Sequence of Events Monitoring	Feb-12		
10	Procedure	C-01	NPCC Emergency Preparedness Conference Call Procedures - NPCC Security Conference Call Procedures	May-13		
11	Procedure	C-15	Procedures for Solar Magnetic Disturbances Which Affect Electric Power Systems	Jan-07		
12	Procedure	C-25	Procedure to Collect Power System Event Data	Sep-07		
13	Procedure	C-29	Procedures for System Modeling:Data Requirements and Facility Ratings	Mar-07		
14	Procedure	C-30	Procedure for Task Force on System Protection Review of Disturbances and Protection Misoperations	Dec-09		
15	Procedure	C-33	Procedure for Analysis and Classification of Dynamic Control Systems	Apr-06		
16	Procedure	C-39	Procedure to Collect Major Disturbance Event Data	Dec-09		
17	Procedure	C-43	NPCC Operational Review for the Integration of New facilities	Aug-08		
18	Procedure	C-45	Procedure for Analysis and Reporting of Protection System Misoperations	Nov-14		

NPCC Directory Executive Tracking Summary

Revised: **11/25/2014** Further details regarding the individual documents may be found at:

Line No.	Document	Developed From	Title of Directory	Responsible Task Force	Latest Version	Comments	Status	
1	Directory #1	Criteria A-2	Design and Operation of the Bulk Power System	TFCP	Dec-09	CP11/CO7 Reviewing Phase 2 Draft	CO7/CP11 has completed drafting responses to comments received in the 2nd Open Process Posting and has returned the draft to the TFCO and TFCP.	x
2	Directory #2	Criteria A-3	Emergency Operations	TFCO	Jun-09			
3	Directory #3	Criteria A-4	Maintenance Criteria for Bulk Power System Protection	TFSP	Jun-09	TFSP has completed a Technical Comparision of D#3 with PRC-005-2 and has recommended that D#3 can be retired.	RCC approved the TFSP retirement recommendation and on October 15th, 2014 the NPCC Full Members approved the retirement of D#3 effective April 1st, 2015 to coincide with the enforcement date of PRC-005-2.	
4	Directory #4	Criteria A-5	Bulk Power System Protection Criteria	TFSP	Dec-09	TFSP reviewing D#4 in accordance with NRAP review.	TFSP anticipates posting D#4 to the Open Process by December 2014.	
5	Directory #5	Criteria A-6	Reserve	TFCO	Oct-12			
6	Directory #6		Regional Reserve Sharing		Apr-12			
7	Directory #7	Criteria A-11	Special Protection Systems	TFSP	Jul-13			
8	Directory #8	Criteria A-12	System Restoration	TFCO	Oct-10	TFCO working group CO11 reviewing initial Phase 2 draft of Directory #8.	TFCO anticipates posting D#8 to the Open Process by December 2014.	
9	Directory #9	Criteria A-13	Verification of Generator Gross and Net Real Power Capability	TFCO	Dec-11			
10	Directory #10	Criteria A-14	Verification of Generator Gross and Net Reactive Power Capability	TFCO	Dec-11			
11	Directory #12		Under frequency Load Shedding Program Requirements	TFSS	Jul-13		NPCC anticipates retiring Directory#12 once PRC-006-NPCC-1 is fully implemented.	
12	Directory Manual		Directory Development and Revision Manual	N/A	Dec-13		On October 6th, 2014 the RSC approved revisions to the Directory Manual which incorporated cost considerations into the development of new or revised criteria as mandated by the NPCC BOD.	x

NPCC Directory Criteria Clarifications

Revised: **11/25/2014** Further details regarding the individual documents may be found at: https://www.npcc.org/Standards/Directory%20Interpretations/Forms/Public%20List.aspx

Line No.	Document	Title of Directory	Date Final	Task Force Review	Posted Open Process?	RCC Approval	Comments	Status
1	Directory #8 Interpretation	System Restoration	6/18/2012	TFCO	N/A	N/A	Interpretation on behalf of the NYSRC	Complete
2	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	8/28/2012	TFSP	N/A	N/A	Interpretation on behalf of Bangor Hydro	Complete
3	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	12/14/2012	TFSP	N/A	N/A	Interpretation on behalf of Con Ed	Complete
4	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	2/15/2013	TFSP	N/A	N/A	Response Clarified - Interpretation on behalf of Acumen Engineered Solutions	Complete
5	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	10/25/2013	TFSP	N/A	N/A	Interpretation on behalf of Hydro One Networks	Complete
6	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	Pending	TFSP	Yes on October 16th, 2014.			Criteria Clarification Request on behalf of the IESO-Market Assessment and Compliance Division (MACD) posted to Open Process until Nov. 30th, 2014.

x

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

Revised: **11/25/2014**

Line No.	Filing Period	Filing Due	Filing Submitted	Comments
1	October 1 to December 31, 2012	3/1/2013	3/1/2013	This filing is NPCC's initial quarterly filing covering the October 1 to December 31, 2012 period and covers the changes to the NPCC Criteria as a result of voting by the Full Members of NPCC.
2	January 1 to March 31, 2013	6/1/2013	N/A	No changes were made during the refeenced period which required filing.
3	April 1 to June 30, 2013	9/1/2013	N/A	No changes were made during the referenced period which required filing.
4	July 1 to September 30, 2013	12/1/2013	11/25/2013	Revisions to D#7 and D#12 approved by the Full Members on 7/9/2013.
5	October 1 to December 31, 2013	3/1/2014	N/A	No changes were made during the referenced period which required filing.
6	January 1 to March 31, 2014	6/1/2014	N/A	No changes were made during the referenced period which required filing.
7	April 1 to June 30, 2014	9/1/2014	N/A	No changes were made during the referenced period which required filing.
8	July 1 to September 30, 2014	12/1/2014	N/A	No changes were made during the referenced period which required filing.
9	October 1 to December 31, 2014	3/1/2015		10/15/14 NPCC Full Members approved retirement of D#3 effective 4/01/15 coinciding with enforcement date of PRC -005-2.

Milestone Keys:

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

Project Status

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

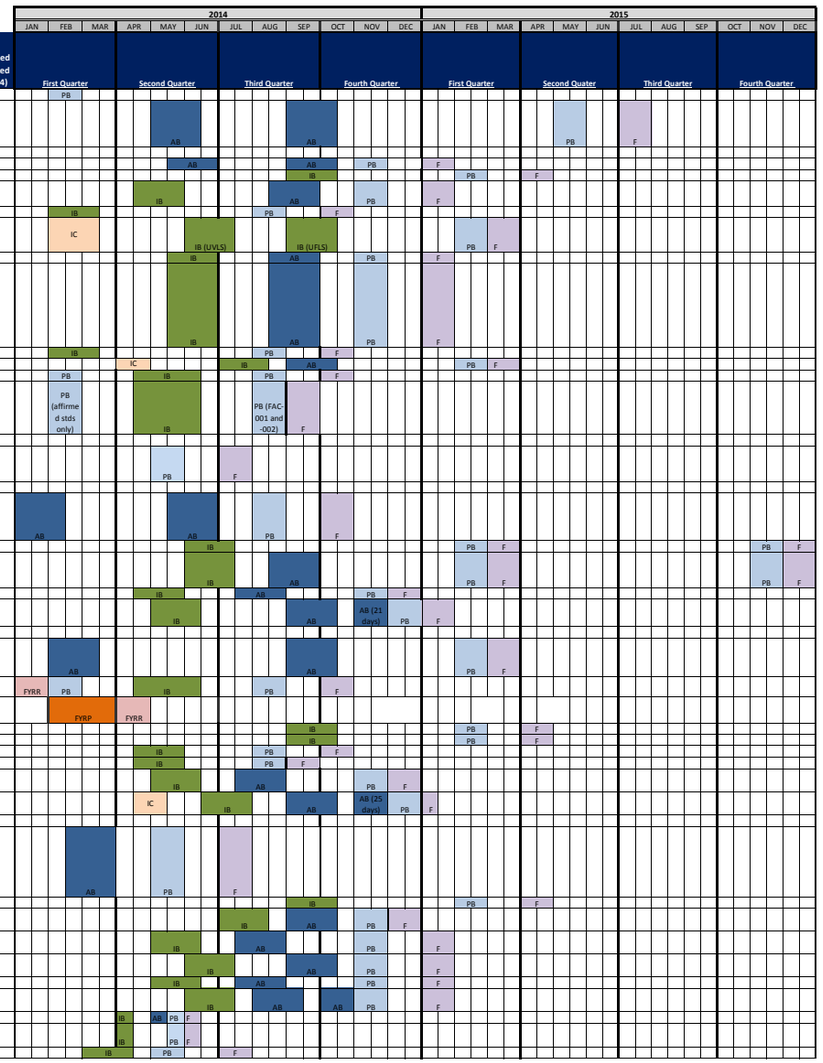
Project Tracking Spreadsheet: 2014 Project Work Plan (Status Updated: 11/19/2014)

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

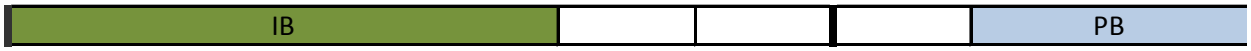
Projected Posting Schedule

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

Project Number	Activity/Project (Project Names Hyperlinked to Project Page)	Deliverable	Deadline, if any	Priority in 2014-2016 RSDP, if applicable (see Note 1, below)	2013 PB1 Reqs	Number of Directives	# of Guidances (see Note 2)	Directionally consistent with IERP findings	Comments	PMOS Liaison	NERC Contact	Status: Green, Yellow, Red	Milestones: Planned vs. Actual/Projected (See Notes 3 and 4)
2007-06	System Protection Coordination	PRC-001, PRC-027		N/A		1		Yes	A 21-day informal comment period for the preliminary draft 5 of PRC-027-1 concluded on October 21. The SDT will not respond but will consider the comments at its upcoming meetings.	Jennifer Sterling	Al McMeekin	Project extended to address an additional issue by FERC	Plan Actual/Projected
2007-11	Disturbance Monitoring	PRC-002, PRC-018		Medium	2		1	Yes	Passed final ballot.	Jennifer Sterling	Steve Crutchfield		Plan Actual/Projected
2007-17.3	Protection System Maintenance: Sudden Pressure Relays	PRC-005		Medium (prioritized by SC March 2014)	1	1		Yes	Passed final ballot.	Charles Yeung	Jordan Mallory		Plan Actual/Projected
2008-02	Undervoltage Load Shedding and Underfrequency Load Shedding	PRC-010, PRC-022, PRC-006, PRC-004		High	2	1	1	Yes	PRC-010-1 and PRC-006-2 passed final ballot. Next Step is to request authorization to post revised PRC-004 that includes UVLS.	Jennifer Sterling	Katherine Street (UVLS) and Lacey Ourso (UFLS)	Delayed to coordinate with the development of the SPS definition	Plan Actual/Projected
2009-02	Real-time Reliability Monitoring and Analysis Capabilities	New Standards or revisions to TOP and IRO standrds	January 31, 2015 deadline to address concerns in NOPR proposing to remand TOP/IRO standards	High		2		TBD	January 31, 2015 deadline to address concerns in NOPR proposing to remand TOP/IRO standards; the directives associated with this project are being addressed in Project 2014-03; consider consolidating the two projects on this spreadsheet.	Jennifer Sterling	Ed Dobrowolski		Plan Actual/Projected
2009-03	Emergency Operations	EOP-001, EOP-002, EOP-003 being replaced by EOP-011		High	14	3	2	Yes	Passed final ballot.	Gary Kruempel	Laura Anderson	Delayed to coordinate with UVLS balloting	Plan Actual/Projected
2010-02	Connecting new facilities to the grid/Five-year Review of FAC standards	FAC-001, FAC-002		Low		1	1	Yes	Passed final ballot.	Ken Goldsmith	Mallory Huggins		Plan Actual/Projected
2010-04	Demand Data (MOD C)	MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, MOD-021		N/A	10	10	4	Yes	Passed final ballot.	Scott Miller	Darrel Richardson		Plan Actual/Projected
2010-05.1	Phase 1 of Protection Systems: Misoperations	PRC-003, PRC-004		N/A			2	Yes	Passed final ballot.	Jennifer Sterling	Scott Barfield		Plan Actual/Projected
2010-05.2	Special Protection Systems: Phase 2 of Protection Systems	PRC	Self-imposed deadline for definition of SPS is February 2015 for coordination with other PRC projects.	Medium				Yes	Passed final ballot.	Jennifer Sterling	Al McMeekin		Plan Actual/Projected
2010-13.3	Relay Loadability Stable Power Swings	PRC	December 31, 2014 deadline to address phase 3 directives covered by this project	Medium (prioritized by SC March 2014)		3		n/a	Additional 21-day comment and ballot period will conclude on November 24, 2014.	Charles Long	Scott Barfield		Plan Actual/Projected
2010-14.1	BARC Directives and Issues-Project 2010-14.1 Balancing Authority Reliability-based Controls	BAL-001, BAL-002, BAL-013		N/A	4			Yes	BAL-002-2 did not pass additional ballot. An additional comment period and ballot will be conducted that concludes in January.	Ron Parsons	Darrel Richardson	Project extended to address an additional issue raised by FERC	Plan Actual/Projected
2010-14.2	Phase 2 of Balancing Authority Reliability-based Control: Time Error, AGC, and Inadvertent	BAL-005-0.1b, BAL-006-2		Medium	11	7	6	Yes	An informal comment period concluded on August 14, 2014.	Ken Goldsmith	Sean Cavote		Plan Actual/Projected
2012-09	Implementation of IRO Review Recommendations	IRO-003, IRO-004, IRO-008, IRO-009, IRO-010		Medium	2	2		On hold pending TOP/IRO project	Many FYRT recommendations being addressed in Project 2014-03	Brian Murphy	Soo Jin Kim		Plan Actual/Projected
2012-13	Implementation of NUC Review Recommendations	NUC-001		Low				Yes	Passed final ballot.	PMOS Oversight	Stephen Eldridge		Plan Actual/Projected
2013-03	Geomagnetic Disturbance Mitigation, Stage II	TPL-007	FERC filing deadline of January 21, 2015	High		14		n/a	A 25-day formal comment period and ballot will conclude on November 21, 2014.	Brian Murphy	Mark Olson		Plan Actual/Projected
2013-04	VAR Directives	VAR-002		N/A	3	6	5	Yes	Passed final ballot.	Ron Parsons	Soo Jin Kim		Plan Actual/Projected
2014-01	Standards Applicability for Dispersed Generation Resources	Various	Goal is to complete (including regulatory approval) prior to BES Phase 2 implementation 7/1/2016	Medium (prioritized by SC January 2014)				n/a	PRC-004-2.1a, PRC-004-3, PRC-005-2, PRC-005-3, and VAR-002-3 passed final ballot. PRC-001-1.1(X), PRC-019-2, and PRC-024-	Gary Kruempel	Sean Cavote		Plan Actual/Projected
2014-02	CIP Version 5 Revisions	CIP	FERC filing deadline for certain directives of February 3, 2015.	High (prioritized by SC March 2014)		8		n/a	Standards addressing two time-sensitive directives passed final ballot. Standards incorporating four directives will be posted for an additional comment period	Scott Miller	Marisa Hecht and Ryan Stewart		Plan Actual/Projected
2014-03	TOP/IRO Revisions	TOP/IRO	Deadline of January 31, 2015	High (prioritized by SC March 2014)				TBD	8 of 9 standards passed final ballot. Remaining standard (TOP-001-3) posted for comment and ballot concluding in	Brian Murphy	Ed Dobrowolski		Plan Actual/Projected
2014-04	Physical Security	CIP-014	Deadline of June 5, 2014			7		n/a	Passed final ballot.	Brian Murphy	Steve Crutchfield		Plan Actual/Projected
			Goal is to complete directives and										Plan



| | | |


IB
PB

		F

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

Item	Description	Owner	Due	Status
4.1	Coordination with the Compliance Committee to develop Joint Activity Action List	Greg Campoli	RSC Meeting	Ongoing RSC decided that it was not necessary to have a joint meeting with CC at the December, 2014 meeting in Halifax.
4.2	New York Adoption of More Stringent/Specific NPCC Criteria - determine more stringent criteria and submit filing	Gerry Dunbar	April 2014	Update: NPCC Executive Staff is providing additional comments. NPCC expects the document to be filed with the NYSPSC by late September pending final NPCC legal review. RSC Members will be notified when the document is filed.
13-5.6	NPCC outreach program development – discussion item: members provide input and opportunities for development of an outreach program	RSC	RSC Meeting	Update: Ongoing, two outreaches have been done with NYPA.
14-1.2	Revise the Directory Development Manual to address cost effectiveness	G. Dunbar		Update: Revisions to the Directory Manual posted to the NPCC Open Process from May, 2014 to July, 2014. Draft RSC responses to Open Process comments and final approval of Directory Manual revisions pending final RSC review and approval.
14-1.4	Follow up with NERC on current RSAW development process	Guy Zito		Update: After discussion the RSC members decided to not immediately address this, but wait for new items to be published.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Weekly Standards & Compliance Bulletin

November 24–30, 2014

SPOTLIGHT ON THE RELIABILITY ASSURANCE INITIATIVE

Please note that this will be the final separate "Spotlight on the Reliability Assurance Initiative." Now that all foundational program guides and documents have been posted to the RAI web page and RAI as a separate initiative is being folded into NERC's overall risk-based Compliance Monitoring and Enforcement Program, NERC will announce all future compliance monitoring and enforcement news below, under "General Compliance and Enforcement News."

Coordinated Oversight of MRREs

The ERO Enterprise is beginning the initial implementation of a program for Coordinated Oversight of Multi-Regional Registered Entities (MRREs). An MRRE is a registered entity that has a single NERC Compliance Registry number in more than one Region or affiliated registered entities in multiple Regions with multiple NCR numbers. Under Coordinated Oversight, a Lead Regional Entity is selected from among the Regional Entities that currently have oversight of the MRRE to coordinate the performance of delegated functions.

Coordinated Oversight is intended to streamline risk assessment, compliance monitoring and enforcement, and event analysis activities for the MRRE. Further, Coordinated Oversight may result in reduced administrative burdens for the MRRE and improved consistency.

In the coming weeks, the ERO Enterprise will send notification letters to an initial list of 43 groups of MRREs, totaling over 150 individual registered entities. The MRREs notified in this initial round will have the option to begin participation in the initial implementation of the Coordinated Oversight program. The notification letters will contain a summary of the protocols the Regional Entities will use to assure coordination of delegated activities. Among other things, these activities include receiving self-reports, conducting compliance audits, handling technical feasibility exceptions, conducting enforcement actions, and handling responses to NERC Alerts.

In June 2015, the Coordinated Oversight program will be fully implemented across the ERO Enterprise. At this time, all registered entities may notify their Regional Entities of their interest in Coordinated Oversight and request to participate or request additional information. Also at this time, registered entities that declined to participate during the initial implementation may request to participate.

Additional information about the Coordinated Oversight program for MRREs, including a Frequently Asked Questions document, is available here.

Final 2015 ERO CMEP Implementation Plan Posted

The final 2015 ERO Compliance Monitoring and Enforcement Implementation Plan, which incorporates each Region's Implementation Plan, is now available under "Key Resources" on the RAI web page.

Resources Available for RAI Industry Outreach Workshops

NERC thanks all stakeholders who attended the November 6 and November 20 RAI Industry Outreach Workshops in Phoenix and Atlanta. The slide presentation from the November 20 event, and the slide presentation and streaming webinar from the November 6 event, are available on the RAI Workshops & Webinars page. The streaming webinar from the November 20 event will be posted soon.

ACTIVE STANDARDS POSTINGS

Current and Upcoming Ballots (ballot periods close at 8:00 p.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings – PRC-026-1	Additional Ballot and Non-Binding Poll	11/14/14	11/24/14
Project 2014-01 - Standards Applicability for Dispersed Generation Resources – PRC-001-1.1(X), PRC-019-2, PRC-024-1(X)	Initial Ballots	12/10/14	12/19/14

Join Ballot Pools (ballot pool windows close at 8:00 a.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2014-01 - Standards Applicability for Dispersed Generation Resources – PRC-001-1.1(X), PRC-019-2, PRC-024-1(X)	Join Ballot Pools	11/05/14	12/04/14

Posted for Comment (comment periods close at 8:00 p.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings – PRC-026-1 A draft RSAW has been posted for feedback through December 2, 2014. Please submit comments to RSAWfeedback@nerc.net.	Comment Form	11/04/14	11/24/14
Project 2014-01 - Standards Applicability for Dispersed Generation Resources – PRC-001-1.1(X), PRC-019-2, PRC-024-1(X)	Comment Form	11/05/14	12/19/14

OTHER ACTIVE COMMENT PERIODS

There are no other active comment periods.

GENERAL STANDARDS NEWS

QUICK LINKS
Ballot Results
Projected Standards Posting Schedule
Project Tracking Spreadsheet
Standards Related Questions – Single Portal
2014–2016 Reliability Standards Development Plan

NEW Resources Posted

NERC has posted slides and the streaming webinar from the Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings question and answer session on November 13, 2014.

Spring 2015 Standards and Compliance Workshop

NERC will be introducing a new, semi-combined layout for its ERO Auditor and Standards and Compliance Workshops in 2015. The ERO Auditor Workshop will be held from March 30–April 1, 2015, followed by the Standards and Compliance Workshop from April 1–3, 2015. A joint session with auditors and industry will be held on April 1, allowing the industry better transparency into the auditing process and the application of specific standards. NERC will be eager for industry feedback on the joint session and hopes it enhances the workshop value for both auditors and industry.

As preliminary planning for the Spring 2015 Standards and Compliance Workshop begins, NERC welcomes agenda suggestions. Please email any ideas to NERCStandardsComplianceWorkshop@nerc.net by December 19, 2014.

Please Continue to Register for the New Balloting and Commenting Software System

Since launching the new Standards Balloting System (SBS) on April 1, 2014, NERC has been accepting new registrations for both commenting and participating in ballots in the SBS. Before any projects are posted in the SBS, NERC staff will provide notice with an announcement and an update in the Weekly Standards & Compliance Bulletin. In the meantime, stakeholders should continue to register in the SBS and can expedite the vetting process by sending justifications for segment qualifications to SBSRegistration@nerc.net,using the segment criteria from Appendix 3D. Helpful tools for guidance on registration and participation in the SBS are available on the Balloting and Commenting page.

GENERAL COMPLIANCE AND ENFORCEMENT NEWS

There is no additional compliance and enforcement news from last week.

QUICK LINKS

Reliability Assurance Initiative
CIP V5 Transition Program
Reliability Standard Audit Worksheets
Risk-Based Registration Initiative

OTHER NEWS

NEW Canadian Provincial Summaries Available on NERC's Website

Canada's Federal, Provincial, and Territorial Monitoring and Enforcement Sub-group (MESG) has developed provincial summaries of each province's electric reliability standard-making and enforcement functions, with U.S. comparators. The MESG will review the summaries annually and update them as needed. The summaries are available on NERC's Key Players web page.

NEW NERC Releases 2014–2015 Winter Reliability Assessment

The *2014–2015 Winter Reliability Assessment* released on November 21, 2014 provides an independent North American perspective of bulk power system reliability from December 2014 through February 2015. NERC examined key indicators related to electricity demand and generation projections and found that while bulk power system operators have adequate resources and reserve margins to maintain reliability if the 2014–2015 winter is normal, periods of extreme cold could pose a significant challenge to ensuring that fossil-fired power plants have enough fuel to meet anticipated demand. Click here for the full announcement.

STANDARDS SUBJECT TO FUTURE ENFORCEMENT

The following standards are subject to future enforcement. Please refer to the U.S. Enforcement Dates page for more detail:

U.S. Enforcement Date	Standard(s)
January 1, 2015	TPL-001-4 - Transmission System Planning Performance Requirements
April 1, 2015	BAL-003-1 - Frequency Response and Frequency Bias Setting; EOP-010-1 - Geomagnetic Disturbance Operations; PRC-005-2 - Protection System Maintenance
July 1, 2015	MOD-032-1 - Data for Power System Modeling and Analysis; PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding
January 1, 2016	FAC-001-2 - Facility Interconnection Requirements; FAC-002-2 - Facility Interconnection Studies; NUC-001-3 - Nuclear Plant Interface Coordination
April 1, 2016	CIP-002-5.1 - Cyber Security — BES Cyber System Categorization; CIP-003-5 - Cyber Security — Security Management Controls; CIP-004-5.1 - Cyber Security — Personnel & Training; CIP-005-5 - Cyber Security — Electronic Security Perimeter(s); CIP-006-5 - Cyber Security — Physical Security of BES Cyber Systems; CIP-007-5 - Cyber Security — System Security Management; CIP-008-5 - Cyber Security — Incident Reporting and Response Planning; CIP-009-5 - Cyber Security — Recovery Plans for BES Cyber Systems; CIP-10-1 - Cyber Security — Configuration Change Management and Vulnerability Assessments; CIP-011-1 - Cyber Security — Information Protection
July 1, 2016	MOD-025-2 - Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability; PER-005-2 - Operations Personnel Training; PRC-019-1 - Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection; PRC-024-1 - Generator Frequency and Voltage Protective Relay Settings
July 1, 2017	MOD-033-1 - Steady-State and Dynamic System Model Validation

BOARD OF TRUSTEES AND FERC ACTION

NEW FERC Orders Issued

On November 20, 2014, FERC issued three NERC-related orders at its open meeting. First, FERC issued an order approving CIP-014-1–Physical Security. In addition to approving the standard, FERC directed NERC to address the ambiguity of the term "widespread" within six months and to submit an informational filing regarding whether the standard should be applicable to additional control centers within two years. NERC will issue notice in the bulletin when the enforcement date of CIP-014-1 has been calculated.

FERC also issued a Notice of Proposed Rulemaking proposing to approve BAL-001-2–Real Power Balancing Performance, as well as four definitions, associated violation risk factors and violation severity levels, and an implementation plan.

Finally, FERC accepted the second performance assessment of NERC as the Electric Reliability Organization, finding that NERC and the Regional Entities continue to satisfy the statutory and regulatory criteria for certification. In addition, FERC directed NERC to submit an informational filing addressing specific concerns and take actions to further improve its effectiveness as the ERO.

2014 FERC orders are posted here.

UPCOMING EVENTS

For information about other NERC events, such as meetings and conference calls for standard drafting teams, other standing committees, subcommittees, task forces, and working groups, please refer to the NERC calendar.

Workshops and Conferences

- Cause Analysis Training – December 11, 2014, Atlanta, GA (Register)
  - The workshop will include an introduction to cause analysis and the five phases of cause analysis (including some discussion on cause coding and trend analysis). Register early, as the course is limited to 30 attendees.

Webinars

- There are no upcoming webinars.

Standing Committee Meetings and Conference Calls

- Compliance & Certification Committee Meeting – December 3–4 , 2014, Phoenix, AZ (Registration and Details)
- Standards Committee Conference Call – 1:00–5:00 p.m. Eastern, December 9, 2014 (Register) (Details)

ABOUT THE WEEKLY STANDARDS & COMPLIANCE BULLETIN

This weekly bulletin compiles a list of standards and compliance projects with actionable deadlines, as well as upcoming events, recently posted resources, other NERC documents posted for comment, and other relevant news and information. Please email Mallory Huggins with feedback on this bulletin. The current bulletin and old bulletins are available under "Program News" on both the Standards home page and the Compliance & Enforcement home page.

If you would like to receive this bulletin or be added to the distribution list for a particular standards project, please email Arielle Cunningham. For questions or more information about any of the compliance news listed in the bulletin, please contact Brooke Thornton.

NPCC, Inc.

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

September 20, 2014

Members, Reliability Coordinating Committee
and
Members, Task Force on Coordination of Operation
Members, Task Force on Coordination of Planning
Members, Task Force on Infrastructure Security and Technology
Members, Task Force on System Protection
Members, Task Force on System Studies

Re: Minutes of the June 4, 2014 RCC Meeting

Sir / Madam:

Attached are the minutes of the June 4, 2014 meeting of the NPCC Reliability Coordinating Committee, as approved at the September 10, 2014 meeting.

Sincerely,

Phil Fedora

Philip A. Fedora
Assistant Vice President-Reliability Services

cc: NPCC Staff

NORTHEAST POWER COORDINATING COUNCIL
Reliability Coordinating Committee Minutes
June 4, 2014

Mr. Briggs called the meeting of the Reliability Coordinating Committee (RCC), held at the New York Times Square Residence Inn by the Marriott to order at 10:00 am.

Attendance

Officers of the Reliability Coordinating Committee

Alden Briggs, Chair	New Brunswick Power Corporation
Michael Schiavone, Co-Vice Chair	National Grid USA
Brian Evans-Mongeon, Co-Vice Chair	Utility Services, Inc.

Sector 1 - Transmission Owners

Central Hudson Gas & Electric Corp.	James McCloskey (via phone)
Central Maine Power Company	David Conroy (Alternate)
Consolidated Edison Company of New York, Inc.	Mike Forte
Hydro-One, Inc.	(proxy to Tom Irvine)
Long Island Power Authority	(proxy to Anie Philip – via phone)
National Grid USA	Michael Schiavone
New Brunswick Power Corporation	(proxy to Alden Briggs)
New York Power Authority	(proxy to Randy Crissman)
Northeast Utilities	Brad Bentley
Nova Scotia Power Incorporated	(via written proxy)
Rochester Gas & Electric Corporation	John Allen (Alternate - via phone)
The United Illuminating Company	Jonathan Appelbaum
Vermont Transco	Hantz Presume

Sector 2 – Reliability Coordinators

Hydro-Québec TransÉnergie	Pierre Paquet
Independent Electricity System Operator	(proxy to Mark Wilson)
ISO-New England, Inc.	Don Gates (Alternate – via phone)
New Brunswick Power Corporation	Alden Briggs
New York Independent System Operator	Dana Walters (Alternate)

Sector 3 – Transmission Dependent Utilities, Distribution Companies and Load Serving Entities

Hydro-Québec Distribution	(via written proxy)
New York Power Authority	(proxy to Randy Crissman)
Long Island Power Authority	Anie Philip (Alternate – via phone)
Northeast Utilities	Dwayne Basler

Sector 4 Generation Owners

Dominion Energy Marking, Inc.	Mike Garton (via phone)

Dynegy, Inc.	Jim Watson (via phone)
Entergy Nuclear Northeast	(proxy to Raey Yohannes - via phone)
Long Island Power Authority	(proxy to Anie Philip – via phone)
New York Power Authority	Randy Crissman
NextEra Energy Resources	(via written proxy)
Northeast Utilities	(proxy to Dwayne Basler)
Ontario Power Generation, Inc.	(via written proxy)

Sector 5 – Marketers, Brokers, and Aggregators

Constellation Energy Commodities Group	Glen McCartney (via phone)
HQ Energy Marketing Inc.	(via written proxy)
HQ Energy Services (US) Inc.	(via written proxy)
Long Island Power Authority	(proxy to Anie Philip – via phone)
New York Power Authority	(proxy to Randy Crissman)
PPL EnergyPlus, LLC	Elizabeth Davis (Alternate - via phone)
Utility Services	Brian Evans-Mongeon

Sector 6 – State and Provincial Regulatory and/or Governmental Authorities

New York Power Authority	(proxy to Randy Crissman)
New York State Department of Public Service	Ed Schrom (Alternate)

Sector 7 – Sub-Regional Reliability Councils, Customers, other Regional Entities and Interested Entities

New York State Reliability Council, LLC	Roger Clayton

NPCC Staff

Sal Buffamante	Assistant Vice President Compliance Audits and Investigations
Gerry Dunbar	Manager of Reliability Criteria Requirements
Phil Fedora	Assistant Vice President, Reliability Services
Jessica Hala	Manager of Finance and Accounting
Kristin Halper	Regulatory Attorney
Brian Hogue	Information Systems & Security Management
Damase Herbert	Compliance Attorney
Quoc Le	Manager, System Planning and Protection
Rafael Sahiholamal	Compliance Engineer
John Mosier, Jr.	Assistant Vice President of System Operations

Scott Nied	Manager, Compliance Program Development
Andrey Oks	Manager, Reliability Performance Criteria
Paul Roman	Manager, Operations Planning
Ralph Rufrano	Manager, Event Analysis
Edward Schwerdt	President & Chief Executive Officer

Guests

Noel Augustine	ISO-New England
Paul DiFilippo	Chair, Task Force on System Protection
Marc Dusseault	Chair, Task Force on Coordination of Planning
Gregory Goodrich	Chair, Task Force on Infrastructure Security & Technology
Dean Latulipe (via phone)	Chair, SS-38 Working Group
Richard Mailhot (via phone)	TransÉnergie Hydro-Quebec
Alan McBride	ISO-New England
John Norden	Chair, Task Force on Coordination of Operation
Isen Widjaja (via phone)	Chair, Load Modeling Working Group
Raey Yohannes (via phone)	Entergy Services, Inc.

Quorum Statement

Mr. Fedora indicated that a quorum had been achieved, by member attendance, proxy or alternate designation. He also noted having received the following written proxies:

Sector 1 – Transmission Owners
Paul Casey – Nova Scotia Power, Inc.

Sector 3 – Transmission Dependent Utilities, Distribution Companies and Load-Serving Entities
Stephane Dufresne – Hydro-Quebec Distribution

Sector 4 – Generator Owners
David Ramkalawan – Ontario Power Generation
Allen D. Schriver - NextEra Energy Resources

Sector 5 – Marketers, Brokers, and Aggregators
Yannick Vennes – HQ Energy Marketing Inc.
Louis Guilbault - HQ Energy Services (US) Inc.

Antitrust Guidelines for NPCC Meetings

Mr. Fedora reviewed the NPCC Antitrust Guidelines in the Agenda package, and suggested contacting NPCC Inc.'s Secretary, Andrianne S. Payson, at (212) 424-8218 for further information.

The RCC observed a moment of silence in remembrance of the recent passing of Donal Kidney.

President & CEO Report

Mr. Schwerdt reported on the following items:

Bulk Electric System (BES) Implementation

NERC sent out letters to all registered entity primary compliance contacts on May 1, 2014 announcing that the BES Notification and Exception Tool (BESNet) application would be available for initial registration by registered entity administrators (only) starting on May 12, 2014. Those administrators that have accessed the application thus far are being vetted by the Regional Entities to verify authenticity prior to the submission of any data into the application. To date there have been approximately 400 applications in total across NERC, with 62 vetted in NPCC, with some 16 of those being Transmission Owners.

Registered entity training sessions on the BES Definition and the BESNet application were conducted during the NPCC 2014 Spring Standards and Compliance Workshop.

A BESNet User Account Management training video, a BES Frequently Asked Questions document, and an exceptions process flow diagram, as well as other resources, are available on the NERC website. Additionally, NPCC will be announcing an informational seminar for its registered entities to provide additional training and clarification regarding the BES versus NPCC's A-10 list of Bulk Power System elements.

NERC 2014 State of Reliability Report

NERC released its State of Reliability 2014 report on May 21, 2014. Five of the key findings and recommendations in the report include:

- ✓ Bulk power system reliability performance remained high. In 2013, there were no high-stress days, including weather events.
- ✓ Frequency response remains stable. All interconnections have shown steady frequency response performance, trending above the recommended obligation at all times during the study period.
- ✓ Protection system misoperations continue to cause transmission events. Protection system misoperations (approximately 10% on a North American basis, with approximately 8% misoperations in NPCC) continue to be a significant contributor to transmission outage severity and more impactful than other events

in 2013. The report recommends that NERC complete development of standard PRC-004-3 – Protection System Misoperation Identification and Correction, and develop actions to address the three most common causes of protection system misoperations: incorrect settings; communications failures and failures of the relays themselves.

- ✓ Substation equipment failures impact transmission event severity. In response to last year's State of Reliability recommendations, an AC Substation Equipment Task Force was formed; Mr. Lombardi of NPCC staff ~~is the~~ Chairs that group. The Task Force is gathering equipment failure data to analyze with a report expected by year-end 2014.
- ✓ Use of Energy Emergency Alert Level 3 continued to decline in 2013**.**

Mr. Schwerdt then described the following Panel Sessions scheduled for the June 10, 2014 FERC Reliability Technical Conference:

- ✓ NERC State of Reliability Report;
- ✓ Emerging issues;
  ERO initiatives; and,
- ✓ ERO Performance.

At this point, Mr. Schwerdt introduced Ms. Hala, NPCC's Manager of Finance and Accounting to give a brief overview of the draft NPCC 2015 Business Plan and Budget.

NPCC 2015 Business Plan and Budget

Ms. Hala provided the following NPCC 2015 Budget Overview:

- ✓ For 2015, total expenses are increasing 3.5% over the 2014 Budget;
- ✓ Major drivers include: Reliability Assurance Initiative (RAI), Risk Assessment, Internal Control Evaluation, CIP V5 implementation, and revised BES definition implementation;
- ✓ No additional FTE's are budgeted for 2015; there are currently two open positions: one in the RAPA program area and one in compliance; and,
- ✓ Salaries expense includes a wage package increase of 3%, assuming a vacancy rate of 2%, based on recent trends.

She then provided the following summary of the change from 2014 budget by program area, noting that the funding requirements are very similar to that of 2014.

- ✓ Total Expenses up by 3.5%;
- ✓ Personnel Expenses reflect a wage package increase of 3% and vacancy rate of 2%;
- ✓ Meetings and travel are being held flat;

- ✓ Conference calls are down by $32k (or 42%) based on better negotiated rates with a new vendor;
- ✓ Consultants and Contracts are up by $393k (or 19.8%), driven by projected, temporary increased resource requirements in the compliance and RAPA programs;
- ✓ Office Costs are up $42k (or 8%) primarily due to higher than previous year computer and network maintenance costs; and,
- ✓ Fixed asset additions include the continued development of CDAA and CITS software enhancements as well as a backup system upgrade ($70k) and document management software ($30k).

She reported that the assessment and reprioritization of staffing resources is ongoing and will continue through 2015. In the compliance program area, the full effect of RAI, Risk Assessment, Internal Control Evaluation and CIP v5 implementation is currently unknown; and in RAPA, the full impact of the revised BES definition implementation is also still unknown, but staffing and resources are expected to be adequate as budgeted; including an increase in consulting and contractor expenses in both program areas.

A new Working Capital and Operating Reserves Policy was approved by NPCC's Board in October of 2013. The new policy calls for Change in Operating Reserves requirement from fixed 8.33% (30 days) to a range between 8.33% and 25.00% (90 days) to provide more stability in annual funding assessment. The Working Capital requirement remains unchanged with a targeted level of 8.33% (30 days) of the annual budget.

She concluded her presentation noting that NPCC is currently actively recruiting for its open positions.

Chair Report

Meeting Agenda

Mr. Briggs said he had received no changes to the meeting Agenda as provided in the Agenda package.

The RCC then approved the Agenda.

Common Task Force Statement of Purpose

Mr. Briggs indicated that the Task Force Chairs have agreed to common wording for their respective Task Force's Statement of Purpose; their revised respective Task Force Scopes are presented in the Agenda package under the Consent Agenda.

Consent Agenda

The Reliability Coordinating Committee approved the following Consent Agenda items (all written proxies in favor, with three abstentions: Sector 4, Generator Owners – David Ramkalawan, Ontario Power Generation, Inc., Sector 5, Marketers, Brokers, and

Aggregators - Louis Guilbault, HQ Energy Services (US) Inc., and Yannick Vennes, HQ Energy Marketing Inc.):

February 26, 2014 Meeting Minutes

The Draft-For-Approval Minutes of the February 26, 2014 Reliability Coordinating Committee were approved, with corrections noted.

RCC Membership Changes

The following changes to RCC Membership were approved:

Sector 1 -Transmission Owners

- ✓ Mr. Tom Irvine of Hydro One Networks Inc. succeeds Mr. Paul Tremblay, as the member. Mr. Ajay Garg will remain as the Alternate.
- ✓ Mr. David Conroy of Central Maine Power Company succeeds Mr. Brian Conroy, as the Member.
- ✓ Mr. Brian Conroy of Central Maine Power Company succeeds Mr. David Conroy, as the Alternate.
- ✓ Mr. Hantz Presume of Vermont Transco succeeds Mr. Paul Renaud, as the Member.
- ✓ Mr. Frank Ettori of Vermont Transco succeeds Mr. Hantz Presume, as the Alternate.
- ✓ Mr. Tony O'Hara succeeds Mr. Randy MacDonald as the Member. Mr. Randy MacDonald succeeds Mr. Tony O'Hara as the Alternate, both of New Brunswick Power Corporation.

Sector 2 - Reliability Coordinators

- ✓ Mr. Mark Wilson of Independent Electricity System Operator succeeds Ms. Barbara Constantinescu, as the member. Mr. Michael Falvo will remain as the Alternate.

Sector 3 -TDUs, Distribution. and LSE

- ✓ Mr. Gian DeLuca succeeds Mr. Mike Lupo as the member, both of New York Power Authority.

Sector 4 - Generation Owners

- ✓ Mr. Raey Yohannes of Entergy Nuclear Northeast succeeds Mr. Thomas Czerniewski, as the Member.

Task Force Roster Changes

The following changes to Task Force and Working Group memberships were approved:

Task Force on System Protection

Mr. Éric Loiselle succeeds Mr. Daniel Renaud as an Alternate from TransÉnergie.

Task Force on System Studies

- ✓ Mr. Francesco Elmi of Consolidated Edison of NY to replace Mr. Mohsen Zamzam (retired), as the Member.
- ✓ Mr. Vitaly Spitsa to replace Mr. Elmi as Alternate, both of Consolidated Edison of New York.

Task Force on Infrastructure Security & Technology

- ✓ Mr. William Temple to replace Mr. Michael Puscas as the Member, both of Northeast Utilities.
- ✓ Mr. William Temple to replace Mr. Neal Hickey as Vice-Chair.

SS-38 Load Modeling Working Group

- ✓ Mr. Jose Conto will represent ERCOT as a Member.

CP-8 Working Group on Review of Resource and Transmission Adequacy

- ✓ Mr. Vipul Agrawal will represent Independent Electricity System Operator as Alternate.

2013 New York Interim Area Transmission Review
Approved as provided in the Agenda package.

Task force Scopes
Approved as referenced in the Agenda package.

Protection System Risk Mitigation Plan Extensions
Approved as provided in the Agenda package.

Reliability Coordinating Committee Actions

2013 New England Comprehensive Area Transmission Review
Mr. McBride presented the 2013 New England Comprehensive Area Transmission Review provided in the Agenda package. He stated that the 2013 New England Comprehensive Area Transmission Review (study year 2018) demonstrates that the New England Transmission system is in conformance with the planning criteria and requirements specified in NPCC Directory No. 1 "*Design and Operation of Bulk Power System.*"

Mr. Dusseault reported that the Task Force on Coordination of Planning reviewed the report on April 15, 2014, and recommends RCC for approval. He stated that the Task Force on System Studies has also accepted the 2013 New England Comprehensive Area Transmission Review.

The RCC then approved the 2013 New England Comprehensive Area Transmission Review as provided in the Agenda package (all written proxies in favor, with three abstentions: Sector 4, Generator Owners – David Ramkalawan, Ontario Power Generation, Inc., Sector 5, Marketers, Brokers, and Aggregators - Louis Guilbault, HQ Energy Services (US) Inc., and Yannick Vennes, HQ Energy Marketing Inc.).

NPCC 2014-2015 Winter Probabilistic Multi-Area Reliability Assessment
Mr. Fedora presented the NPCC 2014-2015 Winter Probabilistic Multi-Area Reliability Assessment provided in the Agenda package. He explained that the assessment estimated the use of NPCC Area Operating Procedures designed to mitigate resource shortages for the winter of 2014/15 (November 2014 through March 2015). The use of operating procedures designed to mitigate resource shortages is not expected for Québec, the Maritimes, Ontario, New York, and New England under the assumed Base Case conditions for the expected load level. The expected load level results were based on the probability-weighted average of the seven load levels simulated.

Only the Maritimes Area show a need for use of operating procedures in response to a capacity deficiency this winter under the Base Case, extreme load conditions and under

the Severe Case conditions. The extreme load level represents the second to highest load level, having approximately a 6% chance of being exceeded.

He further explained that these results assumed the corresponding Base Case and Severe Case conditions occurred in every hour of the assessment period.

Regarding the gas-fired generation outage assumptions, Mr. Walters suggested this fact should be emphasized in the report, in order to demonstrate that the assessment considered the duration aspect of a fuel supply disruption that may occur over a period of days. Mr. Fedora agreed to include such a statement in the report.

Mr. Dusseault stated that the Task Force on Coordination of Planning reviewed this report at its May 14, 2014, meeting and recommends RCC approval. The assessment will be released in conjunction the CO-12 Working Group's corresponding winter reliability assessment, to be presented to the RCC for approval at its December 2, 2014 meeting.

The RCC then approved the NPCC 2014-2015 Winter Probabilistic Multi-Area Reliability Assessment as provided in the Agenda package, subject to the discussed clarification that the gas-fired outages were assumed for the entire assessment period (all written proxies in favor, with three abstentions: Sector 4, Generator Owners – David Ramkalawan, Ontario Power Generation, Inc., Sector 5, Marketers, Brokers, and Aggregators – Louis Guilbault, HQ Energy Services (US) Inc., and Yannick Vennes, HQ Energy Marketing Inc.).

July 3, 2013 Quebec Event Analysis

Mr. Paquet provided the RCC with an overview of the events of July 3, 2013; he explained that a fault of an exceptional duration on one of Hydro-Québec's 735 kV lines initiated by a severe forest fire led to internal load and generation losses and resulted in the sequential tripping of several DC interconnections.

He reported that Hydro-Quebec provided its findings and related recommendations were provided to NPCC as part of its Event Analysis Program, as well as TransÉnergie's compliance self-assessment to NERC standards.

A working group was put in place in December 2013 involving NPCC staff to further review the operations and design of the network, and to monitor TransÉnergie's implementation of its Action Plan addressing its findings and related recommendations.

The working group focused on the following five areas:

- ✓ Operational and maintenance procedures;
- ✓ Operational communications and control maintenance related to outage requests;

- ✓ Enhance the understanding of the impact of maintenance activities on system
- ✓ reliability;
- ✓ Supervision, tools, and communications with neighboring systems; and,
- ✓ Other actions, which include the root cause analysis of the SVC and DC ties tripping.

NPCC's Task Force on the Coordination of Operation, Task Force on System Studies, Task Force on Coordination of Planning, and Task Force on System Protection have completed their respective reviews of the event analysis. They are provided in the Agenda package.

The RCC accepted the analysis presented by TransÉnergie regarding the July 3, 2013 event, including the corresponding NPCC Task reviews of the analysis.

Status Reports

Mr. Briggs referred the RCC to the materials provided in the Agenda package; the RCC discussed the following Agenda items:

NPCC Regional Standards Committee (RSC) Report

Mr. Dunbar stated that the RSC continues to be engaged with comment review and ballot recommendations for various NERC standards, as described in the Agenda package. In addition, he highlighted the following activities:

- ✓ The continent wide disturbance monitoring standard development;
- ✓ Cost Evaluation Assessment Procedure; and,
- ✓ Development of a single portal tool – available on the Standards section of the NERC website.

In response to question, he described NERC goal to reach a "steady state" (by 2015) of the consideration of FERC directives and recommendations addressed in their standards development.

NPCC Reliability Directory Status Report

Mr. Dunbar referred the RCC to the materials provided in the Agenda package. He highlighted the status of Directory No. 1 and Directory No. 3. The Task Force on System Protection (TFSP) is currently conducting a technical comparison of the criteria within Directory No. 3 with the recent FERC approved PRC-005-2 Protection System Maintenance standard in order to assess whether all or portions of the criteria in Directory No. 3 can be retired. The TFSP is looking for NPCC comment of this comparison, currently posted through the NPCC Open Process.

NPCC Compliance Committee

Mr. Buffamante provided a brief summary of the materials provided in the Agenda package, and highlighted the activities related to the RAI Pilot Program and internal control assessment.

Mr. Nied explained that NPCC is participating on the Risk Based Registration Advisory Group, which is charged with the ERO-wide development of a risk-based registration criteria. He noted a June 6, 2014 Webinar regarding risk-based registration. He also summarized the topics presented at the 2014 NPCC Spring Standards and Compliance Workshop.

TFCO/TFCP Phase 2 revision of Directory No. 1

Mr. Dunbar reported that the NPCC Open Process review for the draft Directory No. 1 concluded its NPCC Open Process review on January 25, 2014.

The combined CO7/CP11 Working Group reconvened to develop draft responses to all comments, and has revised the draft of Directory No.1 where appropriate. Since additional revisions to the draft have taken place as a result of the comment review it is likely that Directory No. 1 will be reposted to the Open Process for a second posting.

SP-7 Working Group Review of Protection System Misoperations

Mr. DiFilippo reviewed the material provide in the Agenda package. The overall increase in the number of misoperations for the four quarters ending in 2013 as compared to the number of reported misoperations for 2011 and 2012 is attributed to the expanded reporting of non-BPS facilities. He noted a significant increase in the number of reported unknown/unexplainable misoperations and discussed possible causes for the increase.

The SP-7 Working Group continues to investigate the cause of unknown/unexplainable misoperations.

Load Modeling Working Group Update

Mr. Widjaja stated that the SS-38 Load Modeling Working Group is making progress pursuing regarding the following activities:

- ✓ Expanding the effort on the load survey/end-use load model;
- ✓ Conducting initial load model simulations; and,
- ✓ Reviewing actual system events for event recreation.

He explained that the SS38 Load Modeling Working Group plans to use actual system events, where applicable, to benchmark 'bulk power system events against Eastern Interconnection frequency response and recommend any modeling improvements as a result.'

UFLS Adequacy Assessment

Mr. Latulipe summarized the SS-38 Working Group on Inter-Area Dynamic Analysis UFLS Adequacy Assessment Study update provided in the Agenda package. He stated

that preliminary results indicate that each of the five NPCC areas ~~the~~ will meet the NPCC UFLS performance requirements for the study year (2018). He noted that Hydro-Québec is expecting to increase the total amount of load shedding by about 400 MW (~6% increase) for 2018.

He reported that the next step will be to perform sensitivity analyses as described in the Agenda package.

TFIST Cyber Update

Mr. Goodrich summarized the activities related to Project 2014-02 - Critical Infrastructure Protection Revisions, as described in the Agenda package. He reviewed upcoming due dates for CIP posted proposed revisions and a scheduled NERC webinar related to the RAI (June 19, 2014). He stated that TFIST plans to meet June 25-26, 2014 to review the CIP version 5 updates and comments received.
He also mentioned the following key dates:

- ✓ July 7- 16, 2014 CIP version 5 revisions formal ballot period; and,
- ✓ July 14, 2014 – survey responses due regarding BES Cyber assets

He then explained that the Department of Energy has released the Cybersecurity Procurement Language for Energy Delivery. He urged the RCC to review the information and consider appropriate application in their procurement activities going forward. Procurement was a threat reviewed in the 2014 Energy Threat Summit. A copy of the document is provided in the Agenda package.

Additionally, he mentioned that the Electric Sector Coordinating Council has taken over the Electric Sub-Sector Security Clearance process in the US. Mr. Nathan Mitchell, Director of Electric Reliability Standards and Compliance at APPA is coordinating Electric Sub-Sector Security Clearances going forward.

Physical Security Update

Mr. Goodrich summarized the materials presented in the Agenda package related to Physical Security activities.

He stated that the April 2013 PG&E Metcalf Substation attack was a major contributor to media coverage of physical security vulnerabilities in the beginning of 2014. The NERC Alert Advisory on February 28, 2014 - Elevated Risk due to media assertion of electric sector vulnerabilities, generated concerns for the Electric Sub-Sector substation security. On March 7, 2014 FERC Docket No. RD14-6-000 - Reliability Standards for Physical Security Measures was issued.

In response, NERC created the Project 2014-04 – Physical Security Standards Drafting Team. The team developed (in less than three months) CIP-014-1, which received industry

initial ballot Quorum/Approval of 92.53% / 85.61%. The implementation plan, upon approval by FERC, will span at most 120 days.

Additionally the NERC CIPC sponsored an industry Webinar on Physical Security Assessments, Design, and Protection Strategies presented by DOE's Lawrence Livermore National Lab; presentation materials are included in the Agenda package.

Area Compliance with NPCC Document A-10 Implementation Plan

Mr. Conroy reported that the New York ISO conducted BPS testing as part of the 2010 New York Comprehensive Area Transmission Review, and that the Ontario IESO conducted BPS testing in 2013, and as part of its 2012 Comprehensive Area Transmission Review.

He said it is expected that the remaining NPCC areas will have their testing completed by the end of the year.

2014-2015 Task Force Work Plan Progress

The Chairs of the NPCC Task Forces provided a brief summary of their respective 2014-2015 Task Force Work Plan Progress reports provided in the Agenda package.

NPCC Reliability Assessment Program (NRAP) Highlights Report

Mr. Fedora indicated that the '*NPCC Reliability Assessment Program Highlights Report*' has been updated as of May 30, 2014 and is posted on the NPCC website.

NERC Agenda Items

Operating Committee (OC)

Mr. Mosier reviewed the following June 2014 NERC Operating Committee Agenda items:

- ✓ Approval of a new reliability Guideline for communications during a complete loss of communications;
- ✓ The flooding Event in Toronto;
- ✓ New York ISO presentation regarding Electric/Gas Coordination; and,
- ✓ The NERC Physical Security Standard.

Planning Committee (PC)

Mr. Fedora reviewed the following items from the Draft June 2014 NERC Planning Committee Agenda:

- ✓ Essential Reliability Services Task Force White Paper;
- ✓ Integration of Variable Generation Task Force –draft Task 1-6 – the role that probabilistic methods can play in improving analysis;
- ✓ GADS Wind White paper – PC will be requested to review and provide comments;

- ✓ 2014 Long Term Reliability Assessment – review schedule and approval dates;
- ✓ NERC 2014 Probabilistic Assessment Update;
- ✓ Benchmark GMD Event White paper – PC will be requested to review and comment; and,
- ✓ Regional Challenges – Regional Representatives to help the PC identify and prioritize key issues and work products going forward.

Critical Infrastructure Protection Committee (CIPC)

Mr. Hogue reported that there were no voting items on the June 2014 NERC Critical Infrastructure Committee Agenda; the previously identified Cyber Security issues will be discussed.

NPCC Directory Applicability – BES/BPS

Mr. Fedora summarized discussions at the 2014 NPCC Standards and Compliance Workshop and the NPCC Joint Task Force Chairs regarding BES/BPS applicability to the NPCC Directories and Criteria. A NPCC Webinar on the subject is planned for June 25, 2014.

Informational Items

Mr. Briggs referred the RCC to the materials included in the Agenda package. The following Informational Items were discussed at the meeting:

Events Analysis Program – Overview and Status

Mr. Rufrano provided a status and overview of the Events Analysis program provided in the Agenda package.

Operational Highlights

Mr. Mosier briefly described the May 25, 2014 Milestone event; a thorough assessment of the incident is planned through the Event Analysis process.

TFCO Action Plan regarding NPCC "C" Documents

Mr. Mosier reported that the Task Force on Coordination of Operations has reviewed the existing operations-related NPCC "C" Procedure documents; he informed the RCC of several actions taken to either update, remove or consolidate the documents.

Definition of the Bulk Electric System

Mr. Fedora described the recent activities related to the revised definition of the Bulk Electric System (BES) and other supporting materials regarding the NERC Bulk Electric System Definition, Notification, and Exception Process Project Web Page.

The NERC notice for industry virtual question and answer Webinar session for the Bulk Electric System definition and its application has been included in the Agenda package. Mr. Carter Edge, Director of the Office of Coordinated Activities for the Regional Entity

Management Group, and Mr. Bob Cummings, Director of Reliability Initiatives and System Analysis at NERC will be conducting the Webinar to answer questions about the BES core definition, inclusions, exclusions, Self-Determined Notifications, and the exception process.

Other Matters

The RCC meeting was then adjourned.

Next RCC Meeting Date	**Location**
September 10, 2014	New York Times Square Residence Inn by the Marriott

Distribution of Approved Minutes

NPCC Full & General Member Representatives and Alternates
Members, NPCC Board of Directors
Members, NPCC Reliability Coordinating Committee
Members, NPCC Public Information Committee
Members, NPCC Compliance Committee
Members, NPCC Regional Standards Committee
Members, NPCC Task Force on Coordination of Operation
Members, NPCC Task Force on Coordination of Planning
Members, NPCC Task Force on Infrastructure Security and Technology
Members, NPCC Task Force on System Protection
Members, NPCC Task Force on System Studies
NPCC Officers
NPCC Staff
Andrew J. Fawbush, Esq.
Andrianne S. Payson, Esq.

And:
Federal Energy Regulatory Commission – Mike Bardee, David O'Connor, Juan Villar
La Régie de L'Énergie – Daniel Soulier
Ontario Energy Board – Peter Fraser
United States Department of Energy – David Meyer
New Brunswick Department of Energy and Mines – David Sallows
Nova Scotia Utility & Review Board – S. Bruce Outhouse, Q.C.

North American Electric Reliability Corp.
Bulk Electric System Exception Process Flow Diagrams
May нф, 2013

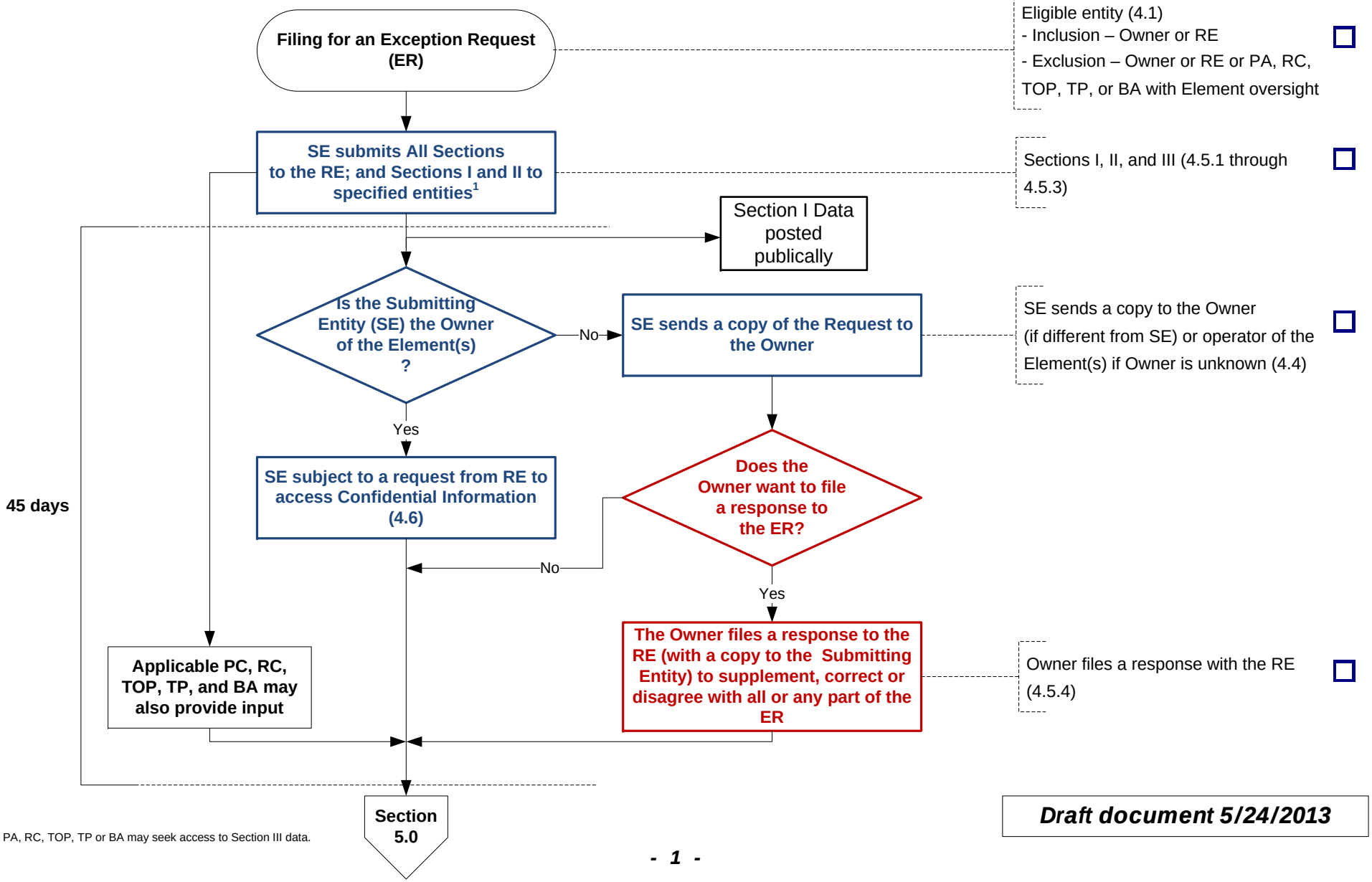
Note: Every effort has been made to ensure that the content of these flow diagrams match the Bulk Electric System Exception Process as described in the NERC Rules of Procedure. However, in the case of discrepancies between the NERC Rules of Procedure and these flow diagrams, the NERC Rules of Procedure govern.

BES Element Exception Process

Section 4.0 - Form, content and submission on an exception request

(from the Submitting Entity's perspective)

Timeline	Flowchart	Checklist



Eligible entity (4.1)
- Inclusion – Owner or RE
- Exclusion – Owner or RE or PA, RC, TOP, TP, or BA with Element oversight

☐

Sections I, II, and III (4.5.1 through 4.5.3)

☐

SE sends a copy to the Owner (if different from SE) or operator of the Element(s) if Owner is unknown (4.4)

☐

Owner files a response with the RE (4.5.4)

☐

[1] Owner, PA, RC, TOP, TP or BA may seek access to Section III data.

Draft document 5/24/2013

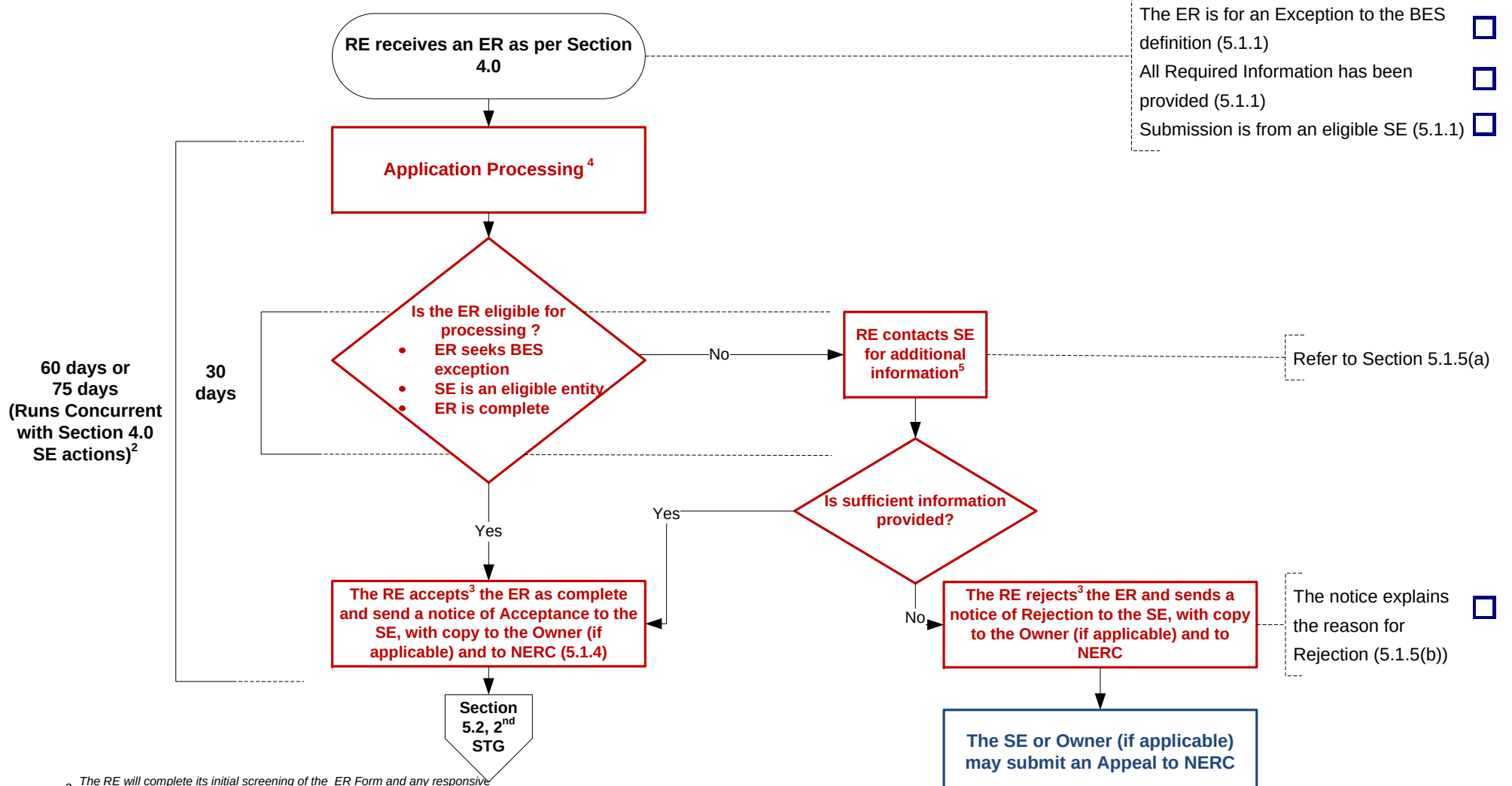
BES Element Exception Process

Section 5.0 – Review, acceptance or rejection, and reccomendation regarding ER

(from the Regional Entity's perspective)

FIRST STAGE – Initial Screening

Timeline	Flowchart	Checklist



Checklist

- Assign a unique identifier to ER (5.1.2)[6]
- The ER is for an Exception to the BES definition (5.1.1)
- All Required Information has been provided (5.1.1)
- Submission is from an eligible SE (5.1.1)
- The notice explains the reason for Rejection (5.1.5(b))

2 *The RE will complete its initial screening of the ER Form and any responsive document filed by an Owner no later than either 60 calendar days after receiving the ER or 30 calendar days after receiving any responsive document from the Owner, whichever is later. Included in this timeframe is 45 days of the Section 4 Process since the action of the SE and RE run concurrently.*

3 *The RE may either accept the ER in its entirety, reject the ER in its entirety, or if the ER is for more than one Element, may accept it with respect to a subset of the Elements and reject it with respect to the remainder based on the similarity of the evidence presented for the Exception Request.*

4 At any stage before the issuance of a final Recommendation, a Submitting Entity may provide supplemental information which may reset the evaluation timeline. (Section 6.0)

5 If additional information is provided, the initial screening time will be extended to 15 days after the receipt of the additional information.

6 When the RE is the SE, after a unique identifier is assigned the process proceeds to section 5.2 second stage.

Draft document 05/24/2013

BES Element Exception Process

Section 5.0 – Review, acceptance or rejection, and reccomendation regarding ER

(from the Regional Entity's perspective)

SECOND STAGE – Substantive Review

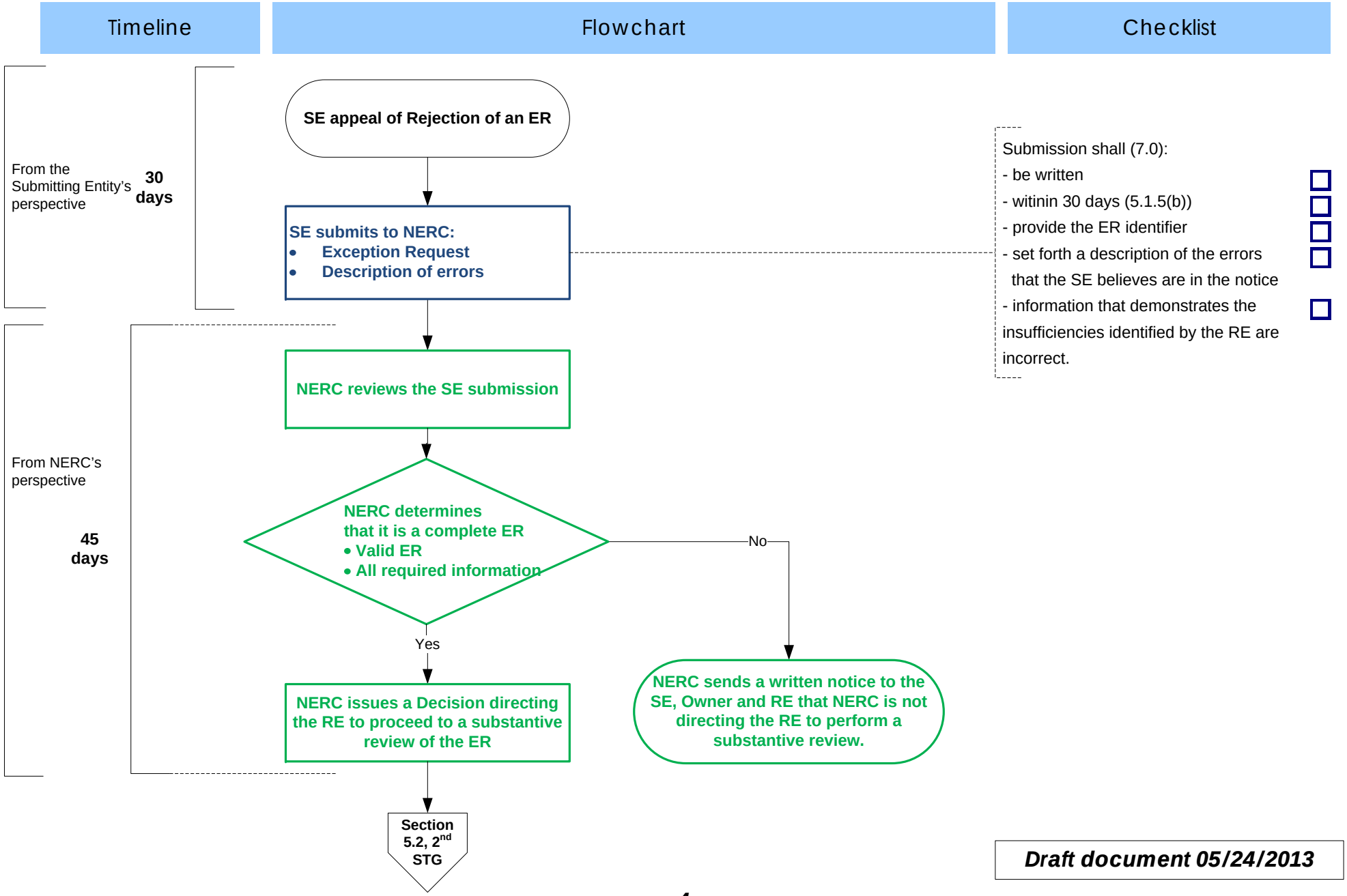
Timeline	Flowchart	Checklist
Up to 6 months	**RE sets milestones and sends copy to Submitting Entity and Owner, if different.**	Set milestones pursuant to Section 5.2.2. ☐
	Is the RE Recommendation to disapprove ER? — Yes → **Review and Opinion from Technical Review Panel[8]**	TRP Opinion pursuant to Sections 5.0(iii), 5.2.4, and 5.3 ☐
	No	The notice is in accordance with Section 5.2.3 ☐
	The RE issues a Recommendation to NERC and SE (and Owner if different from the SE)[7]	The Recommendation (5.2.3): ☐ - includes an evaluation - states the Elements covered - States the basis of the Recommendation - includes information considered by the RE in arriving at its Recommendation
	Section 8.0	

7 At any stage, pursuant to section 6.0, before the issuance of a final Recommendation a Submitting Entity may provide supplemental information which may reset the evaluation timeline.

8 A Technical Review Panel opinion is only required where a Regional Entity intends to issue a disapproval Recommendation to NERC. The Technical Review Panel consists of not less than three (3) individuals appointed by the Regional Entity senior executive (CEO, President, General Manager, etc.).

BES Element Exception Process

Section 7.0 – Appeal of Rejection of an ER Application based on its completeness

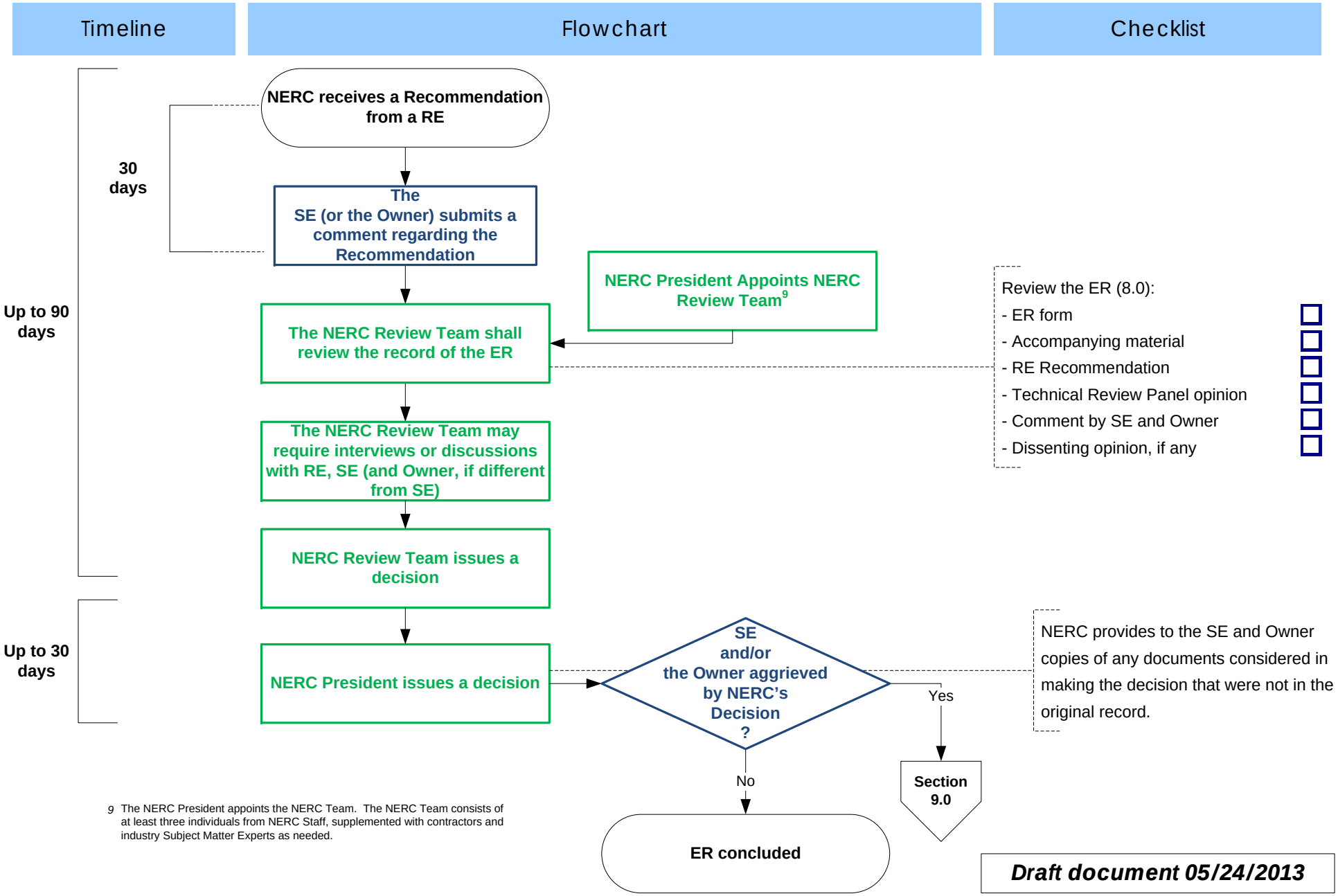


Draft document 05/24/2013

BES Element Exception Process

Section 8.0 – Approval or Disapproval of an ER

(from NERC's perspective)



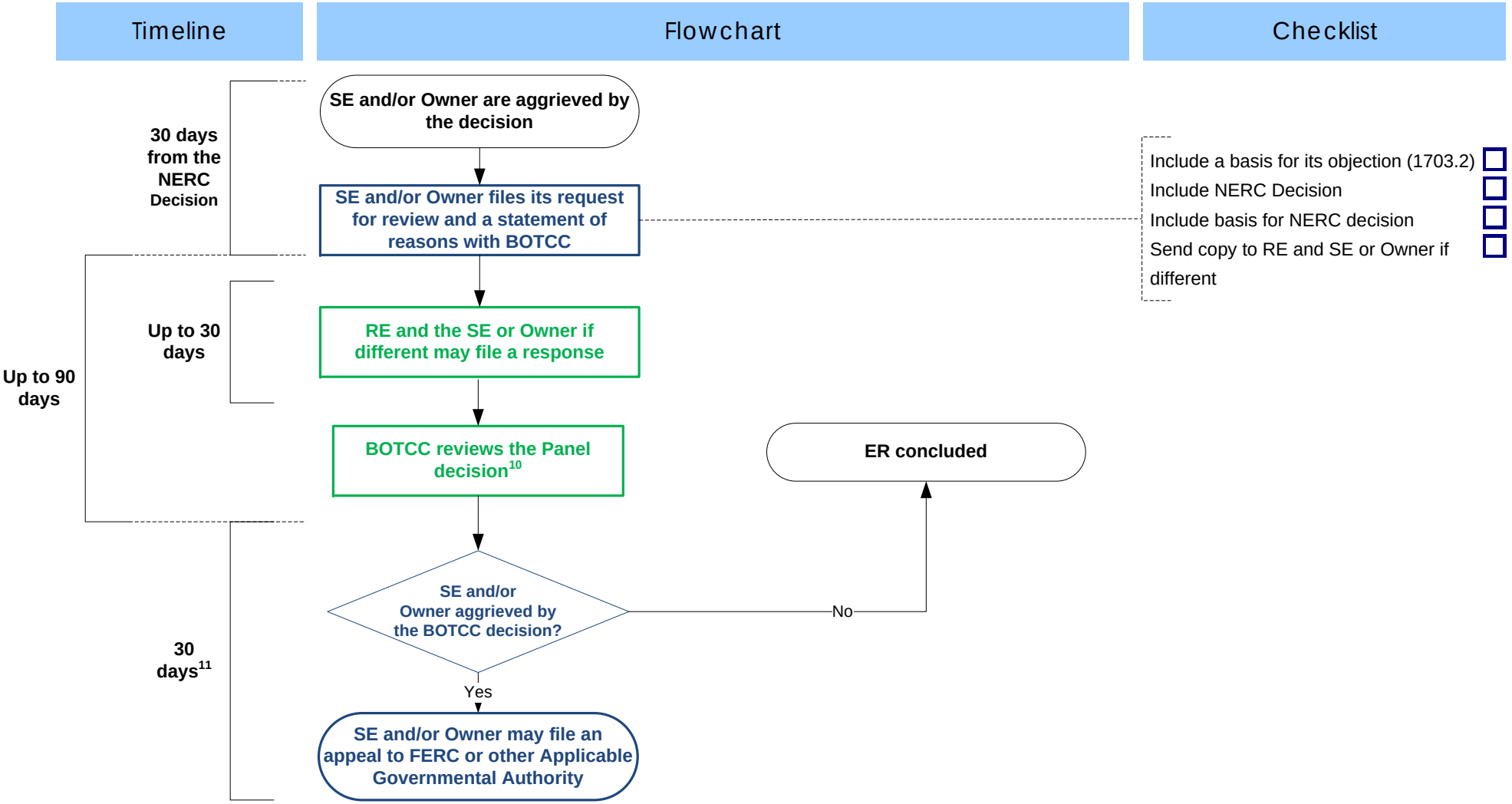
9 The NERC President appoints the NERC Team. The NERC Team consists of at least three individuals from NERC Staff, supplemented with contractors and industry Subject Matter Experts as needed.

Draft document 05/24/2013

BES Element Exception Process

Section 9 – NERC BOT Review of a Decision

(from Submitting Entity and NERC perspective)



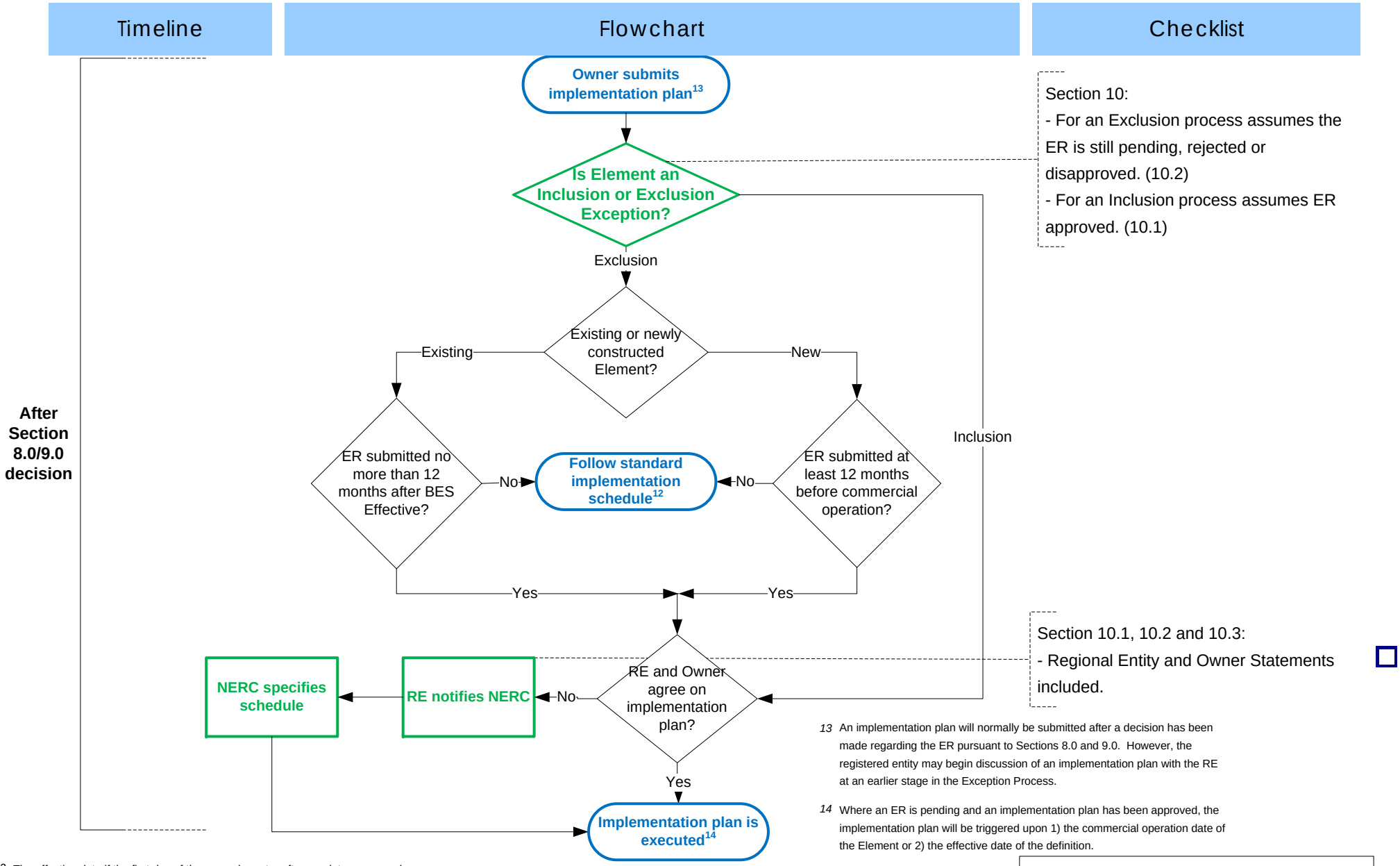
10 The Board of Trustees Compliance Committee may extend the deadline date for its decision to a date more than 90 days following submission of the challenge, by issuing a notice to the SE, the Owner (if different) and the RE stating the revised deadline date and the reason for the extension.

11 Within thirty (30) days following the date of the decision of the BOTCC, or within such other time period as is provided for in the legal authority, rules or procedures of the Applicable Governmental Authority.

BES Element Exception Process

Section 10.0 – Implementation Period for Exceptions

(from the Regional Entity's and NERC's perspective)



13 An implementation plan will normally be submitted after a decision has been made regarding the ER pursuant to Sections 8.0 and 9.0. However, the registered entity may begin discussion of an implementation plan with the RE at an earlier stage in the Exception Process.

14 Where an ER is pending and an implementation plan has been approved, the implementation plan will be triggered upon 1) the commercial operation date of the Element or 2) the effective date of the definition.

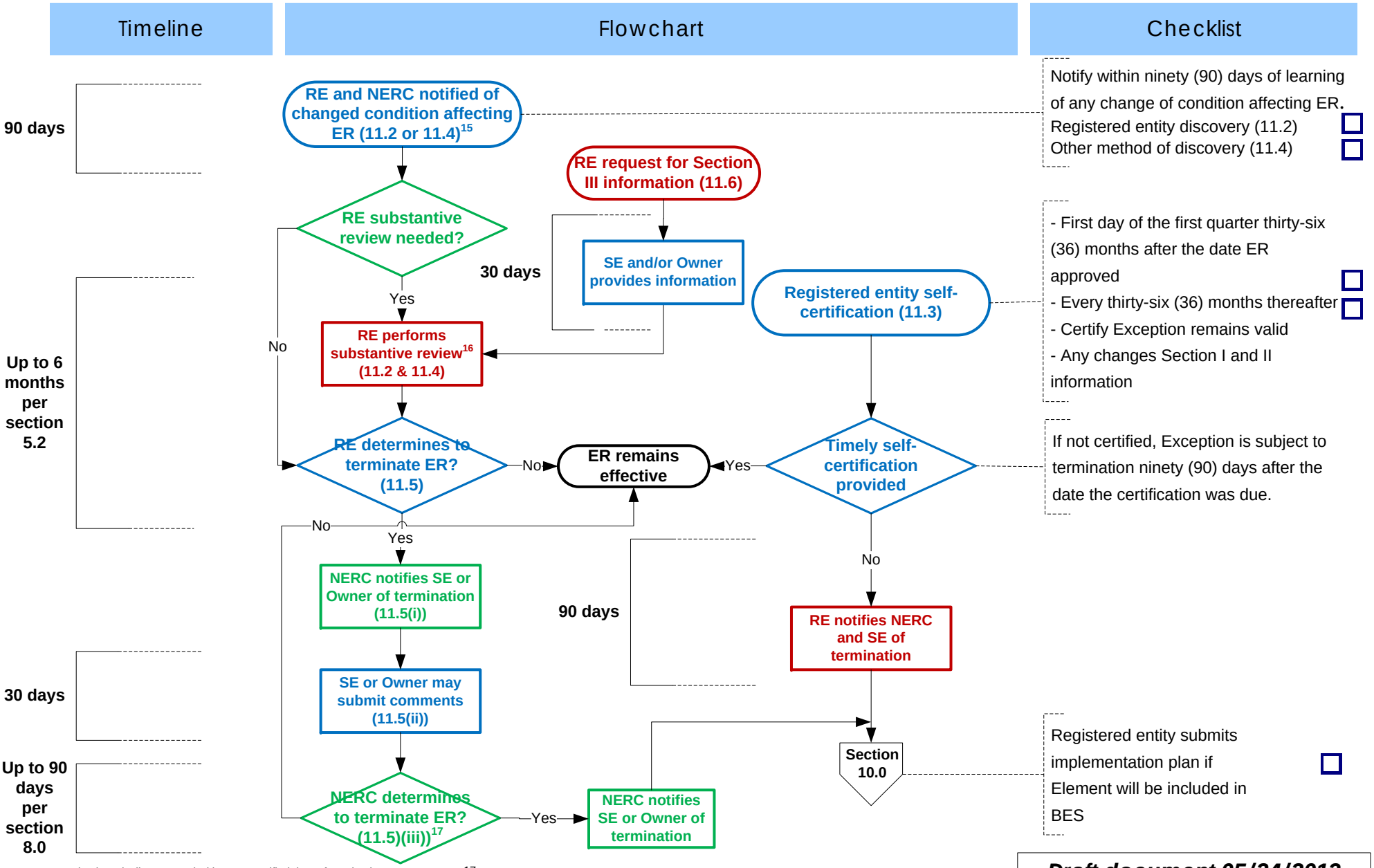
12 The effective date if the first day of the second quarter after regulatory approval (July 1, 2013 for U.S. jurisdictional entities) or if no regulatory approval is required then the first day of the second quarter after NERC Board adoption. The implementation period is 24 months after the applicable effective date.

Draft document 05/24/2013

BES Element Exception Process

Section 11.0 – Termination of an Approved Exception

(from the Regional Entity's and NERC's perspective)



15 An Exception is typically approved without a specified date of termination, see section 11.1.

16 Upon request by the Regional Entity, the Submitting Entity(ies) and/or Owner if different shall provide within thirty (30) days the most recent versions of any Section III Required Information so requested.

17 NERC review is in accordance with Section 8.0.

Draft document 05/24/2013

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BES Frequently Asked Questions

Version 1.5
August 22, 2014

RELIABILITY | ACCOUNTABILITY






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

Table of Contents

Preface iii

1. Version History 1

2. General Questions 2

2.1. When will the revised BES definition be effective? 2

2.2. What are the processes associated with implementing the new BES definition? 2

2.3. How will the ERO implement the BES definition? 2

2.4. What should Entities do to prepare for July 1, 2014? 2

2.5. How do currently registered owners of existing dispersed power producing resources need to report their Facilities on July 1, 2014 when Inclusion I4 takes effect? 3

2.6. Our existing dispersed generation Facility has a generator addition that will bring its aggregate nameplate rating over the 75 MVA threshold of Inclusion I4. How does this affect the Facility's status in the BES and what reporting is expected for the change? 4

2.7. If the ownership of an Element that was granted an Exception (inclusion or exclusion) changes, what is necessary to do to retain the Exception? 5

2.8. Are there any additional Reliability Standard development projects involving dispersed generation Facilities (Inclusion I4)? 5

2.9. What is the "Special Notification Submission Period?" 5

2.10. Does the "Special Notification Submission Period" apply to Notifications of Inclusion as well? 5

2.11. Does the "Special Notification Submission Period" apply to Exception Requests? 6

2.12. Can you provide any guidance about the level of detail needed in one-line diagrams submitted with Self-Determined Notifications or Exception Requests? 6

3. Training and Reference Resources 10

3.1. Will there be any training prior to July 1, 2014? 10

3.2. Will there be any training after July 1, 2014? 10

4. Notification of Self-Determination Process 11

4.1. When can I start entering in my BES Self-Determined Notifications? 11

4.2. Can a Registered Entity discuss matters with the Regional Entity prior to submitting a Self-Determined Notification and/or Exception Request? 11

4.3. What information will I need to supply with a notification of self-determinations? 11

4.4. Am I required to notify the Region of a change of BES status due to the new BES definition? 11

4.5. If nothing has changed in my Element's BES status after applying the new BES definition, do I need to submit a BES Self-Determined Notification? 12

4.6. Do newly identified Elements require the submittal of Self-Determined Inclusion Notifications? 12

4.7. Which Entity should provide Self-Determined Notifications for jointly-owned Elements? 12

4.8. Under legacy Regional BES definitions, certain transmission elements were considered as BES, but will now be excluded under the new BES definition. What should be submitted in the Self-Determination Notifications? 12

5. Exception Request Process 13

5.1. What process will NERC utilize to make evaluate BES Exception Requests? 13

5.2. What supporting information is needed to submit an exception request? 13

5.3. Who evaluates and approves Exception Requests? 13

5.4. What is a technical review panel? Who is on it? How are they chosen? 13

5.5. What is the NERC review panel? Who is on it? 14

5.6. How long will the process take? 14

5.7. How can an Entity appeal a Rejection of an Exception Request? 15

5.8. How can an Entity appeal the NERC decision? 16

5.9. Who can submit BES Exception Requests? 16

5.10. What happens if my system configuration changes after I have an approved Exception Request? 17

5.11. What if I have Elements that cross multiple Regional Entity boundaries? 17

5.12. Do I need to go to my Reliability Coordinator or Balancing Authority before submitting my BES Exception Request? 17

5.13. If an Exception Request is to be submitted for a jointly-owned Element, which Entity should submit the request? 18

5.14. What if I don't submit a BES self-determined BES notification for an exclusion or an inclusion as a result of the new BES Definition? 18

5.15. Should I concurrently file a BES Exception Request with NERC and a petition to exclude local Distribution Elements with FERC? 18

6. BES Notification and Exceptions Tool (BESNet) 20

6.1. What is the BESNet application and for what will it be used? 20

6.2. When will BESNet be available for submitting Exception Requests or Self-Determined Notifications? 20

6.3. Will there be software-related User Guides? 20

6.4. Is the information I enter into the BESNet application safe and secure? 20

6.5. Am I required to register for BESnet access? 21

6.6. Our company is divided into several organizational units that are exclusively registered as different NERC Functional Entities. How should we register for BESnet access? 21

6.7. I am preparing a series of Self-Determined Notifications (SDNs) and Exception Requests (ERs) for a number of Elements on my transmission system. How should the groupings of Elements be organized so as to provide an orderly and efficient approach that will minimize effort, aid review and expedite approval? 21

7. Compliance and Registration Questions 23

7.1. What is the implementation plan for the new BES definition, and when do the related compliance obligations begin? 23

7.2. When will compliance be mandatory with NERC Reliability Standards for existing Elements that are newly identified as BES Elements? 23

7.3. When do compliance obligations begin for newly built Elements that are classified as BES Elements under the new BES definition? 23

7.4. What are the obligations of the owner of a Facility that is designated as a part of the BES? 23

7.5 If I need to register based on the new BES definition, when should I register? 24

7.6. If an Entity does not own or operate BES assets, does that mean they have to follow NERC standards? 24

7.7. Can an Entity's registration requirements change as a result of applying the new BES definition? 24

7.8. If an Element is excluded from the BES through an exception request, what happens to compliance obligations, monitoring and enforcement? 24

7.9. If an Element is excluded from the BES through self-determination, what happens to compliance obligations, monitoring and enforcement? 24

7.10. In FERC Order No. 773-A (P 109), FERC stated, "in the absence of bad faith, if a registered entity applies the bulk electric system definition and determines that an element no longer qualifies as part of the bulk electric system, upon notifying the appropriate Regional Entity that the element is no longer part of the bulk electric system the element should not be treated as part of the bulk electric system unless NERC makes a contrary determination in the exception process." How is NERC implementing this language? 25

7.11. For excluded facilities, do I still have any compliance obligations? 26

7.12. If I am registered for the Distribution Provider function and I do not own or operate any BES Elements, can I request deactivation of my compliance registration? 26

8. NERC Process 28

8.1. Will the BES definition be applied consistently across the Regional Entities? 28

8.2. If my Element is not considered a part of the BES, might I still be required to provide information to NERC about it? 28

9. FERC 29

9.1. Does FERC have a role in designating Facilities as part of the BES? 29

9.2. Should I concurrently file a BES Exception Request with NERC and a petition to exclude local Distribution Elements with FERC? 29

10. Definition Questions 30

10.1. Protection Systems were explicitly included in the Legacy Regional Definition and the new NERC BES Definition is silent on Protection Systems. Do I need to do anything in BESnet for these Protection Systems? 30

Preface

The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk power system (BPS). NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce Reliability Standards for the BPS. NERC develops and enforces Reliability Standards; assesses adequacy annually via a 10-year forecast and summer and winter forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. ERO activities in Canada related to the reliability of the BPS are recognized and overseen by the appropriate governmental authorities in that country.[1]

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight Regional Entity areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC Regional Entities

NERC Regional Entities Map



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

[1] As of June 18, 2007, FERC granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the BPS and made compliance with those standards mandatory and enforceable. Equivalent relationships have been sought and for the most part realized in Canada and Mexico. Prior to adoption of §215 in the United States, the provinces of Ontario (in 2002) and New Brunswick (in 2004) adopted all Reliability Standards that were approved by the NERC Board as mandatory and enforceable within their respective jurisdictions through market rules. Reliability legislation is in place or NERC has memoranda of understanding with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, Manitoba, Saskatchewan, British Columbia and Alberta, and with the National Energy Board of Canada (NEB). NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. Manitoba has adopted legislation, and standards are mandatory there. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain Reliability Standards have been approved in that jurisdiction; others are pending. NERC standards are now mandatory in British Columbia and Nova Scotia. NERC and the Northeast Power Coordinating Council (NPCC) have been recognized as standards setting bodies by the Régie de l'énergie of Québec, and Québec has the framework in place for Reliability Standards to become mandatory. NEB has made Reliability Standards mandatory for international power lines. In Mexico, the Comisión Federal de Electricidad (CFE) has signed WECC's reliability management system agreement, which only applies to Baja California Norte.

1. Version History

The following is the history of changes to this document.

Version	Date	Change(s) Made	Change Tracking
1.0	May 6, 2014	Original Publishing	
1.1	June 4, 2014	Editorial changes to 7.1 Added FAQs: 2.7, 2.8, 4.7, 5.13, 5.14, 5.15, 6.4, and 7.8.	
1.2	June 26, 2014	Updates to 2.8, 3.1. Added FAQs: 2.9, 2.10, 2.11, 3.2, 4.8, 6.5, 6.6, 6.7, 7.9, 7.10, 7.11, 9.2, and 10.1.	
1.3	July 1, 2014	Updates to 2.5	
1.4	July 23, 2014	Factual corrections to 2.5	
1.5	August 25, 2014	Factual correction to 2.2 Added FAQs: 2.12, 7.12	

2. General Questions

2.1. When will the revised BES definition be effective?

The definition will be effective July 1, 2014.

2.2. What are the processes associated with implementing the new BES definition?

- Notification of Self-Determination: Facility owners notify Regional Entities of Elements excluded from the BES (by application of the BES definition) that were previously included in the BES, as well as Elements that are now included in the BES by application of the BES definition that were previously not included.
- Local distribution exclusions: In accordance with FERC Order No. 773-A, Entities may petition FERC for Facilities to be excluded as local distribution at any time.
- Rules of Procedure Exception process: Entities may request that Facilities either be included in the BES or excluded from the BES after applying the BES definition.

2.3. How will the ERO implement the BES definition?

The ERO has developed a process and single web-based tool for asset owners to provide industry with a uniform method to notify the Regional Entities of changes and to identify BES inclusions or exclusions as directed by the Federal Energy Regulatory Commission's (FERC) Order Nos. 773 and 773-A, as well as the March 20, 2014 Order[2] approving the Revised Definition.

- Provide a uniform process for Self-Determined Notifications of newly identified BES inclusions or exclusions.
- Provide a common tool for Entities to submit Exception Requests.
- Create a consistent method for the Regional Entities and NERC to efficiently process BES Exception Requests.
- Address regulatory requirements in FERC Order Nos. 773 and 773-A, as well as the March 20, 2014 Order approving the Revised Definition.

2.4. What should Entities do to prepare for July 1, 2014?

Step 1: Identify BES Facilities and Elements

NERC suggests that each Entity that owns or operates Facilities and Elements apply the revised BES definition to such Facilities and Elements to determine if they are included in the BES. This analysis should identify Facilities and Elements that:

i. should be included in the BES, or
ii. may be excluded from the BES, based on the revised BES definition.

[2] *Order Approving Revised Definition*, 146 FERC ¶ 61,199 (March 20, 2014) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/E-7.pdf

After July 1, 2014, Entities are required by the NERC Rules of Procedure[3] to notify their Regional Entity of new Self-Determined Inclusions and Exclusions from application of the bright-line BES definition.

Step 2: Perform a Gap Analysis

Each Entity owning or operating Facilities and Elements that have been newly identified for inclusion in the BES should perform a gap analysis for both:

i. Registration (and Certification, if applicable), and
ii. Compliance with applicable Reliability Standards.

Step 3: Develop BES Implementation Plans

An Entity with newly included Facilities or Elements may need to develop a registration implementation plan (which may include the need for Certification or a revision to an existing Certification), a compliance implementation plan, or both. In either case, the Entity should submit its implementation plan(s) to the applicable Regional Entity for review and concurrence.

Additional information on preparations is contained in the *BES Definition Implementation Guidance Document* and the *BES Definition Reference Document*, which are posted at:

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

2.5. How do currently registered owners of existing dispersed power producing resources need to report their Facilities on July 1, 2014 when Inclusion I4 takes effect?

Dispersed power producing resources with an aggregate nameplate rating greater than 75 MVA should already be included as BES, based on the former NERC BES Definition. In cases where dispersed power producing resources with an aggregate nameplate rating greater than 75 MVA have not been included as part of the BES, a Self-Determined Notification should be submitted. See the section below for MRO and WECC for a summary of information that should be included with the Notification.

Inclusion I4 within the new BES Definition clarifies which parts of the Facility are considered BES. Based on the approved BES Definition, the individual dispersed generators and equipment that aggregate to ratings of greater than 75 MVA are included in the BES. Inclusion I4 further clarifies that the elements between individual devices or machines and the point where the aggregate nameplate rating is greater than 75 MVA are not BES Elements.

Regional differences in past implementation of the former BES Definition with regard to dispersed power producing resources have led to inconsistencies, which the application of the new BES Definition is intended to address. The following outlines the specific

[3] See Section of 501 of the Rules of Procedure "Scope of the Organization Registration and Organization Certification Programs" located at http://www.nerc.com/pa/RAPA/Pages/BES.aspx.

steps involved in achieving consistent implementation of the new BES Definition across the ERO for dispersed power producing resources.

In FRCC, NPCC, RF, SERC, SPP, and TRE: Registered Entities that own or dispersed power producing resources already considered by their Regional Entity to be part of the BES based on the former definition do not need to submit a Self-Determined Notification (provided that the elements 100 kV and above between the point where the aggregate nameplate rating is greater than 75 MVA and the point of Interconnection to the BES, as well as the individual wind turbines, were also already considered to be part of the BES). There is no obligation to submit a Notification through the BESnet system stating that elements below 100 kV used for common point delivery below a 75 MVA aggregation point are excluded, or that individual turbines are included.

In MRO and WECC: The Regional Entities did not consider the individual devices or machines comprising a dispersed power producing Facility where the aggregate nameplate rating is greater than 75 MVA to be part of the BES. In these cases, the Registered Entity must complete a Self-Determined Notification of inclusion. Registered Entities must submit supporting information with the Self-Determination, which should include one-line diagrams of the facility showing individual machines or devices, the lines used to deliver capacity to common points of connection, and the substation and other Facilities up to the point of transmission interconnection, as well as the point(s) at which output is aggregated and exceeds 75 MVA. The Registered Entity should submit a summary list of the Elements that comprise the facility that are considered part of the BES, including the number, manufacturer (and model), and nameplate MVA rating of the individual machines or devices. Explicitly identifying each of the Elements within the BESnet application is not required. The Regional Entity will review the one-line diagrams and the summary list to validate that the BES Definition was applied correctly. In some instances, additional documents may be requested by the Regional Entity to perform this validation. Registered Entities that submit a valid notification under this approach are permitted up to a two year transition period to bring the newly identified BES Elements into compliance with applicable NERC Reliability Standards.

2.6. Our existing dispersed generation Facility has a generator addition that will bring its aggregate nameplate rating over the 75 MVA threshold of Inclusion I4. How does this affect the Facility's status in the BES and what reporting is expected for the change?

Under the scenario above, this is a change in the Facility's inclusion/exclusion status per the "bright line" in Inclusion I4. The Entity should use the BESNet application to provide a notification of inclusion of this Facility. Supporting details should be provided, including one-line diagrams. The Regional Entity will examine the one-line diagrams for identification of the number, manufacturer (and model), and nameplate MVA rating of the individual machines or devices, the number of collector lines, and the collector substation and other substation Facilities up to the point of transmission interconnection, as well as the point at which output is aggregated and exceeds 75 MVA. In some instances, additional documents may be requested by the Regional Entity.

However, it is not necessary for the owner to provide details in the BESNet application for each individual dispersed machine or device and step-up transformer, nor the individual non-BES collector lines, beyond the one-line diagram, provided the one-line diagram clearly indicates the size of the individual machine or device and their step-up transformers. BESNet should be used for reporting the Facility status change in the aggregate.

2.7. If the ownership of an Element that was granted an Exception (inclusion or exclusion) changes, what is necessary to do to retain the Exception?

The new Element owner must notify the appropriate Regional Entity of the change of ownership. The Regional Entity will then make the reassignment of ownership in the BESNet for the Exception.

The former Element owner also must notify the appropriate Regional Entity of the change in its assets.

2.8. Are there any additional Reliability Standard development projects involving dispersed generation Facilities (Inclusion I4)?

The Project 2014-01 Standard Drafting Team is focusing on identifying Reliability Standard requirements applicable to dispersed power-producing resources. The list developed from the Standards Authorization Request (SAR) may provide a subset of applicable Reliability Standards. Once the Standard Drafting Team concludes its work, NERC will determine next steps, including alignment with the Risk-Based Registration Initiative.

2.9. What is the "Special Notification Submission Period?"

Registered Entities submitting Notifications of Exclusion may perceive a potential compliance benefit in submitting those Notifications as soon as possible, resulting in the possibility of a large number of Notifications being submitted on July 1. In order to reduce the potential for congestion, NERC has established a period beginning July 1, 2014, and ending September 1, 2014, during which all complete and valid notifications of exclusion submitted will be deemed to have been submitted on July 1 for purposes of determining compliance obligations (in so doing, all entities that submit within that period will have the same potential compliance date, reducing any perceived incentive to submit on July 1). Thus entities are encourage to pace their submission of Notifications of Exclusion within this period.

2.10. Does the "Special Notification Submission Period" apply to Notifications of Inclusion as well?

No. Because Notifications of Inclusion are already subject to a transition period, there is no need for the "Special Notification Submission Period" to apply to Notifications of Inclusion.

2.11. Does the "Special Notification Submission Period" apply to Exception Requests?

No. There is no direct relationship between Notifications of exclusion and Exception Requests for exclusion. Exception Requests are processed differently than Self-Determined Notifications, and the submission date of an Exception Request does not have a direct relationship with the dates associated with Compliance and Enforcement. Instead, once an Element is excluded from the BES through an approved Exception Request, for all cases in which the excluded Element would have previously been subject to Reliability Standards and Requirements, compliance obligations for those standards will be considered to have ceased upon the affirmative determination of the exception request.

2.12. Can you provide any guidance about the level of detail needed in one-line diagrams submitted with Self-Determined Notifications or Exception Requests?

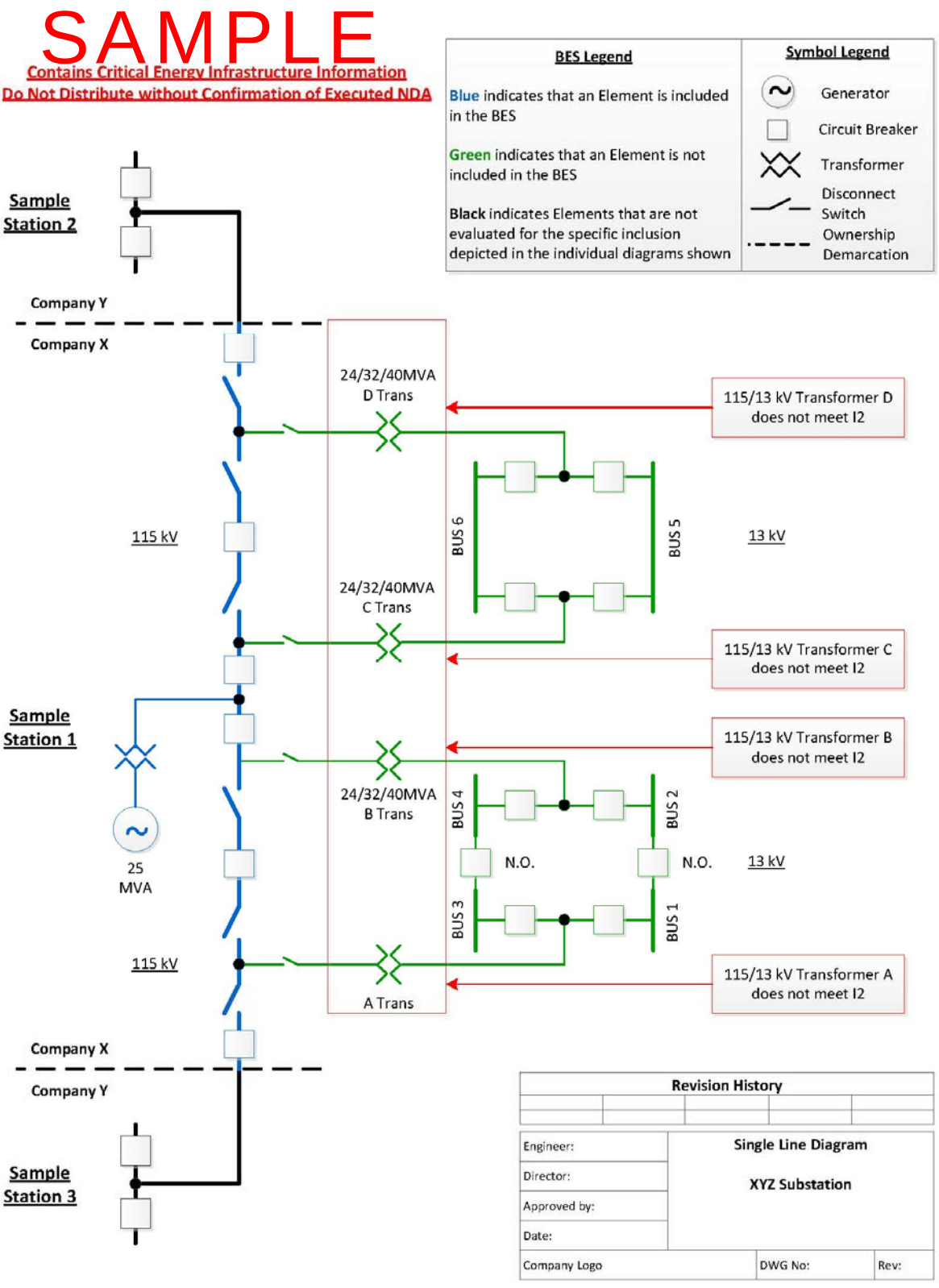
The level of detail required for one-line diagrams submitted in support of SDN or ER is illustrated in the BES Definition Reference Document Version 2, April 2014. The entity submitting an inclusion or exclusion SDN or ER should submit a one-line diagram possessing the following attributes:

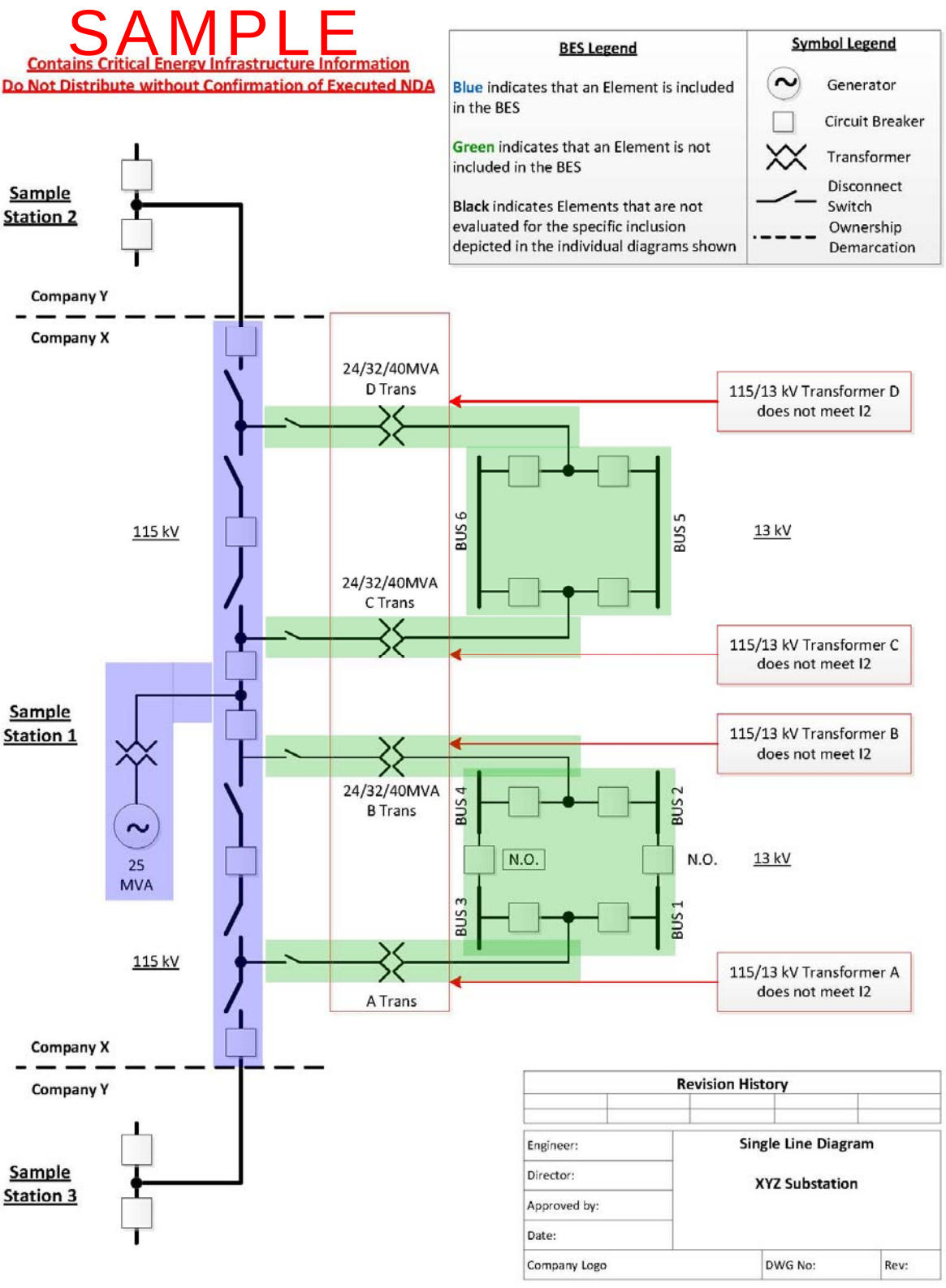
1. One-lines should be complete, officially approved diagrams with company approval blocks. Simplified one-lines may be provided as visual aids but must be accompanied by complete, official company one-lines.
2. If considered CEII, the one-lines must be clearly marked as such.
3. One-lines should clearly indicate change of ownership points and clearly identify the owners on each side of a facility. In the case of joint ownership the joint ownership parties should be indicated on the diagram.
4. The diagrams should clearly indicate the status (BES or non-BES) on the diagram of all facilities; not limited to those expressly identified in the SDN or ER. This can be done by highlighting Elements as Blue (BES) or Green (non-BES) as illustrated in the BES Definition Reference document (Version 2, April 2014).
5. The Elements specifically called out for inclusion or exclusion should be clearly marked (such as with a box, circle, etc…).
6. The applicable provision(s) of the BES core definition, inclusions and exclusions, should be indicated for each element.
7. A sufficient portion of the surrounding system should be provided to enable the Regionals Entity/NERC reviewer to apprehend the context of the Element. The following should be included as relevant to the particular Element:
    a. Portray the complete sub-transmission system less than 100 kV but greater than 50 kV and the sub-transmission system to a bus less than or equal to 50 kV.
    b. Neighboring sub-stations on either end of a transmission line Element.

c. Neighboring substations related to Elements that are part of a local network or radial transmission line.

8. All BES and non-BES generating resources on the diagram should indicate name plate rating, regardless of whether they are the subject of the SDN or ER or not.
9. All breakers/switching devices with indication of whether they are normally opened or normally closed.

Sample diagrams conforming to the above guidance are included on the following pages for reference.


SAMPLE
Contains Critical Energy Infrastructure Information
Do Not Distribute without Confirmation of Executed NDA
BES Legend
Blue indicates that an Element is included in the BES
Green indicates that an Element is not included in the BES
Black indicates Elements that are not evaluated for the specific inclusion depicted in the individual diagrams shown
Symbol Legend
Generator
Circuit Breaker
Transformer
Disconnect Switch
Ownership Demarcation
Sample Station 2
Company Y
Company X
24/32/40MVA D Trans
115/13 kV Transformer D does not meet I2
115 kV
BUS 6
BUS 5
13 kV
24/32/40MVA C Trans
115/13 kV Transformer C does not meet I2
Sample Station 1
115/13 kV Transformer B does not meet I2
24/32/40MVA B Trans
BUS 4
BUS 2
N.O.
N.O.
13 kV
25 MVA
BUS 3
BUS 1
115 kV
115/13 kV Transformer A does not meet I2
A Trans
Company X
Company Y
Sample Station 3
Revision History
Engineer:
Director:
Approved by:
Date:
Single Line Diagram
XYZ Substation
Company Logo
DWG No:
Rev:


SAMPLE
Contains Critical Energy Infrastructure Information
Do Not Distribute without Confirmation of Executed NDA
BES Legend
Blue indicates that an Element is included in the BES
Green indicates that an Element is not included in the BES
Black indicates Elements that are not evaluated for the specific inclusion depicted in the individual diagrams shown
Symbol Legend
Generator
Circuit Breaker
Transformer
Disconnect Switch
Ownership Demarcation
Sample Station 2
Company Y
Company X
24/32/40MVA D Trans
115/13 kV Transformer D does not meet I2
115 kV
BUS 6
BUS 5
13 kV
24/32/40MVA C Trans
115/13 kV Transformer C does not meet I2
Sample Station 1
115/13 kV Transformer B does not meet I2
24/32/40MVA B Trans
BUS 4
BUS 2
N.O.
N.O.
13 kV
25 MVA
BUS 3
BUS 1
115 kV
115/13 kV Transformer A does not meet I2
A Trans
Company X
Company Y
Sample Station 3
Revision History
Engineer:
Director:
Approved by:
Date:
Single Line Diagram
XYZ Substation
Company Logo
DWG No:
Rev:

3. Training and Reference Resources

3.1. Will there be any training prior to July 1, 2014?

Yes.

Several webinars and workshops have been scheduled and several training resources are available. Schedules and logistics for the webinars and workshops are posted in the Implementation Schedule. NERC has also posted several training videos on its website. These videos cover both the BES definition and how to apply it, as well as the Bulk Electric System Notification and Exception Tool (BESnet) application.

The following available reference documents may also be of particular interest:

BES Definition Reference Document – Provided to assist Entities with application of the revised BES definition; provides examples of applications of the revised BES definition on specific of BES Elements.

BES Implementation Guidance Document – Provides implementation guidance on the transition to the new BES definition.

All of this information is posted on the NERC Bulk Electric System (BES) Definition, Notification, and Exception Process Project Page, located at:

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

3.2. Will there be any training after July 1, 2014?

Yes. In addition to the resources above, NERC is planning on hosting two additional webinars describing how to use the BESnet application. These will be announced shortly. NERC may schedule additional webinars as needed.

4. Notification of Self-Determination Process

4.1. When can I start entering in my BES Self-Determined Notifications?

The BESNet application will be available to receive BES Self-Determined Notifications on July 1, 2014.

4.2. Can a Registered Entity discuss matters with the Regional Entity prior to submitting a Self-Determined Notification and/or Exception Request?

Yes. NERC encourages Registered Entities to contact applicable Regional Entities to achieve common understanding of the application of the "bright-line" BES definition and corresponding identification of the BES Elements, and to discuss evidentiary expectations before submitting a Self-Determined Notification or Exception Request.

This will help minimize the potential number and extent of submitted BES Exception Requests. Refer to the *BES Notification Review Guidelines* for additional information.

4.3. What information will I need to supply with a notification of self-determinations?

A "Regional Entity BES Notification Review Checklist" is included in the *BES Notification Review Guidelines*, located at:

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

The checklist details information the Regional Entities will consider to support notifications of self-determinations. For example:

- Is the Self-Determined Notification exclusion being submitted on the basis of the Element being a Distribution Element? If yes, provide a record of the status of the Entity's petition filed with FERC.
- Was a sufficiently detailed one-line diagram(s) provided with the Self-Determined Notification?
- Were normally open switches marked in the diagrams?
- Was appropriate hourly integrated flow information provided to support E2 and E3 Exclusions?

The Regional Entities may request additional information, as needed, under existing authority.

4.4. Am I required to notify the Region of a change of BES status due to the new BES definition?

Yes. In Order No. 773, at Paragraph 317, FERC also determined that "registered entities are obligated to inform the Regional Entity of any self-determination that an element is no longer part of the BES." Refer to the *BES Notification Review Guidelines* for additional information.

Conversely, if the result of application of the new BES definition is that an element should be added to the BES, Entities should file a Self-Determined Inclusion Notification with their Regional Entity.

4.5. If nothing has changed in my Element's BES status after applying the new BES definition, do I need to submit a BES Self-Determined Notification?

No.

4.6. Do newly identified Elements require the submittal of Self-Determined Inclusion Notifications?

Yes. Self-Determined Notifications for newly included Elements should be submitted through the BESNet application to the Regional Entity during the 24-month implementation period for the BES definition, beginning July 1, 2014.

In addition, newly identified exclusions of Elements that were previously part of the BES under the prior definition require similar Self-Determined Exclusion Notification through the BESNet application to the Regional Entity.

4.7. Which Entity should provide Self-Determined Notifications for jointly-owned Elements?

For jointly-owned facilities, a lead owner, on behalf of the joint owners, should submit any Self-Determined Notifications.

4.8. Under legacy Regional BES definitions, certain transmission elements were considered as BES, but will now be excluded under the new BES definition. What should be submitted in the Self-Determination Notifications?

Elements excluded by application of the new BES Definition must be reported through the self-determined notification process in the BESNet application. This encompasses any such elements included in the BES by legacy Regional BES definitions (for example, line sections tapped directly off a BES line, transformers with the only primary terminal operated at 100 kV, etc…).

The Entity is expected to supply unique circuit identifiers for each of the newly-excluded Elements along with a one-line diagram clearly identifying the Elements being excluded.

5. Exception Request Process

5.1. What process will NERC utilize to make evaluate BES Exception Requests?

Appendix 5C of the NERC Rules of Procedure sets forth the procedure for requesting and receiving an Exception from the application of the BES definition. Appendix 5C is available at:

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

5.2. What supporting information is needed to submit an exception request?

A "BES Exception Process Review Checklist" is included in the *BES Exception Request Evaluation Guidelines,* located at:

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

Those considerations provide specificity regarding the data and studies that the Regional Entities and NERC require to evaluate an Exception Request and provide submitting entities with additional information as to the level of analysis expected.

As a general principle, studies should model actual control settings and configurations, model the Year One horizon, address a range of system conditions in terms of load level and generation dispatch, and include an explanation of why the system conditions and contingencies studied are sufficient to address the most limiting system conditions relevant to the requested Exception.

5.3. Who evaluates and approves Exception Requests?

Appendix 5C of the NERC Rules of Procedure governs the process by which an Entity may request and receive an Exception.

The Regional Entities will review exception requests in accordance with the *BES Exception Request Evaluation Guideline*. NERC reviews the Regional Entity recommendations, and then NERC decides all BES Exception Requests, subject to an appeal process.

5.4. What is a technical review panel? Who is on it? How are they chosen?

A Technical Review Panel (TRP) is appointed by the Regional Entity to review the Regional Entity's proposed recommendation and provide an opinion on the Exception Request before a Regional Entity issues a Recommendation to NERC to disapprove an Exception Request in whole or in part.

A copy of the TRP's opinion will be provided to the Submitting Entity, and Owner if different, and the Regional Entity. The Regional Entity will not be bound by the opinion of the TRP, but the opinion will become part of the record associated with the Exception Request that is sent to NERC as part of the Regional Entity's Recommendation.

Each Regional Entity is required to establish provisions for a TRP consisting of not less than three individuals appointed by the Regional Entity senior executive (CEO, President, General Manager, etc.). Panel members could be drawn from the Regional Entity's staff, from other Regional Entities' staffs, consultants, or other subject matter experts. However, all panel members must comply with Subsection 7 of Section 403 of the NERC Rules of Procedure on the use of industry subject matter experts and Regional Entity Members, cannot have participated in the review of the subject Exception Request, and must have the required technical background to evaluate Exception Requests.

It is important to note that the TRP differs from the NERC review panel described under Section 8 of Appendix 5C of the NERC Rules of Procedure.

5.5. What is the NERC review panel? Who is on it?

The NERC review panel is a body established by NERC in accordance with the NERC Rules of Procedure, Appendix 5C, to evaluate Exception Requests and review the Recommendation and accompanying materials (including the Technical Review Panel's opinion, if applicable) provided by the Regional Entity associated with a particular Exception Request.

The NERC president will appoint a team of no less than three persons with the required technical background to evaluate Exception Requests. NERC contemplates that its review teams would be drawn from NERC staff resources, supplemented by contractors as necessary, but situations may arise in which NERC may need to call on consultant subject matter experts to participate as members of NERC review panels, who must comply with the conflict of interest process.

It is important to note that the NERC review panel differs from the TRP described under Section 5 of Appendix 5C of the NERC Rules of Procedure.

5.6. How long will the process take?

In general, assuming a complete application, no appeals, and taking the allotted time for each subtask, the process could take up to 11.5 months, but is anticipated to be shorter for less complicated Exception Requests.

If the Exception Request is appealed to the NERC Board of Trustees Compliance Committee pursuant to Section 1703 of the NERC Rules of Procedure, the process could take an additional 8.5 months, totaling 20 months. This does not include timing related to an appeal to the applicable legal authority or Applicable Governmental Authority.

A Regional Entity, upon consultation with NERC, may extend the time frame of the substantive review process for individual Exception Requests beyond the allotted six months pursuant to Section 5.2.2 or in the case where the Registered Entity supplements its Exception Request pursuant to Section 6.0.

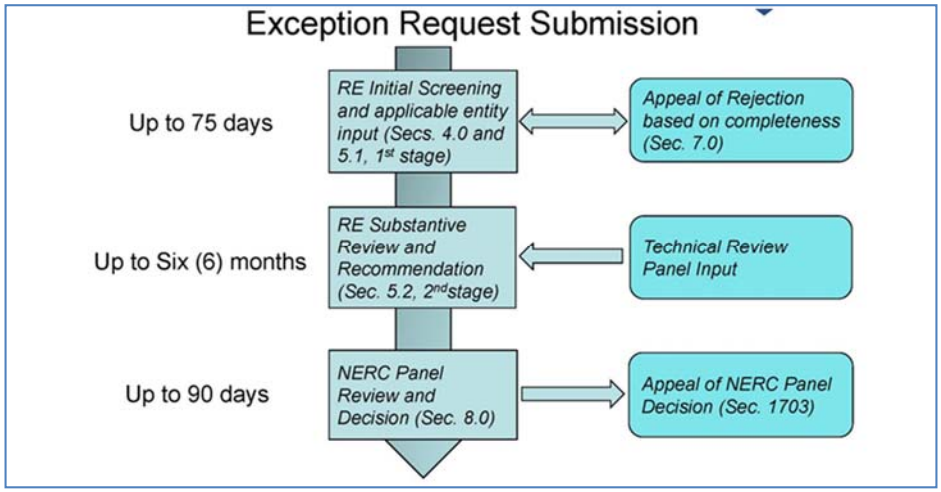


Figure 1: Example of the NERC Exception Process Timeline

5.7. How can an Entity appeal a Rejection of an Exception Request?

Sections 5.1.5b and 7.0 of Appendix 5C of the NERC Rules of Procedure specifically address how a Submitting Entity can appeal a Rejection of an Exception Request by the Regional Entity. Section 5.1.5b states:

> If the Regional Entity rejects the Exception Request in accordance with Section 5.1.5 (a), the Regional Entity's notice shall explain the reason for the Rejection. The Submitting Entity may, within thirty (30) days after receipt of the Rejection, appeal to NERC in accordance with Section 7.0 of this Exception Procedure to reverse the Rejection and to direct the Regional Entity to proceed with a substantive review of the Exception Request.

Also, Section 7.0 states:

> The Submitting Entity may submit to the NERC Director of Compliance Operations, with a copy to the Regional Entity and Owner if different, information that demonstrates that the insufficiencies in an Exception Request Form identified in the notice of Rejection by the Regional Entity pursuant to Section 5.1.5 are incorrect or otherwise do not warrant Rejection of the Exception Request, and that the Exception Request should be accepted and proceed to substantive review. A Submitting Entity's submission to NERC under this Section 7.0 shall be in writing, shall provide the Exception Request which received the Rejection (using the identifier assigned to the Exception Request pursuant to Section 5.1.2), and shall set forth a description of the errors that the Submitting Entity believes are in the notice of Rejection. The Submitting Entity's submission must demonstrate that it is eligible (in accordance with Section 4.1) to submit the Exception Request and that all Required Information for the Exception Request has been provided. NERC will

review the Submitting Entity's submission and the reports submitted by the Regional Entity or Regional Entities pursuant to Section 5.1.5 with respect to the Exception Request, and if NERC determines that the Submitting Entity is eligible (in accordance with Section 4.1) to submit the Exception Request, that all Required Information has been provided, and that the Exception Request should proceed to substantive review, NERC shall, within forty-five (45) days after receiving the submission, issue a decision directing the Regional Entity to proceed to a substantive review of the Exception Request in accordance with Section 5.2. NERC will send a written notice to the Submitting Entity, the Owner if different, and the Regional Entity stating that NERC either directs the Regional Entity to proceed to a substantive review or that NERC does not direct such a review.

5.8. How can an Entity appeal the NERC decision?

Section 9.0 of Appendix 5C to the NERC Rules of Procedure specifically addresses how an Entity can challenge approval or disapproval of Exception Requests. Section 9.0 states:

> A Submitting Entity or Owner aggrieved by NERC's Approval or Disapproval of an Exception Request or termination of an Exception may, within thirty (30) days following the date of NERC's decision, challenge such determination pursuant to Section 1703 of the NERC Rules of Procedure. If neither a Submitting Entity nor Owner challenges, within such period, NERC's determination with respect to any Element to which the Exception Request or the Exception applies, such determination shall become effective with respect to such Element on the thirty-first day following the date of the NERC decision.

5.9. Who can submit BES Exception Requests?

Section 4.1 appendix 5C of the Rules of Procedure states:

> The Owner of an Element may submit an Exception Request for either an Inclusion Exception or an Exclusion Exception regarding that Element.
>
> A Regional Entity, Planning Authority, Reliability Coordinator, Transmission Operator, Transmission Provider, and Balancing Authority that has (or will have upon inclusion in the BES) the Elements covered by an Exception Request within its Scope of Responsibility may submit an Exception Request for the inclusion in the BES of an Element or Elements owned by a Registered Entity, provided that before doing so, (i) the Submitting Entity conferred with the Owner about the reasons for an Exception, and (ii) could not reach agreement regarding the submission

of such an Exception Request. (If the Owner agrees with submitting an Exception Request, the Owner should be the Submitting Entity.)

Only a Regional Entity may submit an Exception Request for the inclusion in the BES of an Element or Elements owned by an Owner that is not a Registered Entity.

Only an Owner or a Regional Entity may submit an Exception Request for the exclusion from the BES of an Element.

5.10. What happens if my system configuration changes after I have an approved Exception Request?

Pursuant to Section 11 of Appendix 5C of the NERC Rules of Procedure, Submitting Entities must notify the appropriate Regional Entity, with a copy to NERC, within ninety days of learning of any change of condition that would affect the basis for NERC approving an Exception Request. If a Regional Entity obtains information that indicates an Exception may no longer be warranted it must also notify NERC. In either instance, NERC will review the notification and determine whether to direct the Regional Entity to perform a substantive review to verify continuing justification for the Exception.

The Submitting Entity and Owner will be notified if the Regional Entity makes a Recommendation to terminate the Exception and will have thirty days from the date of the notice to submit comments or information to NERC to show that the Exception continues to be justified and should remain in effect.

When an Element is included in the BES as a result of the termination of an Exclusion Exception, an implementation plan detailing the schedule for complying with any Reliability Standards applicable to the newly included Element will be developed in accordance with Section 10 as if it were an Inclusion Exception.

There is also a periodic certification process, every thirty-six months, requiring each Registered Entity possessing an Exception to certify that the basis for an Element being included or excluded in the BES through the Exception remains valid. If the certification is not made, the Exception will terminate ninety days after the date the certification was due.

5.11. What if I have Elements that cross multiple Regional Entity boundaries?

Exception Requests for Elements that cross multiple Regional Entity boundaries should identify all Regional Entities involved. The Regional Entities will then determine which Regional Entity will take the lead for coordinating the Exception Request and collecting any additional information from the Entity.

5.12. Do I need to go to my Reliability Coordinator or Balancing Authority before submitting my BES Exception Request?

NERC encourages Entities to coordinate with their Reliability Coordinator and Balancing Authority.

Section 4 of Appendix 5C of the NERC Rules of Procedure requires that the Submitting Entity send copies of Section I and II information to each Planning Authority, Reliability Coordinator, Transmission Operator, Transmission Provider, and Balancing Authority that has, or will have upon inclusion in the BES, the Elements covered by an Exception Request within its Scope of Responsibility. Failure to provide Section I and II information may result in Rejection of the Exception Request as incomplete.

The BES Notifications and Exceptions Tool (BESNet) application handles these notifications.

5.13. If an Exception Request is to be submitted for a jointly-owned Element, which Entity should submit the request?

For jointly-owned facilities, a Lead Submitting Entity, on behalf of the joint owners, should be the Entity submitting any Exception Request.

5.14. What if I don't submit a BES self-determined BES notification for an exclusion or an inclusion as a result of the new BES Definition?

Entities are obligated to notify Regional Entities of changes in its status including BES Elements as required in the NERC Rules of Procedure Section 501.1.3.5. Failure to submit a self-determined BES notification for an Element does not exempt an Entity from compliance obligations (see Paragraph 312 of FERC Order No. 773).

5.15. Should I concurrently file a BES Exception Request with NERC and a petition to exclude local Distribution Elements with FERC?

Order 773-A[4] at Paragraphs 89 and 93 explain that "the two processes are separate, not concurrent and will be used for different determinations" and that FERC "does not direct entities to seek an exception from NERC before seeking a local distribution determination from the Commission."

If concurrent requests are filed with both FERC and NERC, the Exception Request submitted through the NERC BES Notification and Exception Process will be placed "on hold" until FERC has made a determination.

Under the scenario below, three facilities (A, B and C) have not had prior FERC determinations that they are local distribution facilities. Facilities X, Y and Z have had FERC determinations. All six facilities are considered local distribution by the owner.

Paragraph 93 of Order No. 773-A states:

[4] For ease of reference, Order No. 773-A is available at:
http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final_Rule_Rehearing_Clar_BES.pdf

> Thus, if an entity believes its facility is a local distribution facility but after applying the bulk electric system definition including inclusions and exclusions the facility is not excluded, the entity may apply to the Commission to determine whether the facility is used for local distribution. Thus, as explained above, the Final Rule contemplates two separate and distinct processes and does not direct entities to seek an exception from NERC before seeking a local distribution determination from the Commission.

For Facilities A, B and C:

- **Step 1**: Apply the BES core definition – are the facilities above 100kV? – Yes.
- **Step 2**: Do any inclusions or exclusions apply? – If Facilities A, B, and C, are eligible for an Exclusion E3, then they are excluded by definition from the BES.
- **Step 3**: A, B, and C are excluded from the definition of BES.
    - **Step 3a**: Enter this information into BESNet as a notification of self-determined exclusion. Will be reviewed for validation by the Regional Entity with oversight by NERC that the definition was properly applied and no mistakes occurred. The entity must notify the Regional Entity/NERC of any changes in accordance with ROP Section 501.1.3.5.
    - **Step 3b**: If the Regional Entity or NERC disagrees with the self-determined exclusion, there are two options. First, the entity may apply to FERC for determination that these are local distribution facilities.
    - **Step 3c**: Second, if FERC disagrees that these are local distribution, the entity may submit an exclusion exception request. If granted, the entity must submit a certification that the exclusion exception remains valid in accordance with ROP Appendix 5C.

For Facilities X, Y and Z:

- **Step 1**: Apply the BES core definition – are the facilities above 100kV? – Yes.
- **Step 2**: Do any inclusions or exclusions apply? – No, however, FERC has made prior determinations that the facilities are local distribution.
- **Step 3**: The entity should discuss with the Regional Entity whether the FERC determinations are consistent with the approved BES definition.
    - **Step 3a**: If the Regional Entity agrees that the facilities can be removed from application of the BES definition, the Entity may enter this into BESNet as a notification of self-determined exclusion. Will be reviewed for validation by the Regional Entity with oversight by NERC that the FERC determinations are consistent with the proper application of the BES definition. The Entity must notify the Regional Entity and NERC of the change of status of these facilities in accordance with ROP Section 501.1.3.5
    - **Step 3b**: If the Regional Entity or NERC disagrees with the self-determined exclusion, discussions should continue between NERC, the Regional Entity and the Entity to resolve the issue.

6. BES Notification and Exceptions Tool (BESNet)

6.1. What is the BESNet application and for what will it be used?

The BES Notifications and Exceptions Tool (BESNet) is an ERO-enterprise tool that provides a workflow-based on-line process that emulates the BES Exceptions Procedure, as outlined in NERC Rules of Procedure Appendix 5, to route, evaluate, and take actions on Exception Requests and Self-Determined Notifications.

Requests for Exceptions and Notifications of Self-Determination to the BES will only be accepted through the BESNet application.

Entities that anticipate submitting a BES Exception Request should contact their applicable Regional Entity, review the relevant training and resource materials, and establish a user account for the BESNet application.

6.2. When will BESNet be available for submitting Exception Requests or Self-Determined Notifications?

The web-based BESNet application will be available July 1, 2014, for entering Exception Requests or Self-Determined Notifications.

6.3. Will there be software-related User Guides?

Users Guides for the BESNet application will be available and posted at:

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

The *BESNet Users Guides* will be updated periodically based on feedback received by the user group.

6.4. Is the information I enter into the BESNet application safe and secure?

NERC has undertaken a number of steps to secure the BESNet application:

- The BESNet databases are fully encrypted.
- During development, “white-box” and “gray-box” software security assessments were performed, and potential vulnerabilities were identified and addressed.
- Penetration tests of the BESNet infrastructure were performed and passed in 2013 and 2014, and will be periodically repeated.
- BESNet servers are monitored by a third party.
- Internal and external vulnerability scans are routinely performed on the ERO Environment.
- User vetting process is performed during account set-up.
- All application access and communication between servers in the BESNet environment is encrypted via SSL protocols that have been verified to be free of the “Heartbleed” vulnerability.

6.5. Am I required to register for BESnet access?

Entities who intend to submit Self Determined Notifications or Exception Requests must have an ERO Enterprise account with access to the BESnet application in order to do so. Additionally, all entities registered as a Reliability Coordinator, Planning Authority, Transmission Operator, Transmission Planner, or Balancing Authority must have an ERO Enterprise account with access to the BESnet application in order to ensure receipt of notifications of any BES Exception Requests made by other Registered Entities (e.g. Transmission Owners, Generator Owners) for facilities within the recipient's area of responsibility.

6.6. Our company is divided into several organizational units that are exclusively registered as different NERC Functional Entities. How should we register for BESnet access?

We are asking all registered entities to set up an Entity Administrator. The BESnet application grants access to users based on NCR number, so one person's account can have access to multiple NCRs. Depending on how your company is organized, you may have an account with access for all NCRs, an account for each NCR, or any mix of the two. The same is true for regular (non-administrator) user accounts. Storing and processing of actual submissions is handled by NCR, rather than being associated with a specific user.

6.7. I am preparing a series of Self-Determined Notifications (SDNs) and Exception Requests (ERs) for a number of Elements on my transmission system. How should the groupings of Elements be organized so as to provide an orderly and efficient approach that will minimize effort, aid review and expedite approval?

When submitting either an SDN or an ER, multiple Elements (either at the same location or at different locations within the geographic boundaries of a Regional Entity) may be included in one submission with all such Elements or sets of connected Elements separately identified. The Elements within a submission must share a common basis for their BES categorization, and should be similar in form and/or function to aid in efficient processing (for example, all transformers of a certain type, size, or configuration).

Each submission should be as straightforward as possible while including the largest grouping of similar Elements. Considerations to keep in mind include:

a) SDNs must be submitted separately from ERs. Because the method pf processing SDNs, is different than that of ERs, there is no way in the BESNet application to create a single submission that contains both a Notification and an Exception Request.
b) The basis (Core Definition, Not Core Definition, the specific Inclusions, and the specific Exclusions) for an underlying Element or Elements classification within a single submission cannot be mixed. For example, a user cannot submit an SDN

based on both I1 AND I2. While you can include multiple elements in a single submission, their BES classification must share a common basis.

c) Submissions may be grouped on a geographical basis, a regional basis, or any other basis that you desire (for example, Eastern Operating Company, Western Operating Company, etc.)
d) Multiple inter-regional Elements cannot be submitted as part of a single SDN or ER.
e) The BESNet "association" function should be used for interrelated submissions. For example, an entity could place generation related exclusions in one ER, and then use the "Associated Exception Request" function to link to another ER containing related transformer and/or line Elements.
f) Include supporting documentation with your submissions that provide sufficient evidence supporting the basis for BES classification. Include one-line diagrams that provide sufficient detail to support the basis of your submission. Google maps or other aerial photographs are not sufficient.
g) A short summary of the logic being applied, which references the submitted supporting documents and cross references any relevant NERC guidance, will expedite the review process.

7. Compliance and Registration Questions

7.1. What is the implementation plan for the new BES definition, and when do the related compliance obligations begin?

The new BES definition becomes effective July 1, 2014. According to the *Implementation Plan for Project 2010-17: Definition of BES*, the compliance obligations begin:

- Twenty-four months after the applicable effective date of the definition (for newly identified Elements), or
- If a longer time frame is needed for an Entity to be fully compliant with all standards applicable to an Element or group of Elements that are newly identified through application of the BES definition, the appropriate time frame may be determined on a case-by-case basis by mutual agreement between the Regional Entity and the Element owner/operator, and subject to review by the ERO.

7.2. When will compliance be mandatory with NERC Reliability Standards for existing Elements that are newly identified as BES Elements?

For existing Elements that have not been a part of the BES prior to July 1, 2014, but have now been newly identified as part of the BES, Entities will need to be in compliance with the NERC Reliability Standards by July 1, 2016.

7.3. When do compliance obligations begin for newly built Elements that are classified as BES Elements under the new BES definition?

After July 1, 2014, for those newly built Elements that qualify as BES Elements, Entities must be compliant for that Element as of its energization, as per current processes.

Existing Facilities that are now part of the BES and remain a part of the BES must remain compliant at all times.

7.4. What are the obligations of the owner of a Facility that is designated as a part of the BES?

Users, owners, and operators of the BES Facilities must register as transmission owners, generation owners, transmission operators, or generation operators as appropriate, according to the NERC Statement of Compliance Registry Criteria.

Entities owning or operating BES Elements are subject to compliance with the applicable NERC Reliability Standards. It should be noted, however, that several standards refer to Elements that are connected to or impact Reliable Operation of the BES and, therefore, standards may apply in such cases to non-BES Elements.

7.5 If I need to register based on the new BES definition, when should I register?

Entities that have existing Elements that are newly identified as part of the BES by the application of the new BES definition are encouraged to register as soon as practical after July 1, 2014. However, if there are any questions as to whether such Elements should be excluded from the BES through the Exception Request process, Entities should contact the appropriate Regional Entity regarding registration.

7.6. If an Entity does not own or operate BES assets, does that mean they have to follow NERC standards?

Yes, if they meet other criteria in the NERC *Statement of Compliance Registry Criteria* to be a Registered Entity. NERC Reliability Standards are applicable to users of the Bulk Electric System, not just owners and operators. As an example, Distribution Providers, Purchasing-Selling Entities, and Load-Serving Entities are users of the BES, even though they may not own or operate Facilities in the BES.

7.7. Can an Entity's registration requirements change as a result of applying the new BES definition?

NERC's objective in implementing the revised BES definition is to ensure that the proper Entities are registered and responsible for Reliability Standards that are necessary to ensure the reliability of the BPS. In Order No. 773 (at Paragraph 55), FERC stated, "[w]e do not expect there to be significant numbers of entities either needing to register or deregister due to the change in definition." NERC shares FERC's expectation that only a small number of Entities will require changes to their NERC registration as a result of the revised BES definition.

An Entity seeking to modify its current registration, including de-registration or deactivation, must inform its applicable Regional Entity of this change in status. In turn, the Regional Entity will notify NERC of such changes. All changes to registration are processed by the NERC registration and certification department, in accordance with the NERC Rules of Procedure.

7.8. If an Element is excluded from the BES through an exception request, what happens to compliance obligations, monitoring and enforcement?

From the point in time at which the exception request is made to such time as that request is approved, compliance obligations remain in force. Once an Element is excluded from the BES through an approved Exception Request, for all cases in which the excluded Element would have previously been subject to Reliability Standards and Requirements, compliance obligations for those standards will be considered to have ceased upon the affirmative determination of the exception request.

7.9. If an Element is excluded from the BES through self-determination, what happens to compliance obligations, monitoring and enforcement?

The Notification will be reviewed for validation by the Regional Entity, with oversight by NERC, to ensure that the BES Definition was properly applied and no mistakes occurred. The registered entity can facilitate this effort by reviewing these situations with the Regional Entity prior to formally submitting the Notification. This will provide the greatest confidence of appropriate application of the BES Definition to the specific circumstances and facilitate consistent application of the Definition. Once validation is concluded, the registered entity will be advised of the determination. An Element will not be excluded from the BES until the removal is validated.

Until the validation process described for Self-Determined Notifications of Exclusion is completed, the registered entity has the potential to be subject to applicable Reliability Standards. Any instances of non-compliance for potentially excluded Elements will be held in abeyance until such time as the Notification is validated by the Regional Entity, with NERC oversight as described above. If the Self-Determined Notification of Exclusion is accepted as valid, instances of potential non-compliance involving excluded Elements that occurred after the submission of the complete and proper Notification up to the date of its validation will be closed, barring any unique facts and circumstances. A Self-Determined Notification of Exclusion that is incomplete or based on improper application of the BES Definition will result in Elements associated with that Notification remaining subject to compliance monitoring and enforcement until such time all required information is submitted and the BES Definition is correctly applied.

If a Regional Entity believes that a Notification of a Self-Determined Exclusion is based on an incorrect application of the Definition and is unable to come to a common understanding of the Definition with the submitting entity, the Notification will be rejected and the Element at issue will remain part of the BES by application of the Definition. Registered Entities retain the option to pursue exclusion through the exception process.

7.10. In FERC Order No. 773-A (P 109), FERC stated, "in the absence of bad faith, if a registered entity applies the bulk electric system definition and determines that an element no longer qualifies as part of the bulk electric system, upon notifying the appropriate Regional Entity that the element is no longer part of the bulk electric system the element should not be treated as part of the bulk electric system unless NERC makes a contrary determination in the exception process." How is NERC implementing this language?

NERC is implementing its processes with the expectation that entities will submit Self-Determined Notifications in "good faith." Good faith Self-Determinations are those that are made consistent with the BES Definition and reference materials provided by NERC. Taken together, Order Nos. 773 and 773-A, as well as the NERC Rules of Procedure, point to the need for, and appropriateness of, NERC and the Regional Entity review of a Notification to determine if it comports with the Definition and validate the Notification to confirm appropriate application of the Definition.

7.11. For excluded facilities, do I still have any compliance obligations?

Possibly. The BES definition by itself does not establish whether or not an entity has a responsibility to comply with NERC standards. In order to understand compliance obligations, an entity must consider its registration obligations, the applicability of the standards, and the BES categorization of its elements and facilities. The Registration Criteria contained in Appendix 5B of NERC's Rules of Procedure describe what entities must register, and for what functions they must register. These functional registrations generally define what standards may apply to an entity (*e.g.,* BAL-002 Disturbance Control Performance; TPL-001 Transmission System Planning Performance Requirements), although some standards include additional criteria to further refine the applicability of a standard (*e.g.,* BAL-001 Real Power Balancing Control Performance and its limited applicability for Balancing Authorities; PRC-023 Transmission Relay Loadability and its limited applicability based on circuit criteria). Additionally, some standards apply to functions performed regardless of the existence of BES elements and facilities (*e.g.,* IRO-001 Reliability Coordination - Responsibilities and Authorities). Finally, some standards apply to specifically identified equipment that comprises the Bulk Power System, of which the Bulk Electric System is a subset (*e.g.,* PRC-010 Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program). In summary, all three areas – registration, standards applicability, and the BES definition – must be considered together in order to fully understand an entity's compliance obligations.

7.12. If I am registered for the Distribution Provider function and I do not own or operate any BES Elements, can I request deactivation of my compliance registration?

BES protection schemes, including Underfrequency Load Shedding (UFLS), Undervoltage Load Shedding (UVLS), or Special Protection Systems (SPS) and Remedial Action Schemes (RAS), support the reliability of the Bulk Electric System (BES), often serving as the "last-resort" tool for avoiding a total power system blackout. Consequently, NERC and the Regional Entities will not approve the deactivation of the DP function for Registered Entities on the NERC Compliance Registry that have these types of protection devices, solely on the basis that the entity does not own or operate a BES Element by application of the BES Definition. NERC and the Regional Entities will evaluate the relevant facts and circumstances in reaching a decision.

Registered Entities currently performing the DP function may determine to file a Self-Determined Notification of Exclusion of Elements based on the current BES Definition. There is no automatic change in the registration status of an entity for any functional registration categories if a particular Element is excluded from the BES Definition either through the Self-Determined Notification of Exclusion or the BES Exception process. Determinations of registration status are addressed through the registration program. NERC believes that the deactivation of the DP function registration of Registered Entities that have responsibilities relating to BES protection schemes including UFLS, UVLS, and SPS/RAS equipment would present a reliability risk due to the lack of compliance oversight. These types of equipment are essential to the reliable operation

of the BES, even in cases where the equipment is installed below the BES 100 kV bright line. In addition, NERC will closely evaluate requests which involve entities that have transmission Remedial Action Schemes or other types of schemes that have the same or similar BES system protection objectives.

Registered Entities should note that if an Element owned by an entity is excluded from the BES Definition, either through an Exclusion Exception Request or a validated Self-Determined Notification of Exclusion, this exclusion alone does not necessarily provide for deactivation of any functional registration from the NERC Compliance Registry. The Registration Criteria states that a "Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System." The list includes references to required UFLS programs, UVLS programs, SPS/RAS and transmission Protection Systems. The importance of these programs to system reliability is not diminished by the revised BES Definition.

Under the current registration rules, entities have an opportunity to establish that they are not material to the reliability. Such determinations depend on the specific facts and circumstances. In the future, NERC is moving forward with a new proposal for Distribution Provider registration criteria related to the Risk-Based Registration (RBR) initiative. The proposed criteria will accommodate those DPs who are registered only as a result of the owning of UFLS systems and will include a reduced set of reliability standards for which UFLS-Only DPs will be responsible. RBR also will build on current authority to allow an entity to make a case that it should not remain registered if it is not material to the reliability of the BES. To ensure consistency, a new materiality test is being developed that would be reviewed by a new NERC-led panel comprised of NERC and Regional Entity participants, that the entity is not material to the reliability of the BES and should not remain registered as a DP. The draft design program also includes a process for determining a sub-set of applicable Reliability Standards.

NERC notes that, to the extent that direct application of the BES Definition results in a determination that an Entity's Elements are not BES, an Inclusion Exception process can be initiated by a Responsible Entity to bring such Elements back into the BES. While this would not affect the DP registration status, it may affect other functional registration categories.

8. NERC Process

8.1. Will the BES definition be applied consistently across the Regional Entities?

The BES Drafting Team has prepared a *Bulk Electric System Definition Reference Document* to support consistent application of the BES definition. Those documents are posted at:

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

NERC and Regional Entity staffs are coordinating the implementation of the new BES definition and have developed several procedures to ensure consistency. A common checklist has been developed for Regional Entities to use when reviewing Self-Determined Notifications of BES changes. Challenges to the notifications are done via the Exception process. Guidelines for BES Exception Evaluation were also developed for use by NERC and the Regional Entities. Finally, NERC must approve all Exception Requests for inclusion or exclusion from the BES.

8.2. If my Element is not considered a part of the BES, might I still be required to provide information to NERC about it?

Yes. Even if an Element is not classified as part of the BES, information about it may be needed to analyze the effects of load, reactive support, and energy injection on the reliability of the overall electric system. One example of data that might be required is modeling data for powerflow and dynamic analysis. Similarly, information on underfrequency load shedding (UFLS) and undervoltage load shedding (UVLS) may be necessary to understand expected system performance. Additional data may be required by NERC or the Regions based on specific configurations or scenarios.

9. FERC

9.1. Does FERC have a role in designating Facilities as part of the BES?

In Order No. 773 (at Paragraph 66), FERC approved NERC's BES Exception Request process to determine the technical issue of whether Facilities are part of the BES; however, FERC determined that the jurisdictional question of whether Facilities are "used in local distribution" will be decided by FERC. Thus, FERC reserved authority to designate sub-100 kV Facilities, or other Facilities, as part of the BES.

FERC also established a process by which an Entity can seek a determination by FERC whether Facilities are "used in local distribution" as set forth in the Federal Power Act. The Commission will make such case-by-case jurisdictional determinations by applying the Seven Factor Test set forth in Order No. 888.

9.2. Should I concurrently file a BES Exception Request with NERC and a petition to exclude local Distribution Elements with FERC?

Order 773-A at Paragraphs 89 and 93 explain that "the two processes are separate, not concurrent and will be used for different determinations" and that FERC "does not direct entities to seek an exception from NERC before seeking a local distribution determination from the Commission."

When and whether to submit such a jurisdictional question to FERC are business and legal decisions for a registered entity, upon which NERC is not opining in this Frequently Asked Question list.

10. Definition Questions

10.1. Protection Systems were explicitly included in the Legacy Regional Definition and the new NERC BES Definition is silent on Protection Systems. Do I need to do anything in BESnet for these Protection Systems?

No. Because Protection Systems are neither included nor excluded per the NERC BES Definition, Entities are not required to provide a Notification of Self-Determination to their Regional Entity or submit Exception Requests for these Protection Systems through the BESNet application. To the extent that a Protection System is needed to comply with a Reliability Standard (i.e., PRC-005), compliance obligations continue, independent of the application of the NERC BES definition.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff Webinar

PLEASE WAIT
WE WILL BEGIN SHORTLY

May 2, 2014

RELIABILITY | ACCOUNTABILITY



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Overview of the BES Definition

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

NERC BES Kickoff Webinar

May 2, 2014

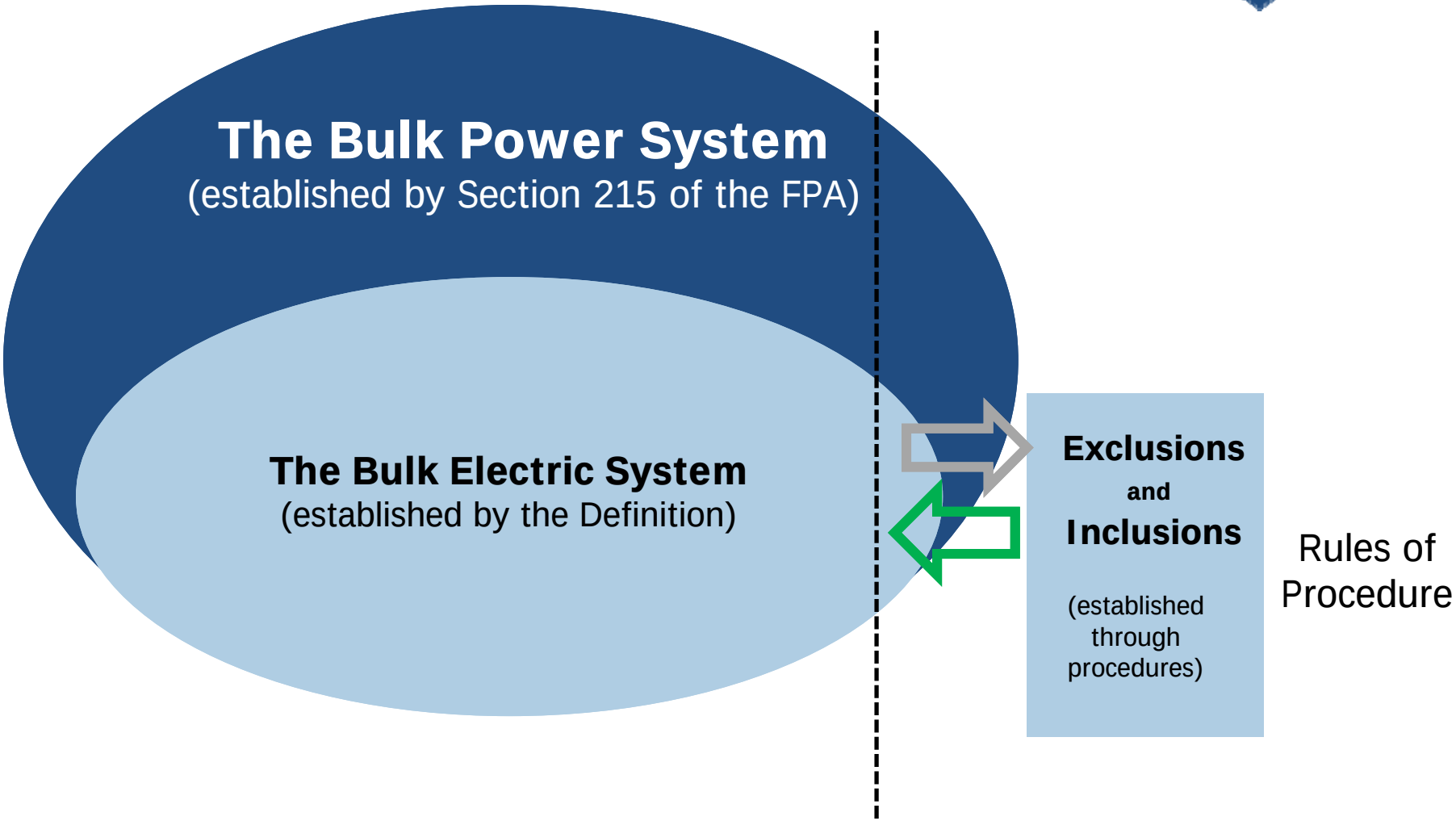
RELIABILITY | ACCOUNTABILITY



BES Definition at a Glance

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

What is the Bulk Electric System?



BES 'Core' Definition

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

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

Inclusions

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

I1. BES Transformers

I2. Real Power Resources

I3. Blackstart Resources

I4. Dispersed power producing resources meeting certain criteria

I5. Reactive Power Resources

Exclusions

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

E1. Radial Systems

E2. Retail Generation

E3. Local Networks

E4. Reactive Power Devices installed solely for retail customers

How to Apply the BES Definition, Inclusions, and Exclusions

Consistent methodology outlined in the BES Definition Reference Document

STEP 1: CORE DEFINITION

STEP 2: INCLUSIONS

STEP 3: EXCLUSIONS

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

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

BES Notifications

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

Self-Determination Notification Information Requirements

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

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



BES Exceptions



Considerations:

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

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



Who can Submit an Exception Request?

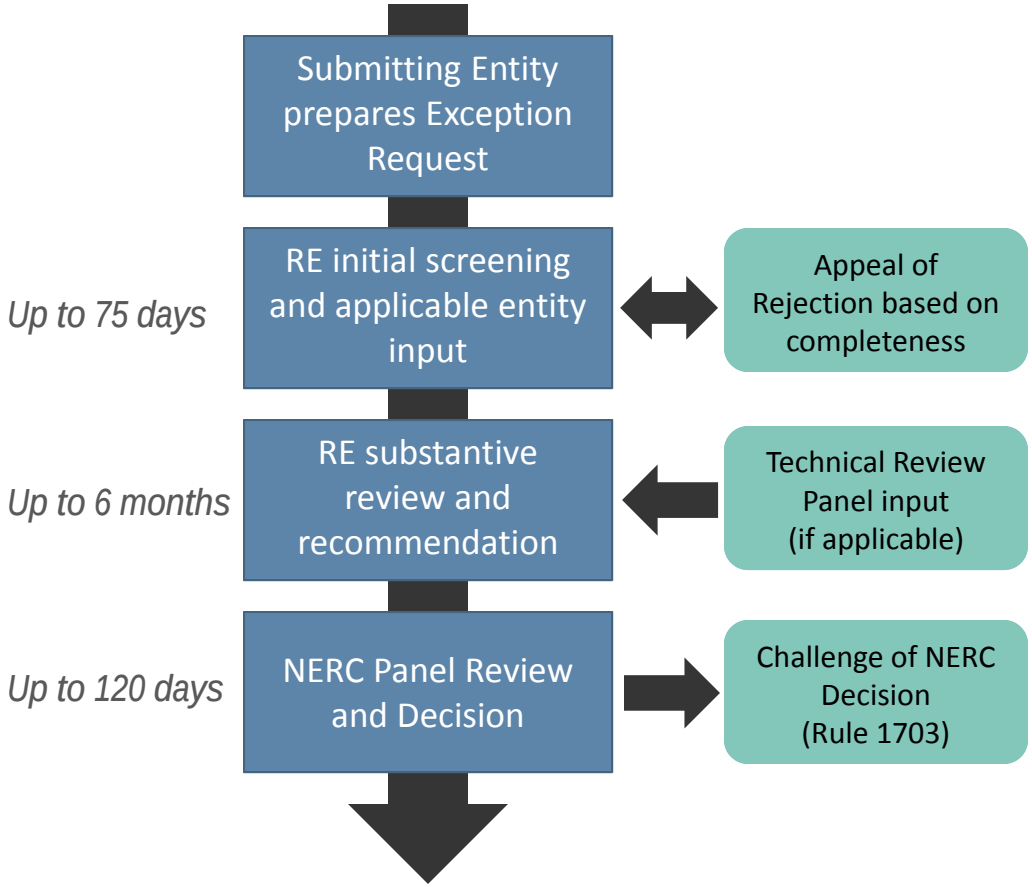
- Owner of the Element(s)
- Regional Entity
- Entity with Scope of Responsibility for the Element(s) under consideration:
  - Regional Entity
  - Planning Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Planner
  - Balancing Authority



The Exception Request Process

The Main Steps in the Exception Process:

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



Many Resources to Assist You

- **Bulk Electric System Definition Reference Document**

  Describes the application of the BES Definition

- **BES Notification Review Guidelines**

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

- **BES Exception Request Evaluation Guidelines**

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

- **BES Implementation Reference Document**

  Outlines standards applicability and registration expectations

Many Resources to Assist You

- **BESnet Application Users Guide**

  Manual for the online BESnet application

- **Frequently Asked Questions (FAQ)**

  Explains application, submittal, and process for BES Definition implementation

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

  Regulations approving modified BES definition

- **NERC Rules of Procedure**

  Section 500 and Appendix 5C

- **Various White Papers**

  Providing Technical Justification

For Additional Information

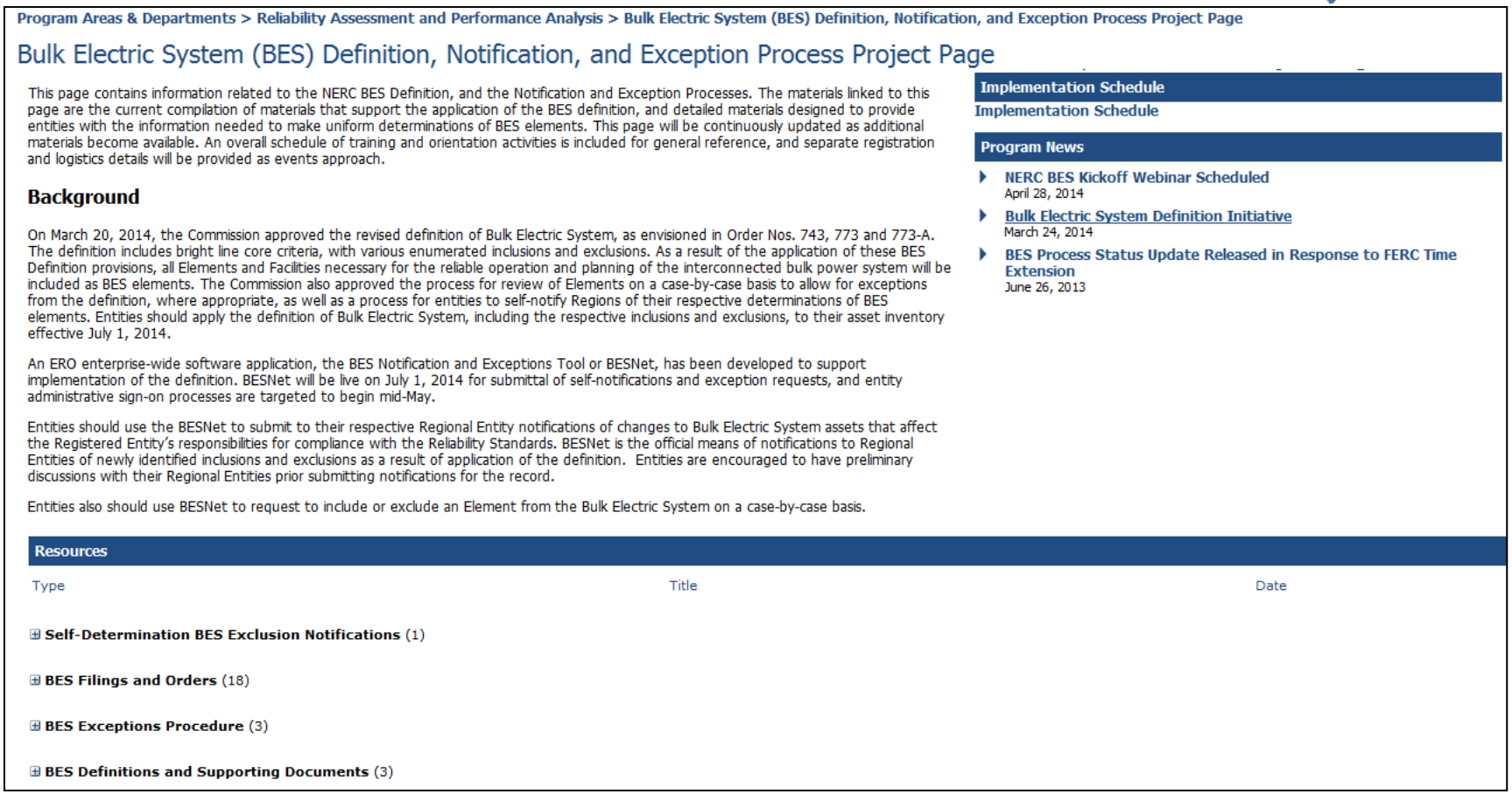


…and most important,

HOW?

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

For Additional Information



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

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

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

Background

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

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

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

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

Implementation Schedule

Implementation Schedule

Program News

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

Resources

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Overview of BESnet

Justin Lofquist, ERO Enterprise Project Manager, NERC

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY






Bulk Electric System Notifications and Exceptions Tool

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Actions

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

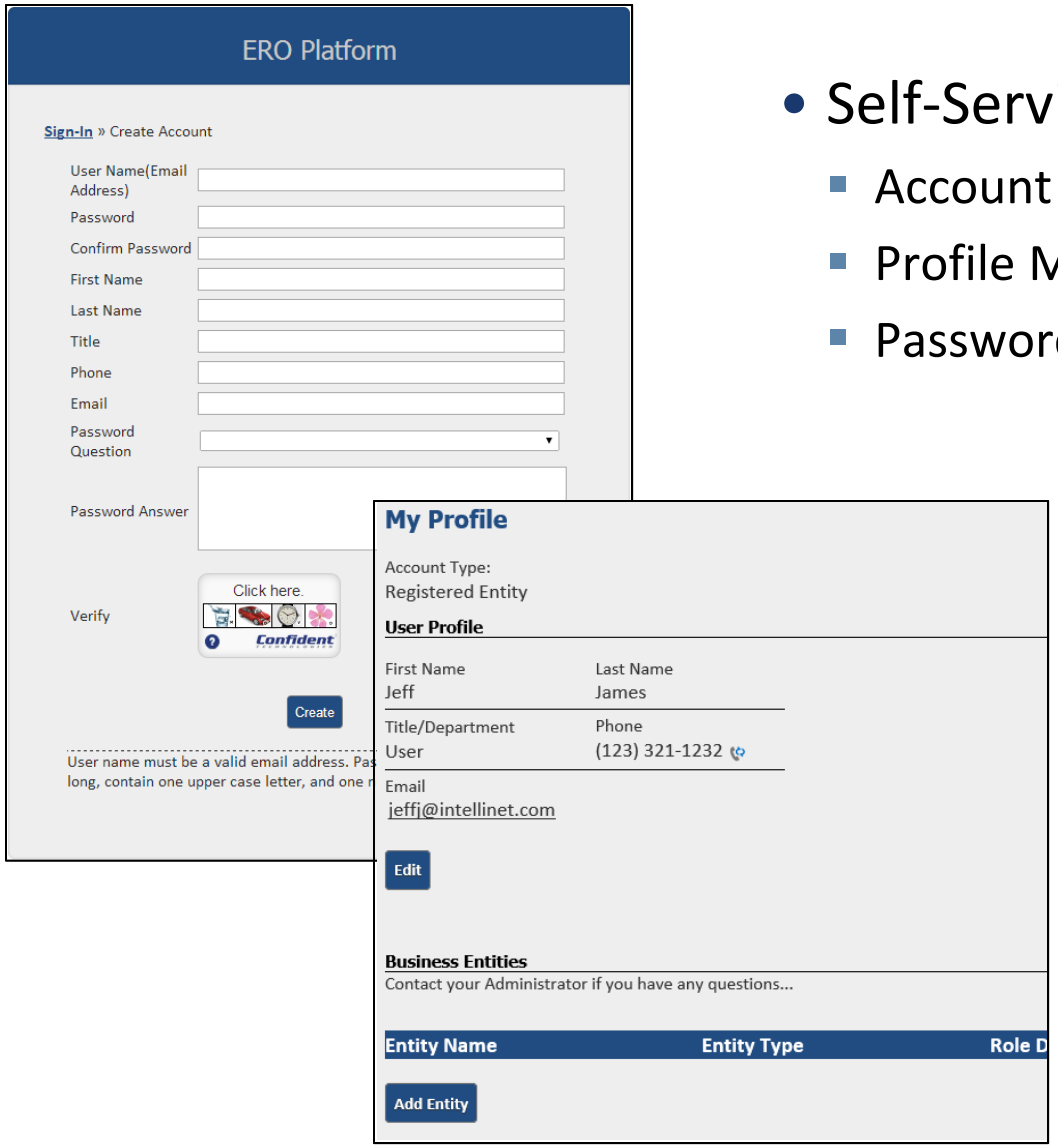
- Automation of NERC Rules of Procedure Appendix 5c
  - Registered and Unregistered Entities:
    - Submission, Appeals and Challenges
  - Regional Entities
    - Initial and Substantive Reviews, Recommendations
  - NERC
    - Proposed and Final Decisions, Certification

Actions (cont.)



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

Accounts



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

- Multi-Entity Management
  - Single user to Multiple Entities

- Distributed Administration
  - Administrator per Entity

Dashboard



Exception Requests

Show in Dashboard

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

Show 10 entries

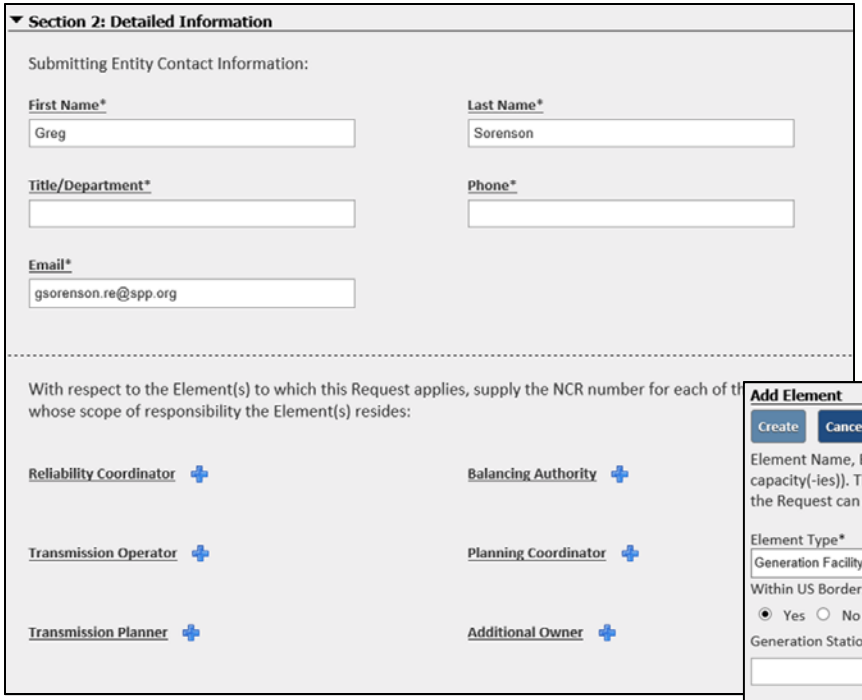
ID	Status	Type	Submitted	Submitting Entity	Region	Next Action Due
2014-FRCC-NCR00005-Exception00002	Certified - Notification of Change	Exception Request	02/28/2014 11:43:15 EST	Calpine Corporation	FRCC	01/01/2017 - Next Certification
d5a4f648-f548-4708-b9f4-d8429236b156	Rejected	Exception Request	02/28/2014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

Showing 1 to 10 of 19 entries

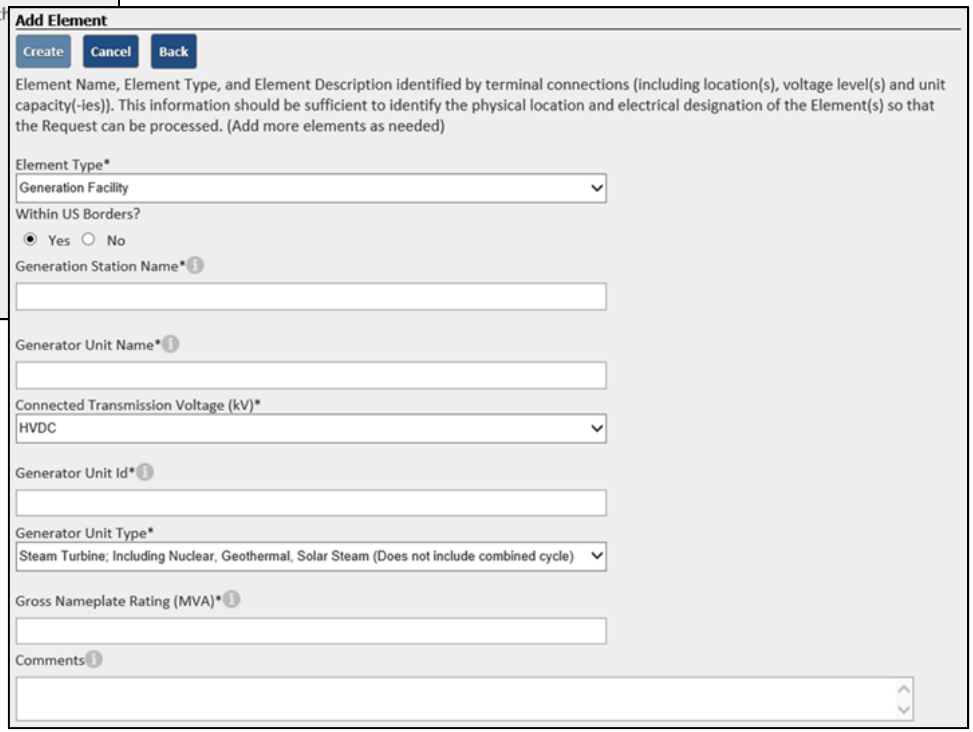
First Previous 1 2 Next Last

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

Creating Exception Requests

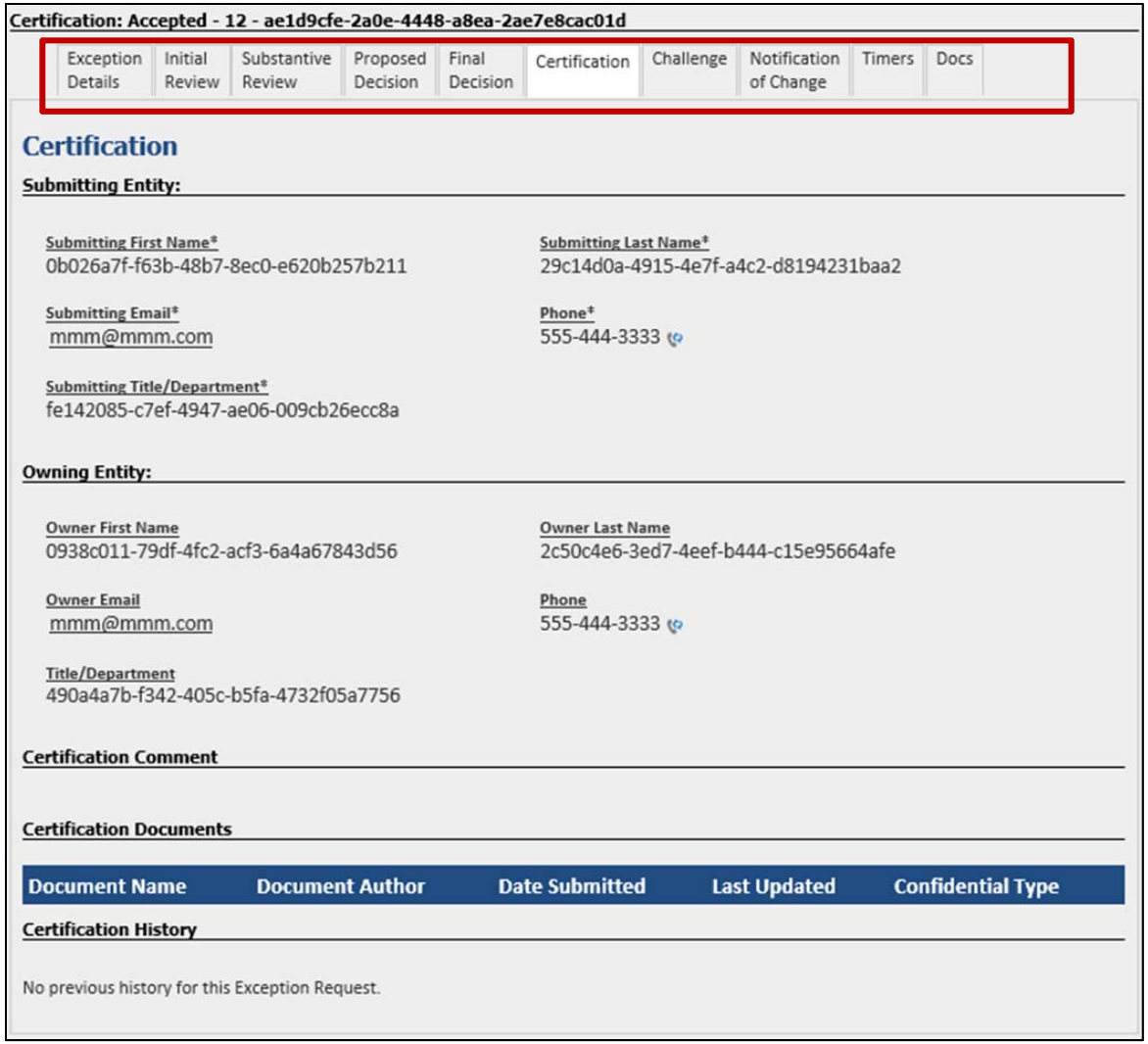


- Exception Request Details
  - Identify Entities within the Scope of Responsibility for an Exception Request



- Add Elements to Exception Request
  - Input Element Characteristics

Exception Requests in Certification


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

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

Certification

Submitting Entity:

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

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

Submitting Email*
mmm@mmm.com

Phone*
555-444-3333

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

Owning Entity:

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

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

Owner Email
mmm@mmm.com

Phone
555-444-3333

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

Certification Comment

Certification Documents

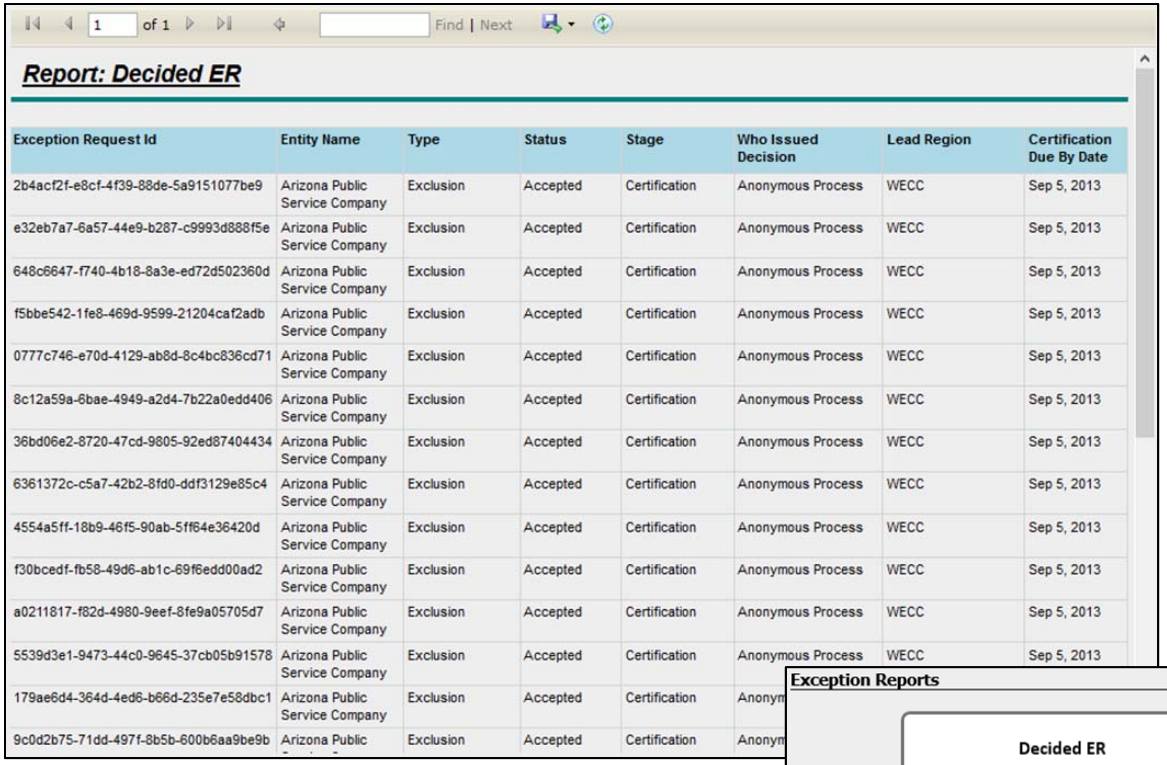
Document Name	Document Author	Date Submitted	Last Updated	Confidential Type

Certification History

No previous history for this Exception Request.

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

Reporting

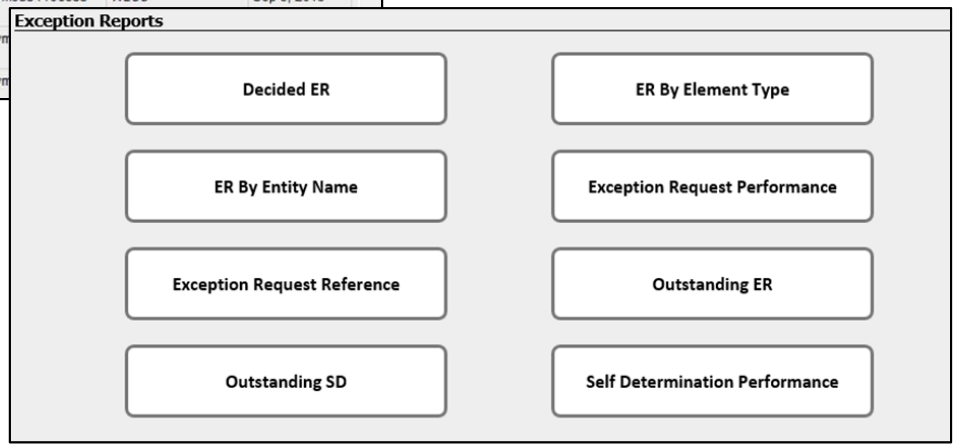


1 of 1 Find | Next

Report: Decided ER

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

- Multiple Report Types



- Security trimmed to return only authorized records

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Review of BES Implementation Schedule

Andy Rodriquez, Director for RAPA, NERC

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY






Key Dates

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

Training Activities

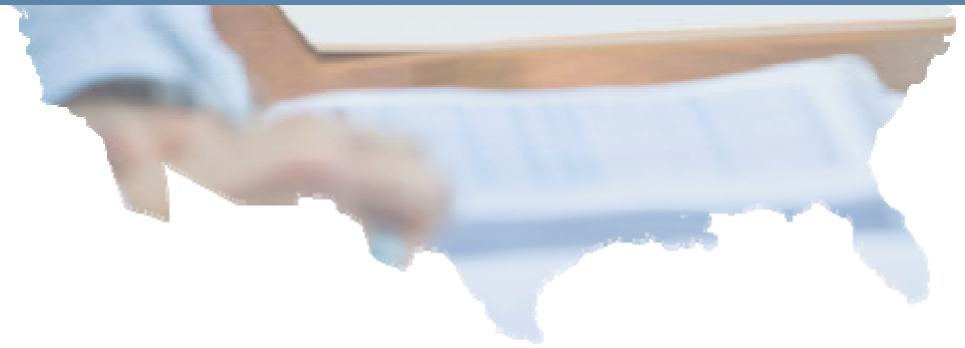
- **Regional BES Training and Workshops (confirmed)**
  - March 17-18 – SERC Compliance Seminar (completed)
  - March 25 – RF Compliance Seminar (completed)
  - April 21-22 – FRCC BES Workshop (completed)
  - May 21 – TRE Standards and Compliance Workshop
  - May 27-30 – NPCC 2014 Spring Compliance and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

Training Activities

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



Questions and Answers



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Bulk Electric System Definition

Question and Answer Sessions
Supporting Diagrams

PLEASE WAIT
WE WILL BEGIN SHORTLY

RELIABILITY | ACCOUNTABILITY



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Bulk Electric System Definition

Question and Answer Sessions
Supporting Diagrams

RELIABILITY | ACCOUNTABILITY



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INCLUSIONS I1

Inclusion I1 - Transformers

The **transformer's** primary and secondary terminals are operated at 100 kV or above, and therefore the transformer is included in the BES by application of Inclusion I1.

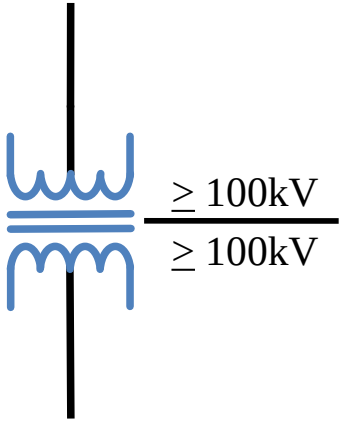


Figure I1-1: Typical Two Winding Transformer (BES)

The **transformer's** primary terminal is operated at 100 kV or above, however the secondary terminal is <u>not</u> operated at a voltage of 100 kV or above. Therefore the transformer is <u>not</u> included in the BES by application of Inclusion I1.

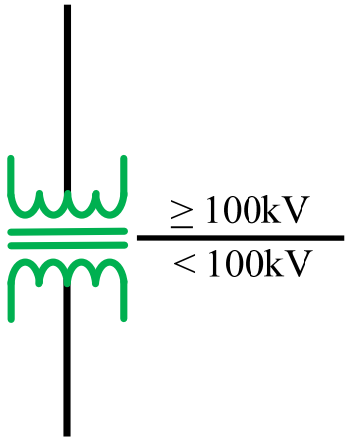
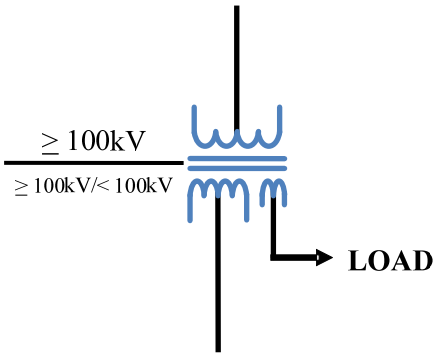


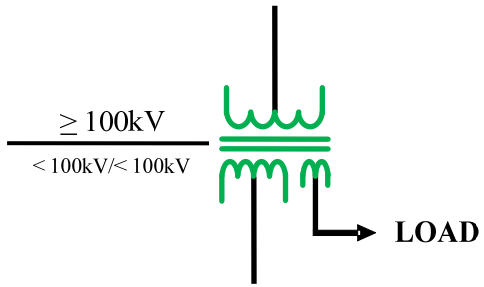
Figure I1-3: Typical Two Winding Transformer (non-BES)

Inclusion I1 - Transformers



The **transformer's** primary terminal and one secondary terminal are operated at 100 kV or above, and therefore the transformer is included in the BES by application of Inclusion I1. Since the transformer is one Element, all windings internal to the transformer (including the tertiary winding) would be included in the BES. The Load and the connection to the tertiary winding, indicated in the diagram, are non-BES as they are connected at a voltage < 100 kV.

Figure I1-2: Typical Three Winding Transformer (BES)



The **transformer's** primary terminal is operated at 100 kV or above, however neither of the secondary terminals are operated at a voltage of 100 kV or above. Therefore the transformer is not included in the BES by application of Inclusion I1. The Load and the connection to the tertiary winding, indicated in the diagram, are non-BES as they are connected at a voltage < 100 kV.

Figure I1-4: Typical Three Winding Transformer (non-BES)

INCLUSIONS I2

Inclusion I2 – Generating Resources

The **generator** has a gross individual nameplate rating > 20 MVA and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 the **generator including the generator terminals through the high-side of the step-up transformer** is included in the BES.

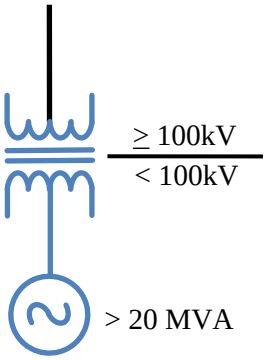


Figure I2-1: Single Generator (BES)

The **generator** has a gross individual nameplate rating ≤ 20 MVA (actual 19 MVA) and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 the **generator including the generator terminals through the high-side of the step-up transformer** is not included in the BES.

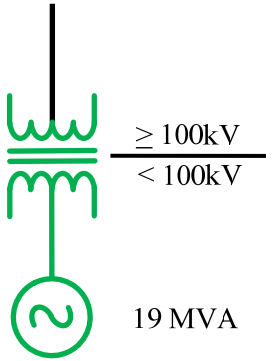
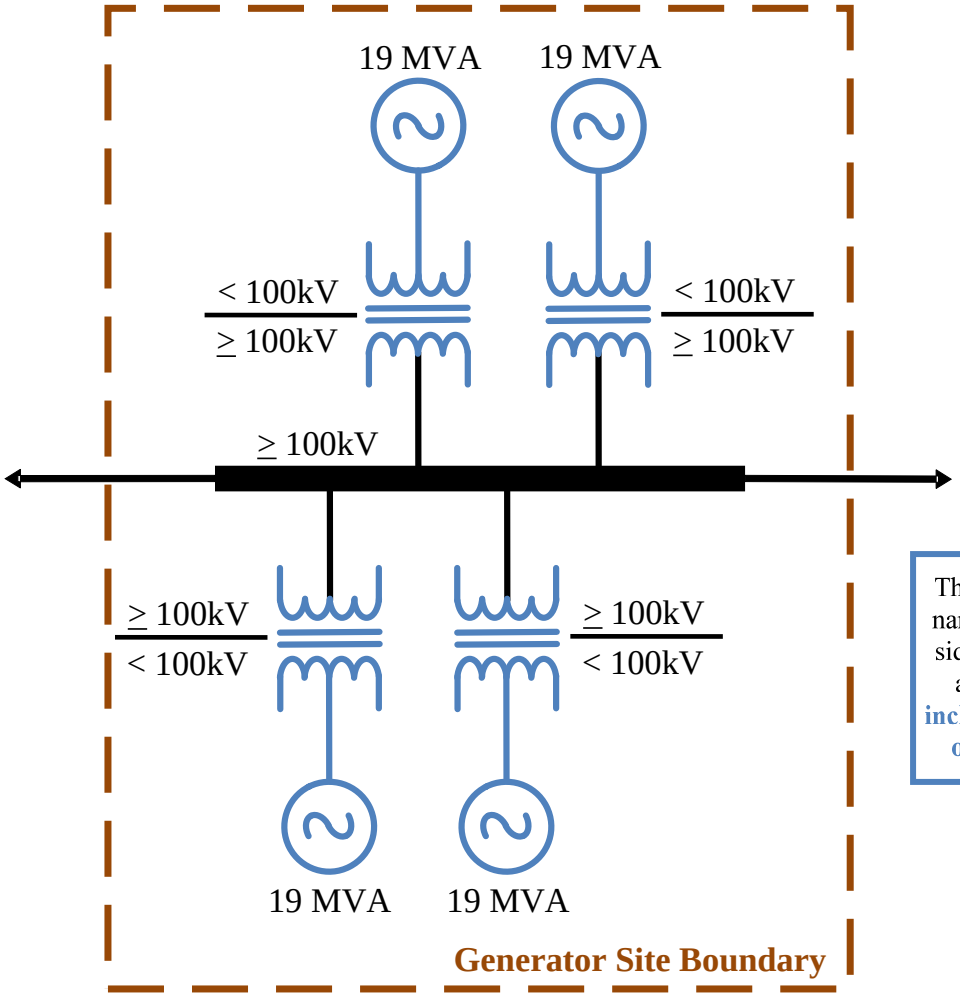


Figure I2-2: Single Generator (non-BES)

Inclusion I2 – Generating Resources



The generation site has generation with a gross aggregate nameplate rating of 76 MVA connected through the high-side of the step-up transformers at a voltage of 100 kV or above. By application of Inclusion I2, the **generators including the generator terminals through the high-side of the step-up transformers** are included in the BES.

Figure I2-3: Multiple Generators at a Single Site (BES)

Inclusion I2 – Generating Resources

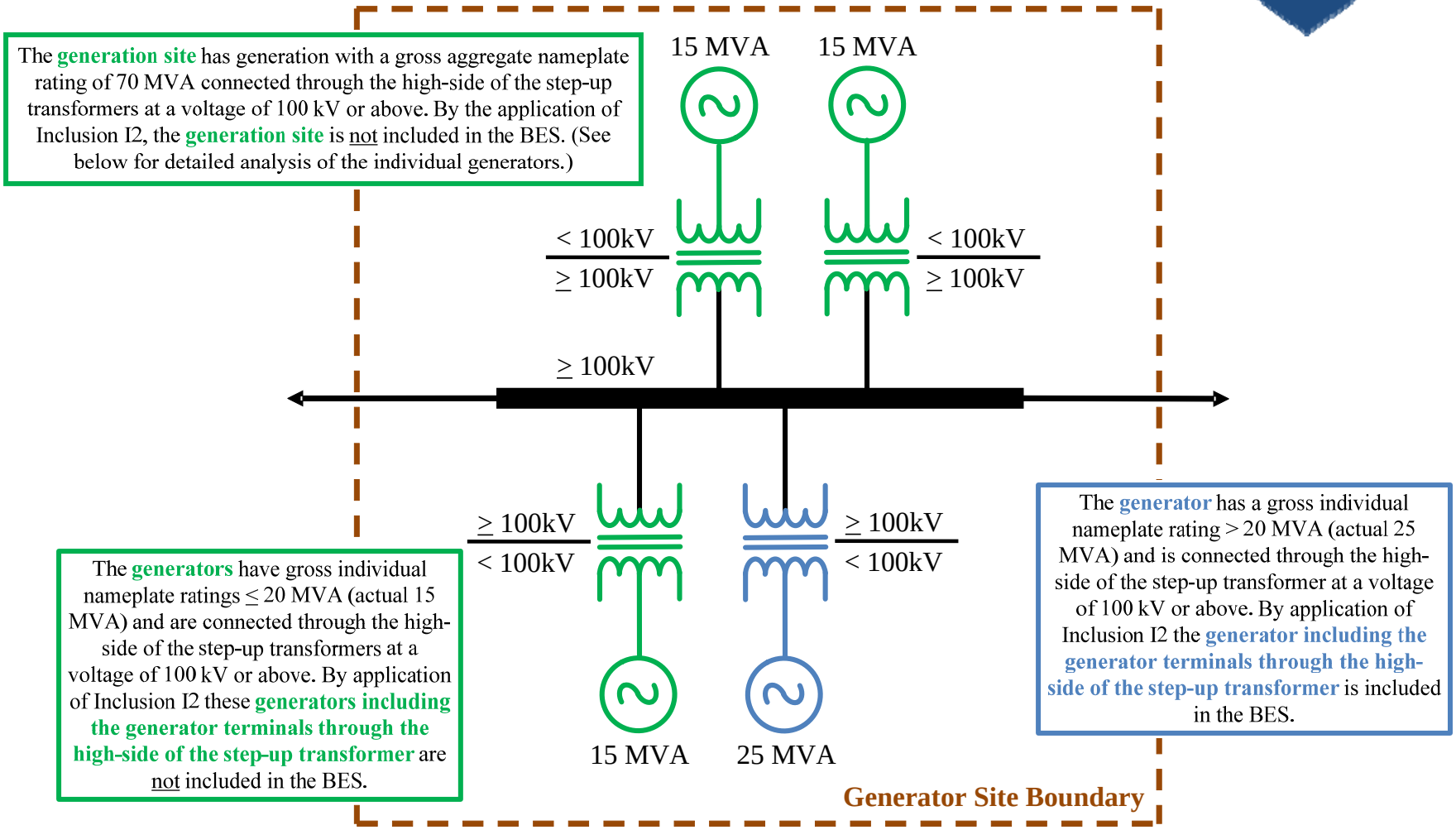
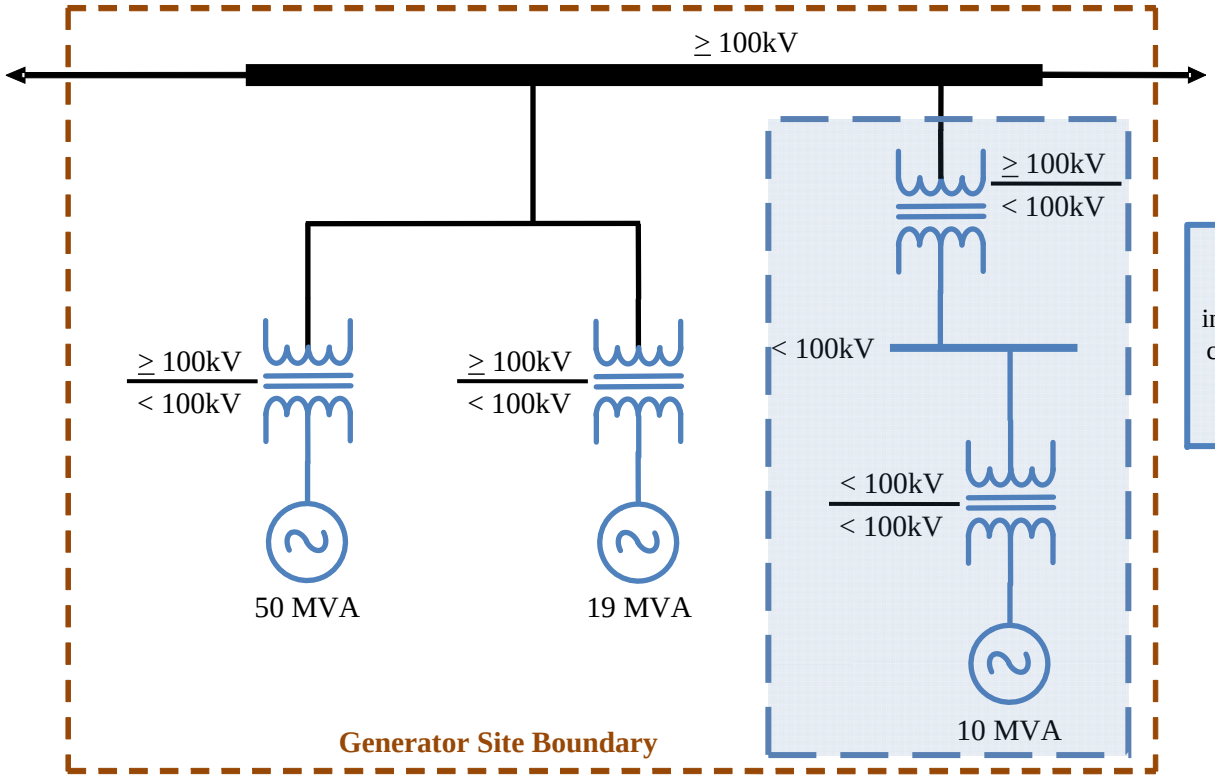


Figure I2-4: Multiple Generators at a Single Site (BES & non-BES)

Inclusion I2 – Generating Resources

The **generation site** has generation with a gross aggregate nameplate rating greater than 75 MVA (actual 79 MVA) connected through the high-side of the step-up transformers at a voltage of 100 kV or above. By the application of Inclusion I2, the **generation site** is included in the BES.

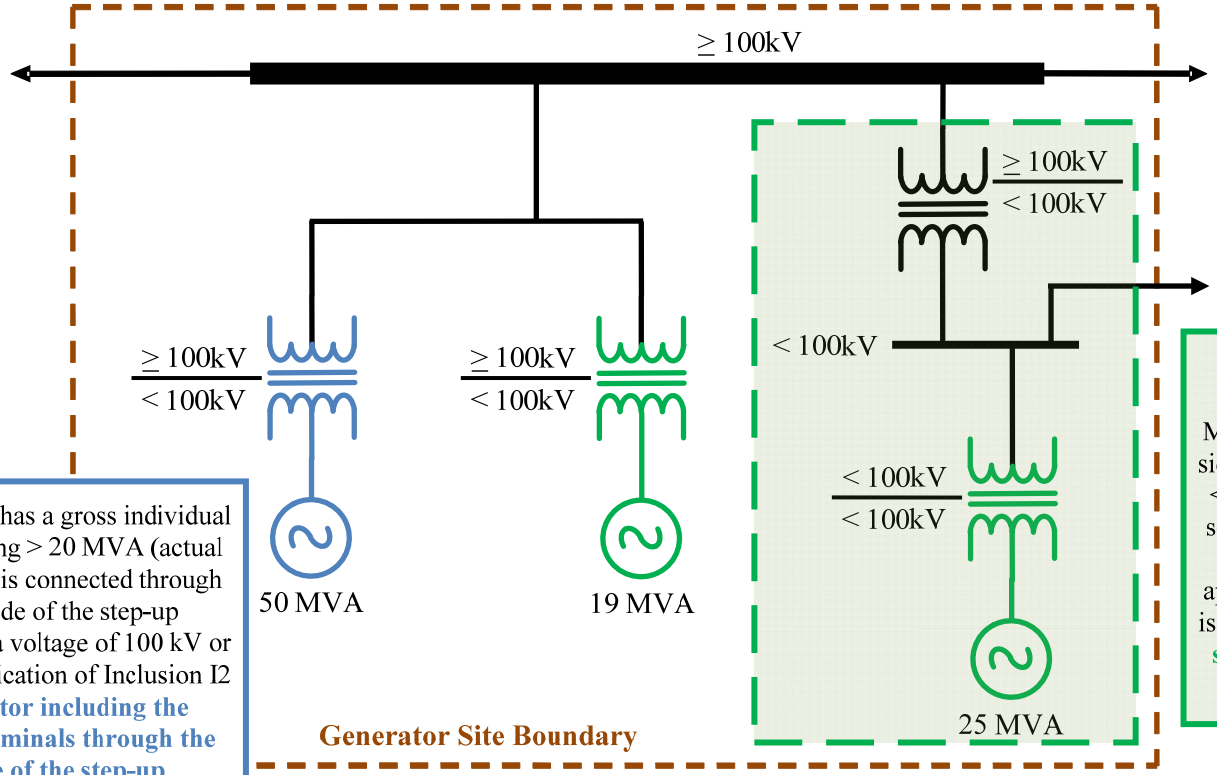


The **generator step-up transformers,** associated with the 10 MVA generator, including the interconnecting bus work are considered a BES Element. The generator contributes to the gross aggregate nameplate rating of the site.

Figure I2-5: Multiple Generators at a Single Site (BES)

Inclusion I2 – Generating Resources

The **generation site** has generation with a gross aggregate nameplate rating of less than 75 MVA (actual 69 MVA (50 + 19 MVA)) connected through the high-side of the step-up transformers at a voltage of 100 kV or above. The 25 MVA generator is not included in the gross aggregate calculation, see textbox on right. By the application of Inclusion I2, the **generation site** is not included in the BES.



The **generator** has a gross individual nameplate rating > 20 MVA (actual 50 MVA) and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 this **generator including the generator terminals through the high-side of the step-up transformer** is included in the BES.

The **generator** has a gross individual nameplate rating > 20 MVA (actual 25 MVA) and is connected through the high-side of the step-up transformer at a voltage < 100 kV. The interconnecting bus work serves Load and provides a connection to sub-100 kV Facilities, therefore by application of Inclusion I2, the **generator** is connected **through the high-side of the step-up transformer** at a voltage < 100 kV and is not included in the BES.

Figure I2-6: Multiple Generators at a Single Site (BES & non-BES)

INCLUSIONS I4

Inclusion I4 – Dispersed Power Producing Resources

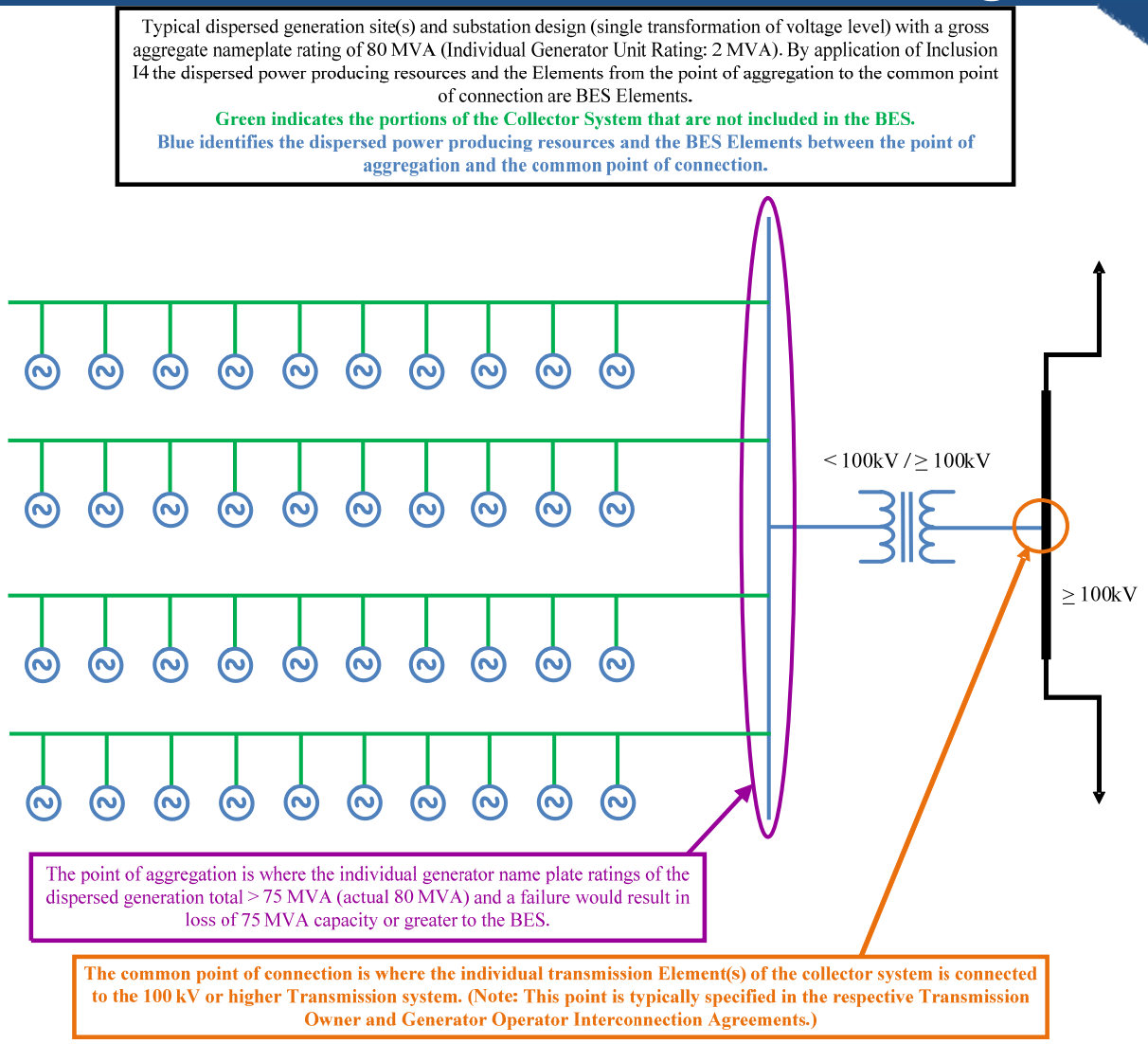


Figure I4-1 Dispersed Generation Site (Single Voltage Transformation) – Wind Farm

Inclusion I4 – Dispersed Power Producing Resources

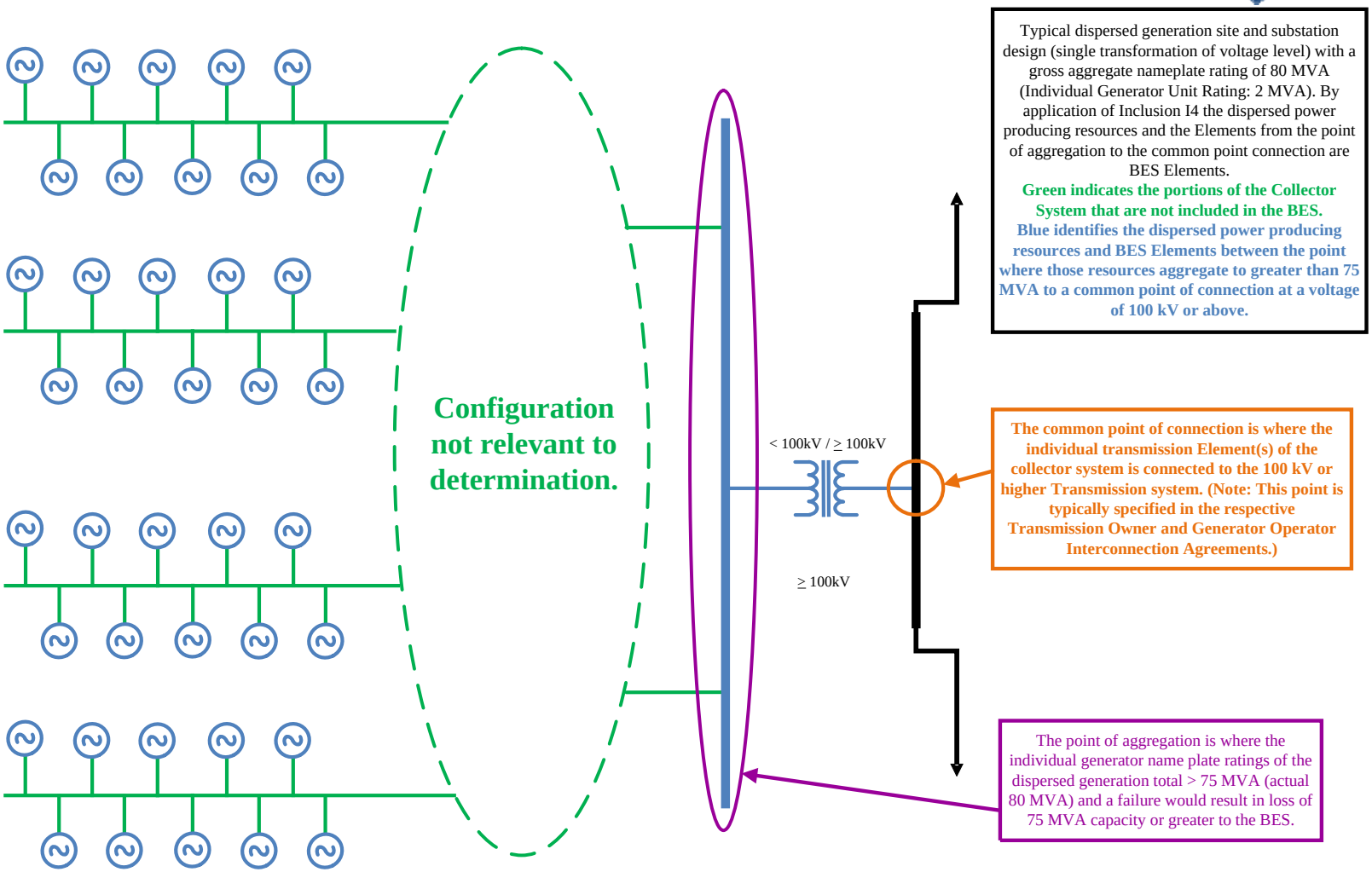


Figure I4-2 Dispersed Generation Site (Unknown Collector System Configuration) – Wind Farm

Inclusion I4 – Dispersed Power Producing Resources

Dispersed generation site and substation design (single transformation of voltage level) with a gross aggregate nameplate rating of 80 MVA (Individual Photovoltaic Bank Rating: 20 MVA). By application of Inclusion I4 the Photovoltaic Cells & Inverters (generators) are included in the BES.

Green indicates the portions of the Collector System that are not included in the BES.

Blue identifies BES dispersed power producing resources (Photovoltaic Cells & Inverters) and the BES Elements between the point of aggregation and the common point of connection.

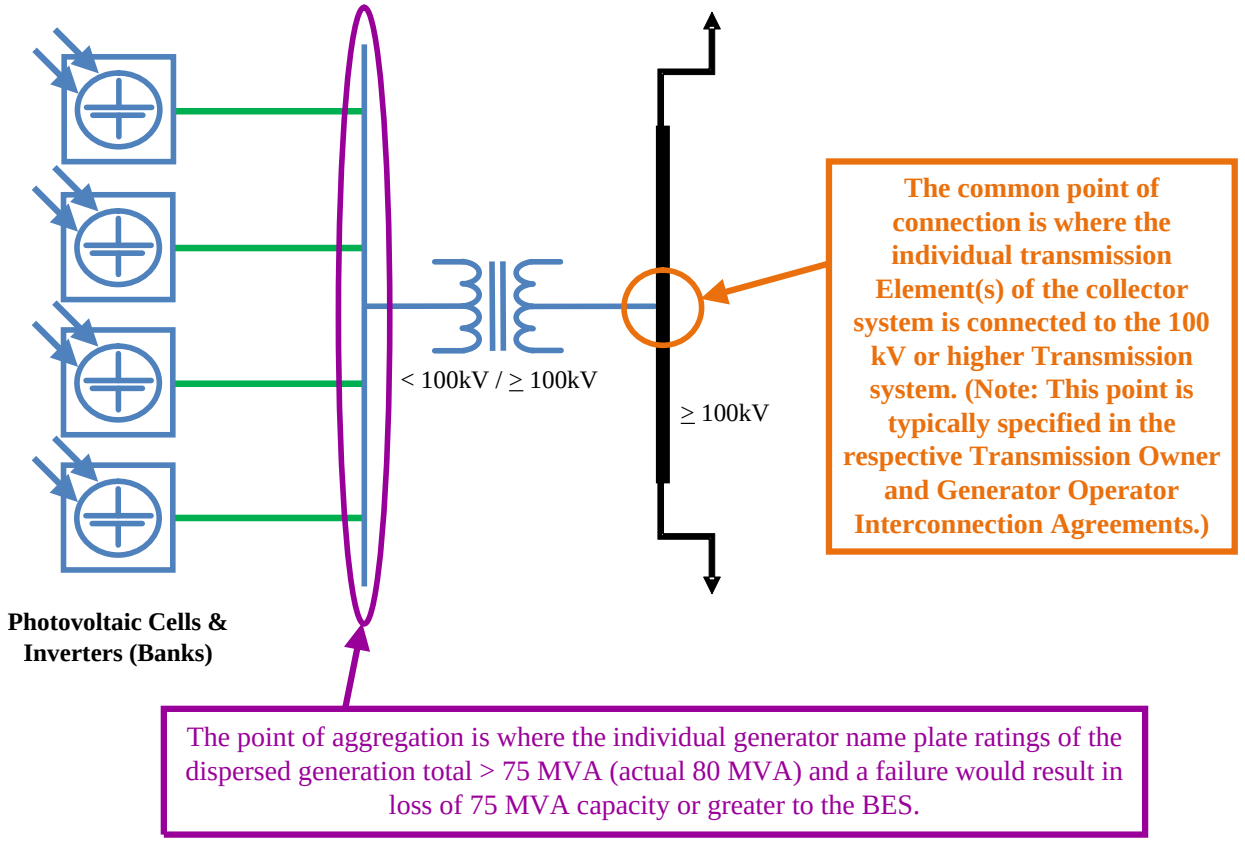


Figure I4-3 Dispersed Generation Site (Single Voltage Transformation) – Solar Array

Inclusion I4 – Dispersed Power Producing Resources

Dispersed generation site and substation design (multiple transformations of voltage level) with a gross aggregate nameplate rating of 80 MVA (Individual Photovoltaic Bank Rating: 20 MVA). By application of Inclusion I4 the Photovoltaic Cells & Inverters (generator units) are included in the BES.

Green indicates the portions of the Collector System that are not included in the BES.

Blue identifies BES dispersed power producing resources (Photovoltaic Cells & Inverters) and the BES Elements between the point of aggregation and the common point of connection.

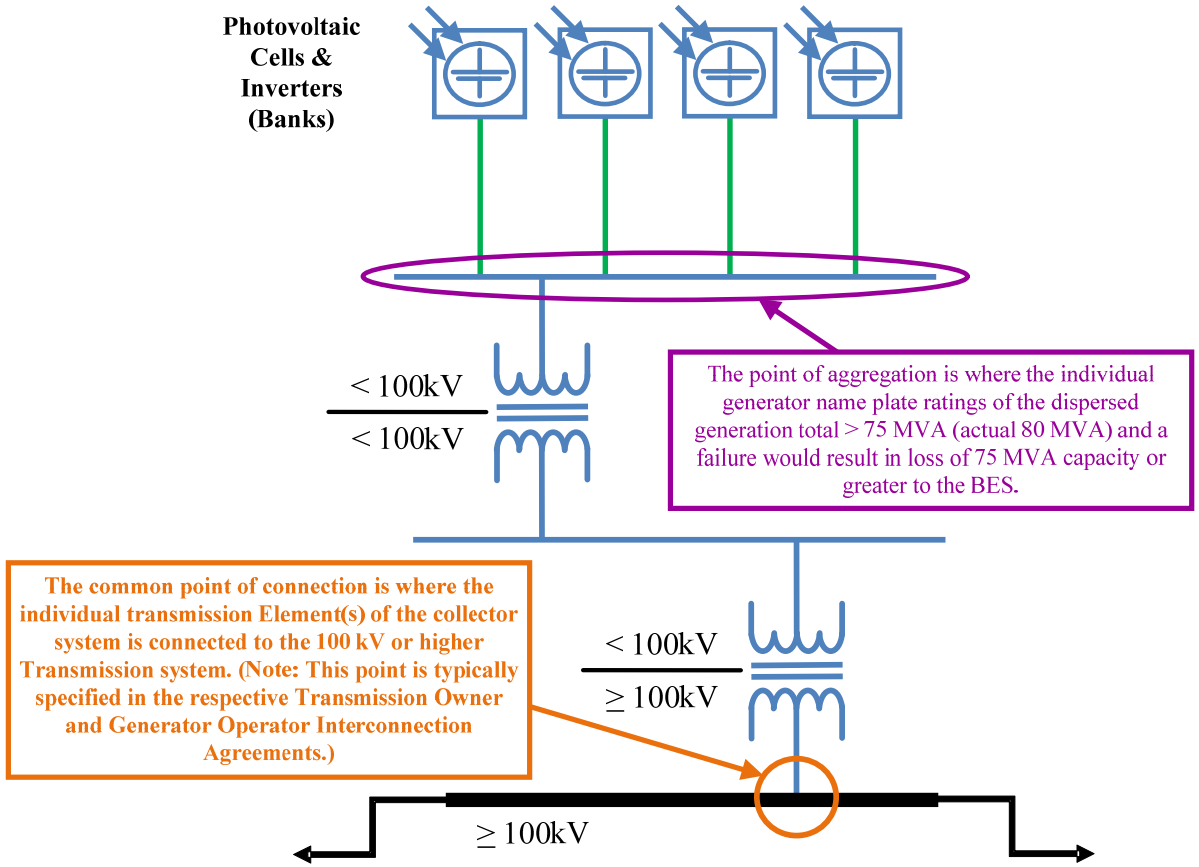


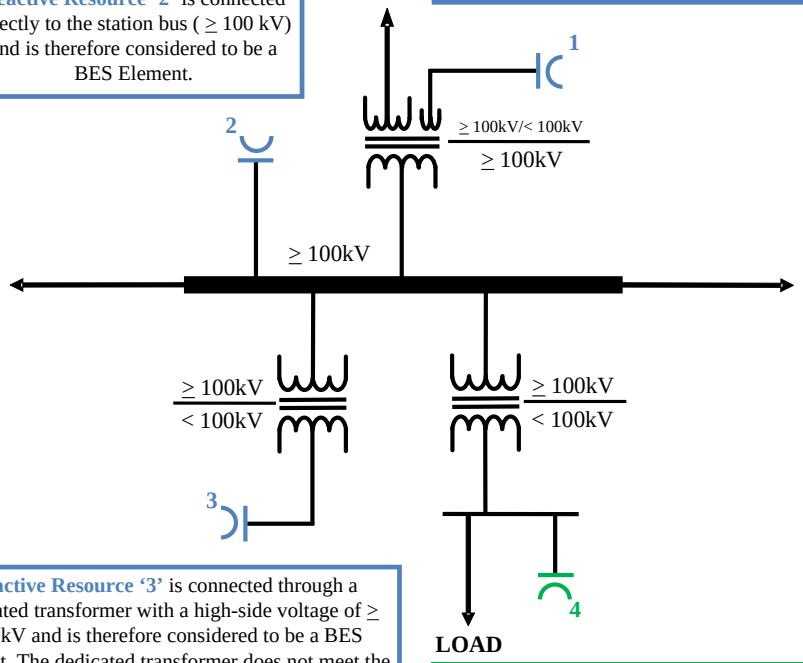
Figure I4-4 Dispersed Generation Site (Multiple Voltage Transformations) – Solar Array

INCLUSIONS I5

Inclusion I5 – Reactive Power Devices

Reactive Resource '1' is connected through the tertiary winding of a transformer that meets the inclusion criteria established by Inclusion I5 (i.e., through a transformer that is designated in Inclusion I1) and is therefore considered to be a BES Element.

Reactive Resource '2' is connected directly to the station bus (≥ 100 kV) and is therefore considered to be a BES Element.



Reactive Resource '3' is connected through a dedicated transformer with a high-side voltage of ≥ 100 kV and is therefore considered to be a BES Element. The dedicated transformer does not meet the inclusion criteria established by Inclusion I1 and is therefore not considered to be a BES Element.

Reactive Resource '4' is connected directly to the station bus (< 100 kV), and is not connected through a dedicated transformer with a high-side voltage of 100 kV or higher or through a transformer that is designated in Inclusion I1, and is therefore not considered to be a BES Element.

EXCLUSIONS
E1

Exclusion E1 Radial Systems
E1.a Serves Load Only

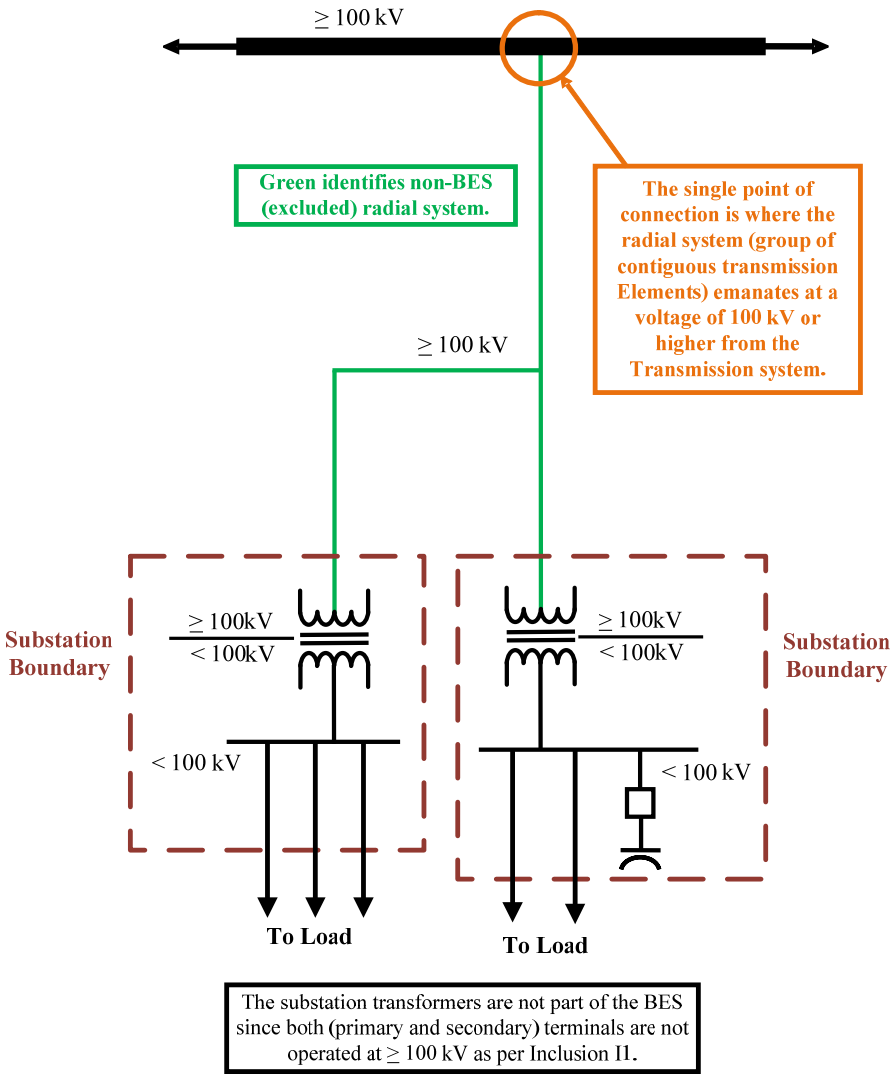


Figure E1-1: Radial System: Serving Only Load

Exclusion E1 Radial Systems
E1.a Serves Load Only

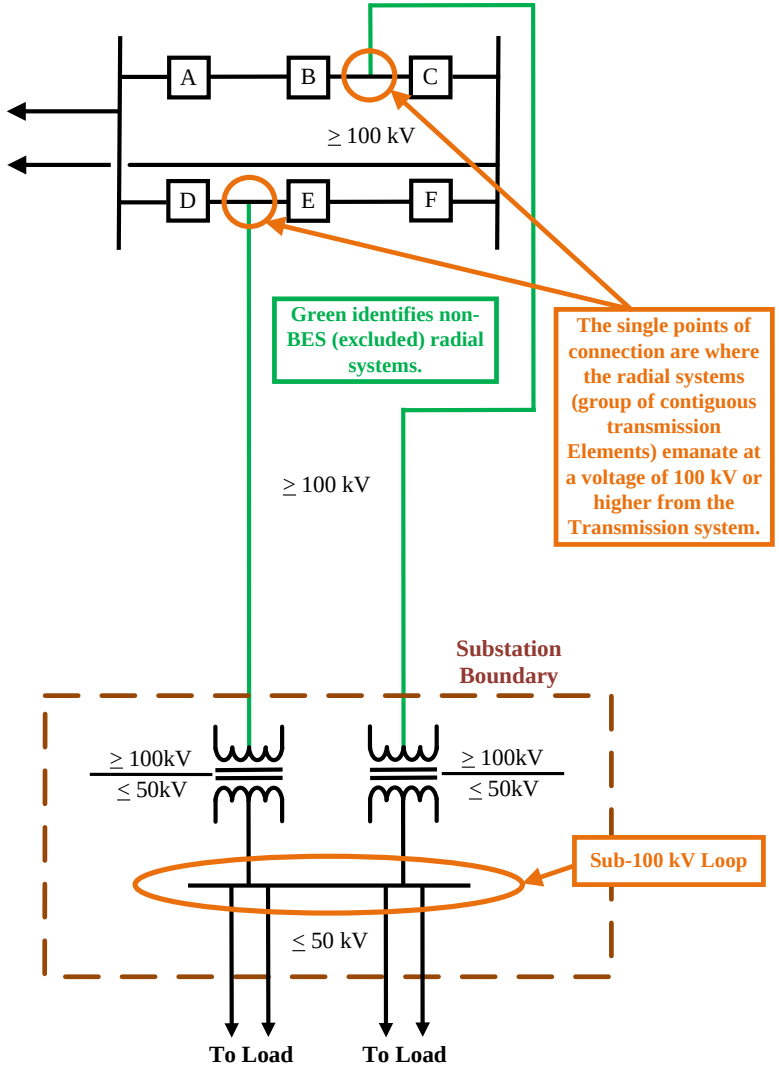


Figure E1-2: Multiple Radial Systems (Underlying Loop Facilities < 50 kV)

Exclusion E1 Radial Systems
E1.a Serves Load Only

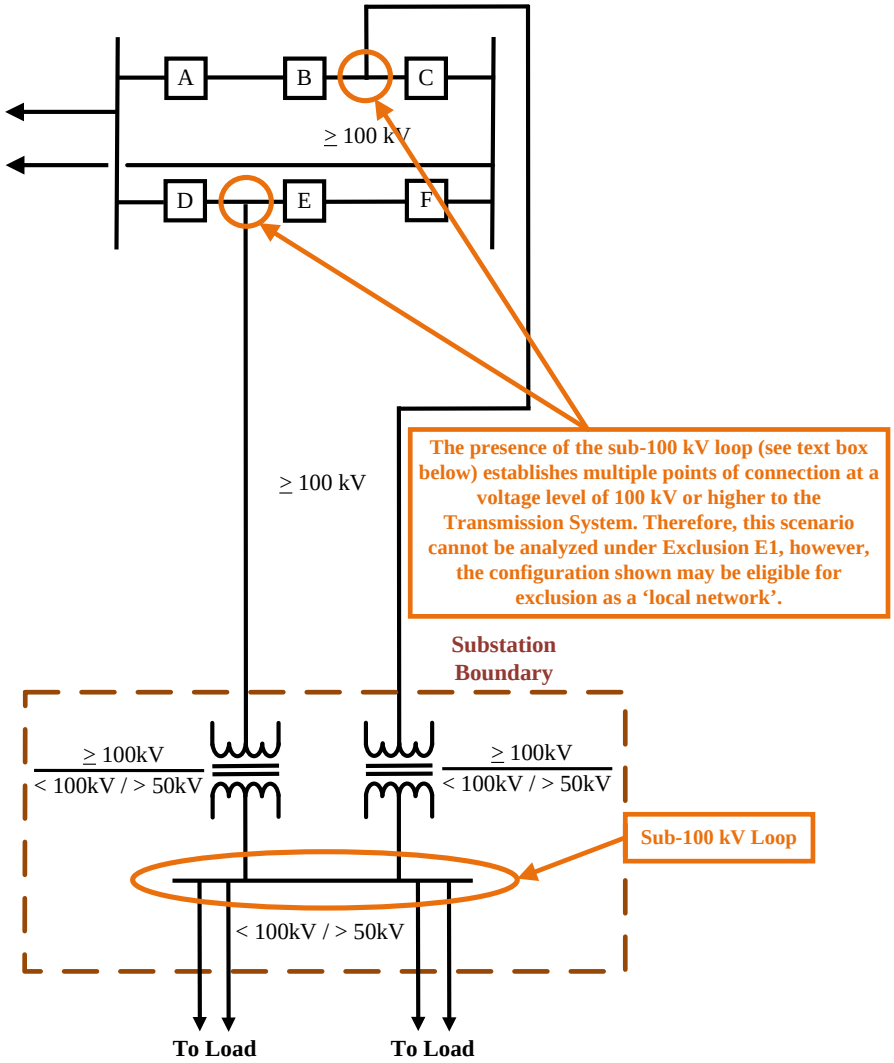


Figure E1-3: Impact of Sub-100 kV Looped Facilities

Exclusion E1 Radial Systems
E1.b Generation Only

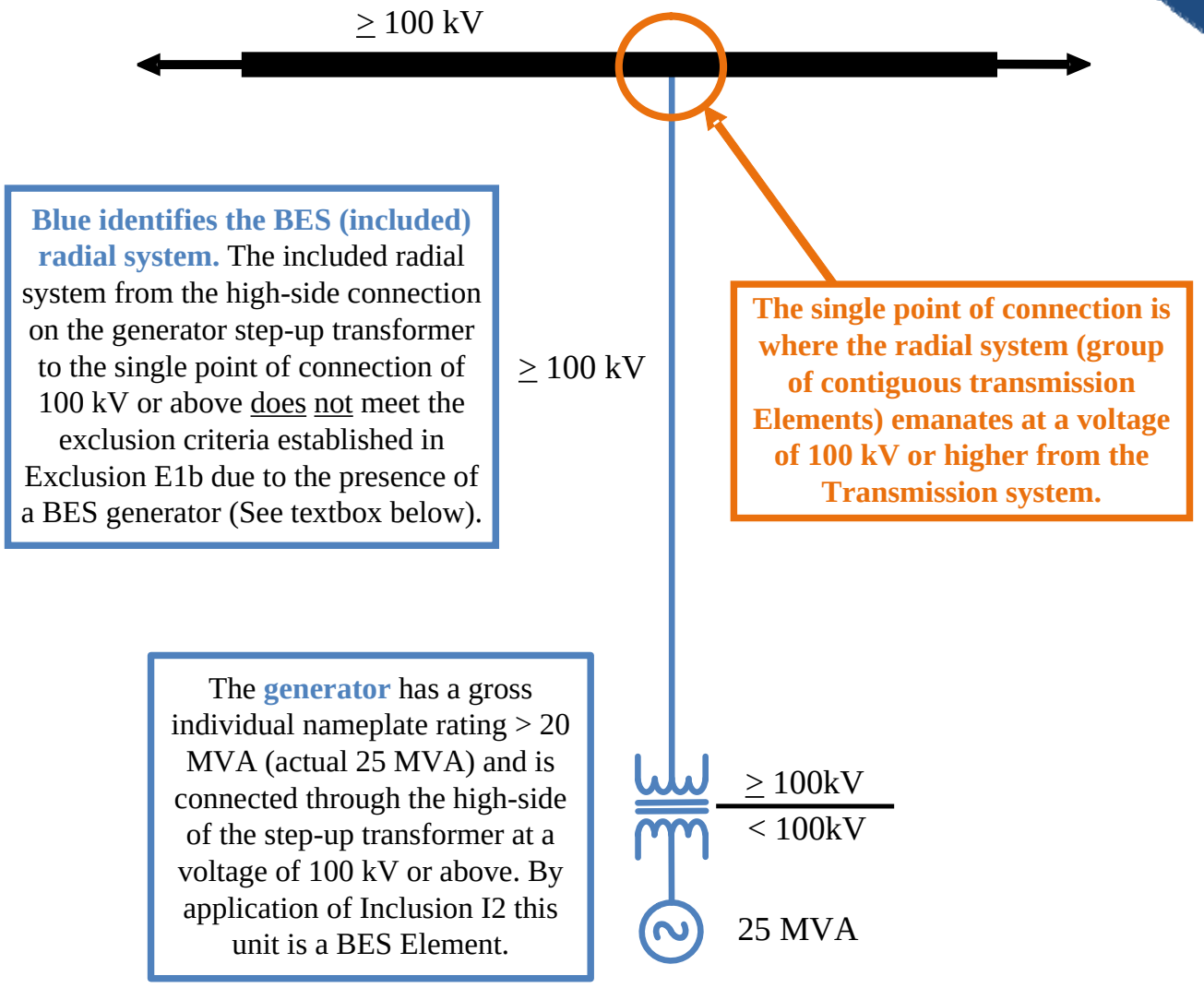


Figure E1-4: Radial System: Single BES Generation Resource

Exclusion E1 Radial Systems
E1.b Generation Only

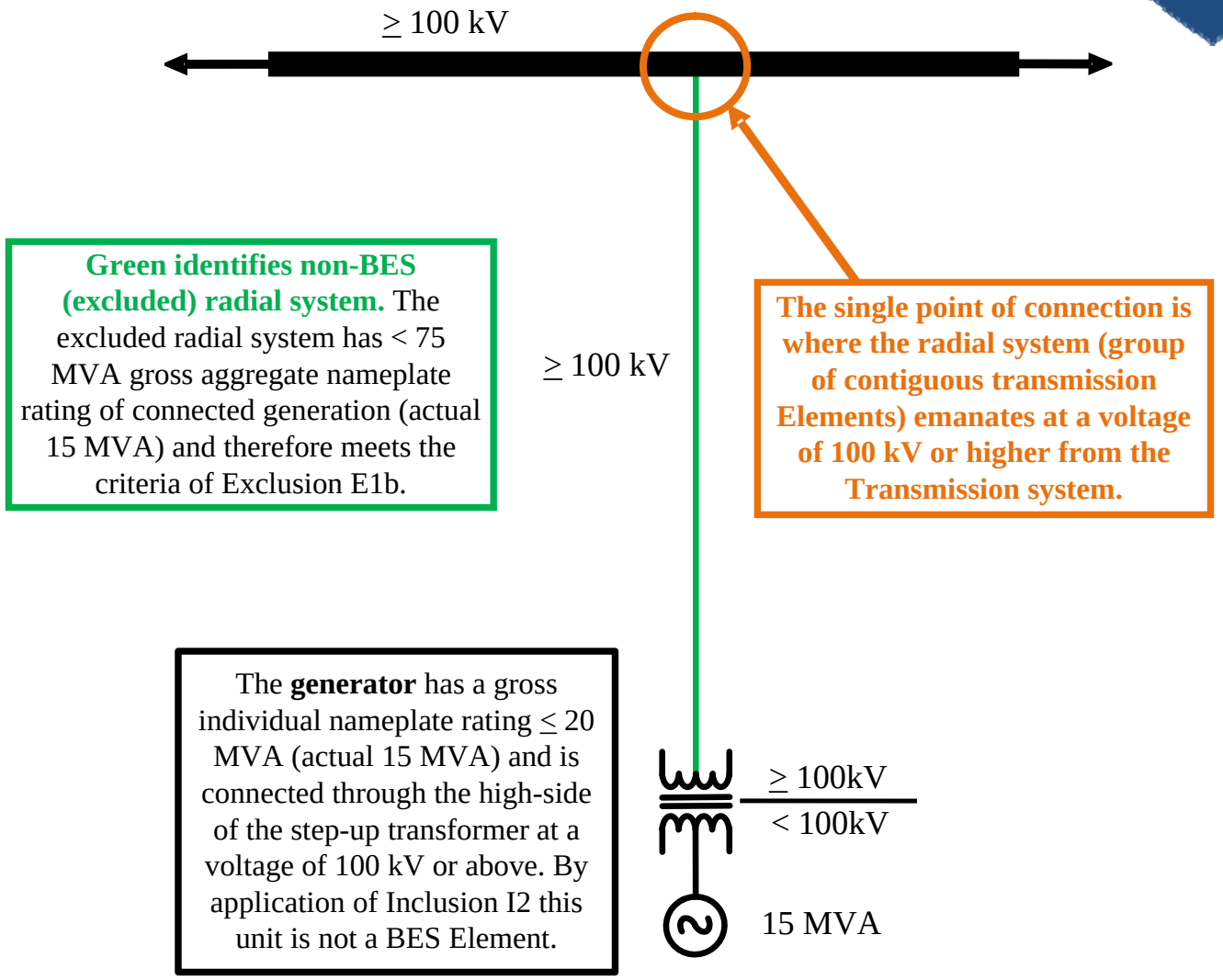


Figure E1-5: Radial System: Single non-BES Generation Resource

Exclusion E1 Radial Systems
E1.b Generation Only

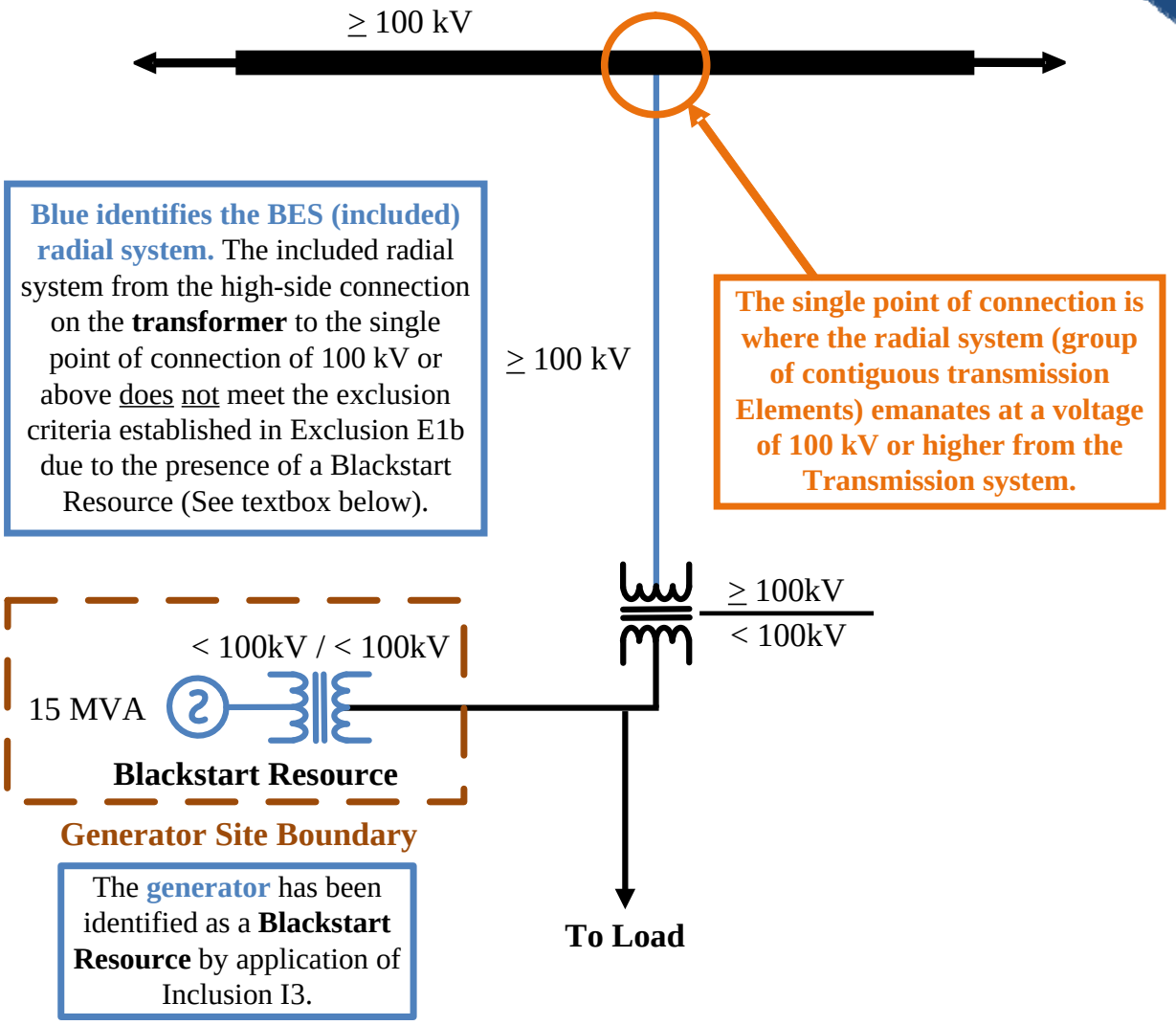


Figure E1-6: Radial System: Blackstart Resource

Exclusion E1 Radial Systems
E1.b Generation Only

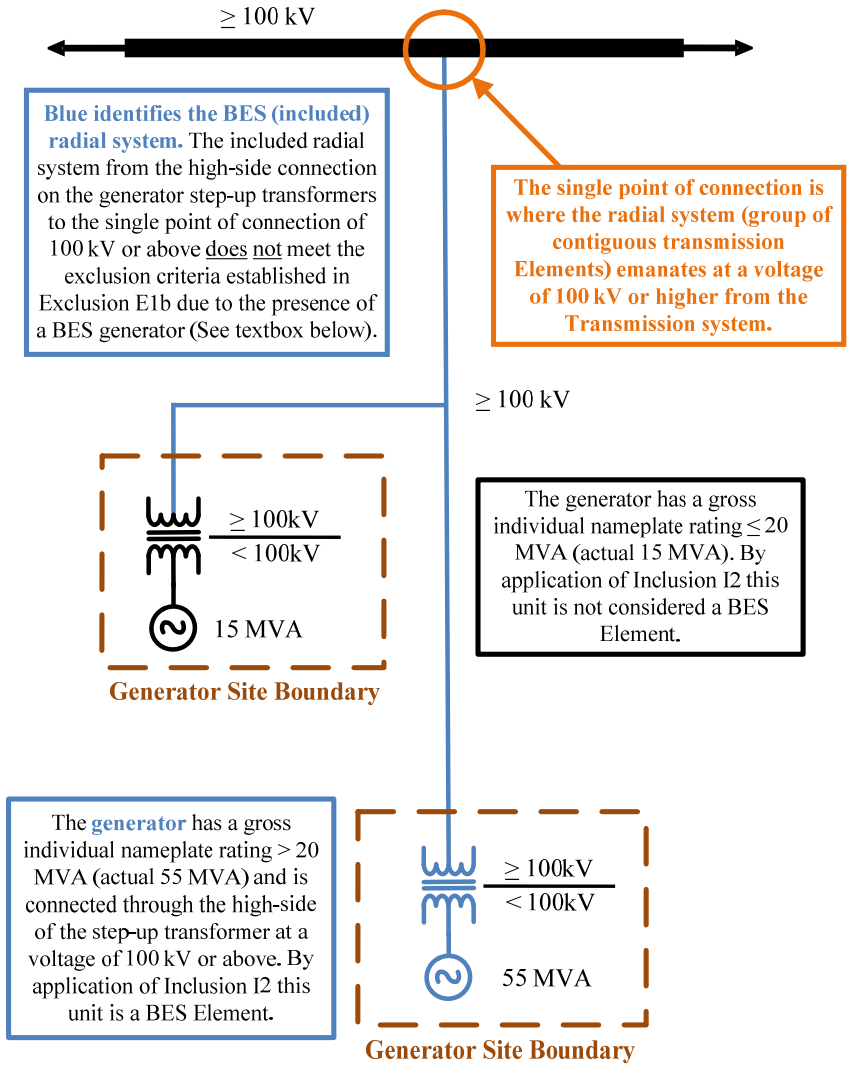


Figure E1-7: Radial System: Multiple (BES & non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.b Generation Only

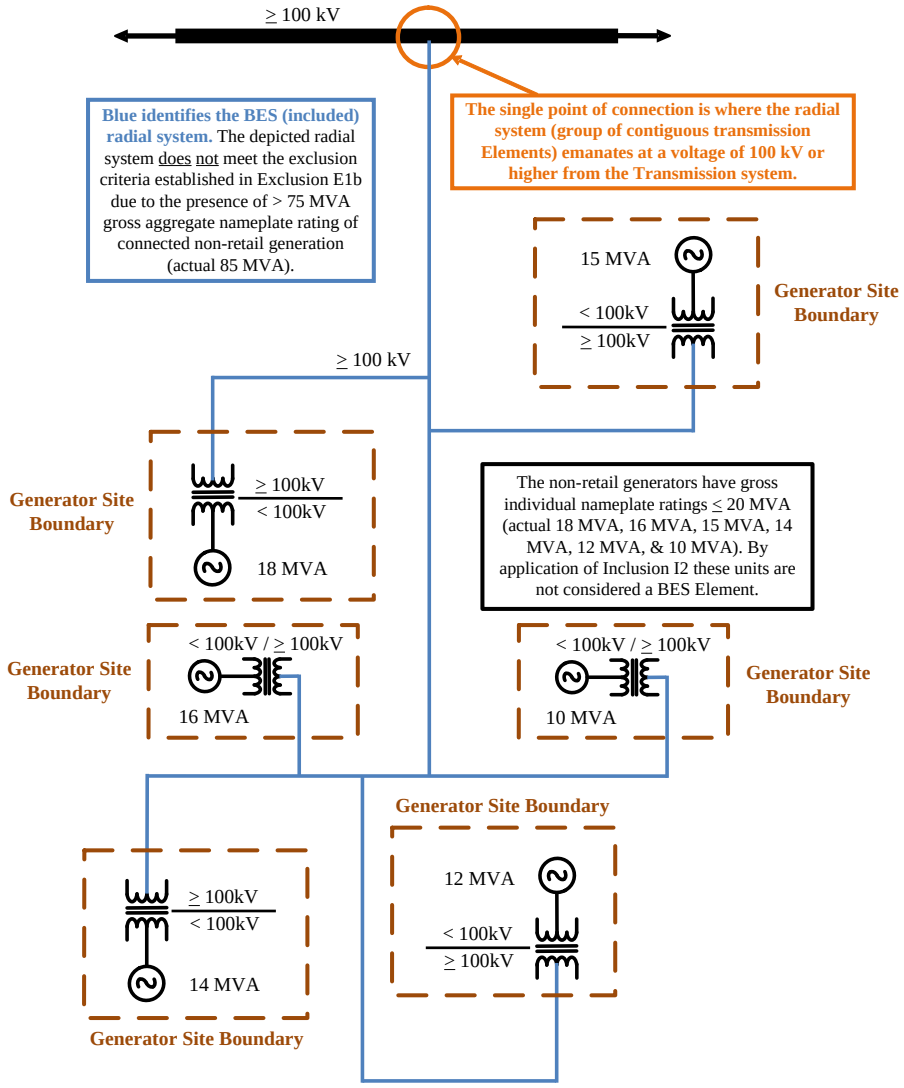


Figure E1-8: Radial System: Multiple (non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.b Generation Only

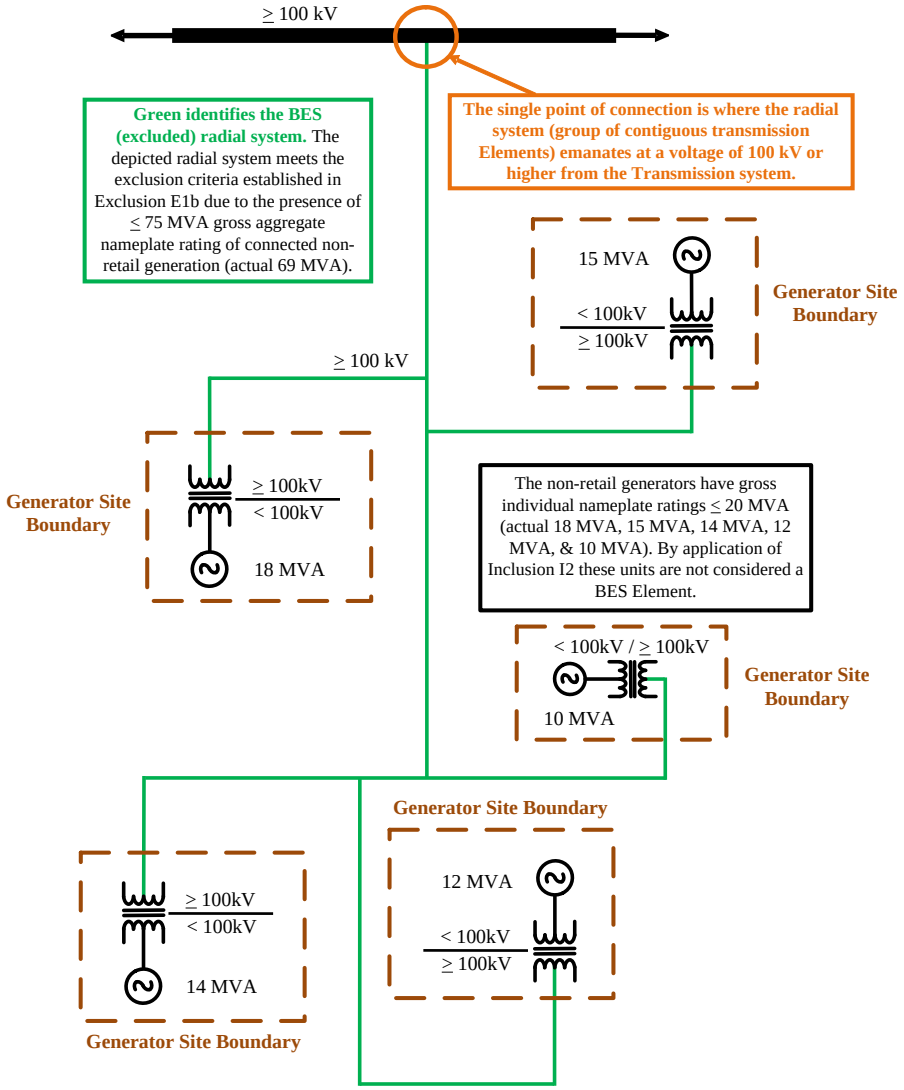


Figure E1-9: Radial System: Multiple (non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

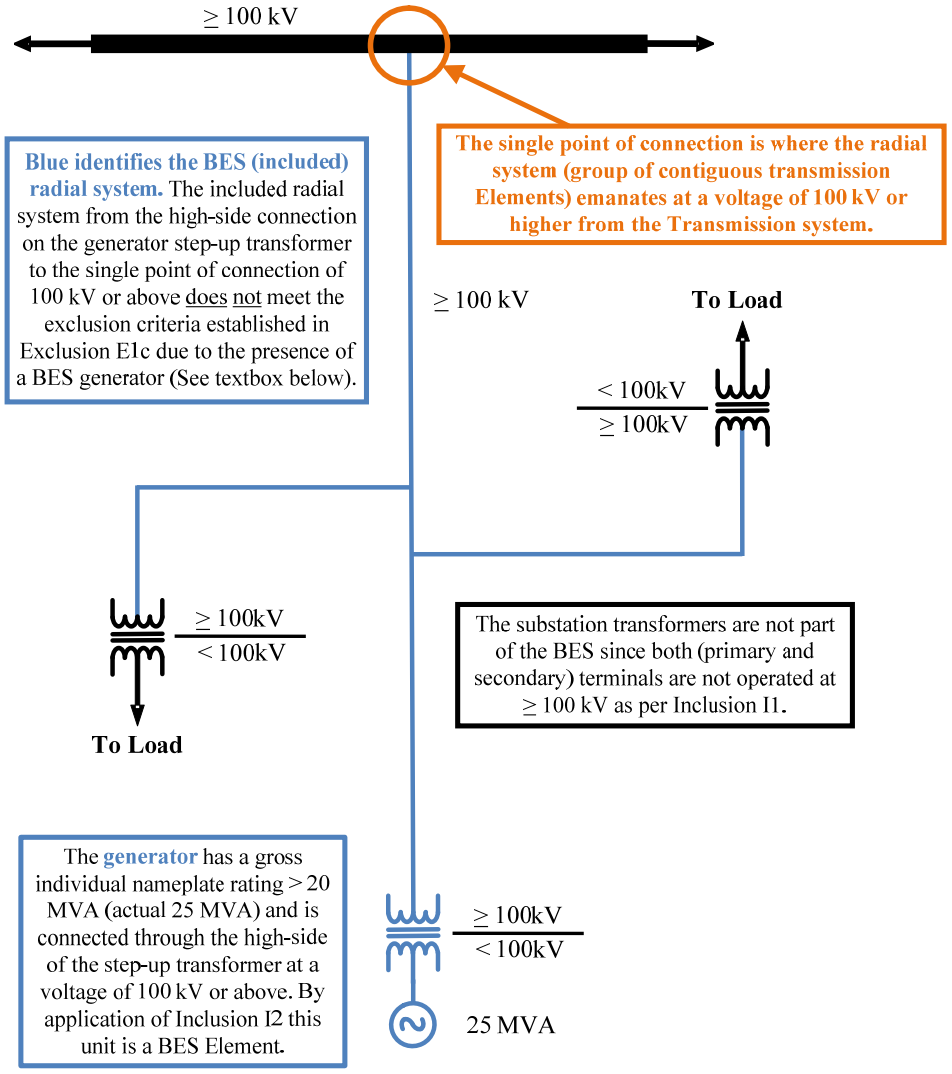


Figure E1-11: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

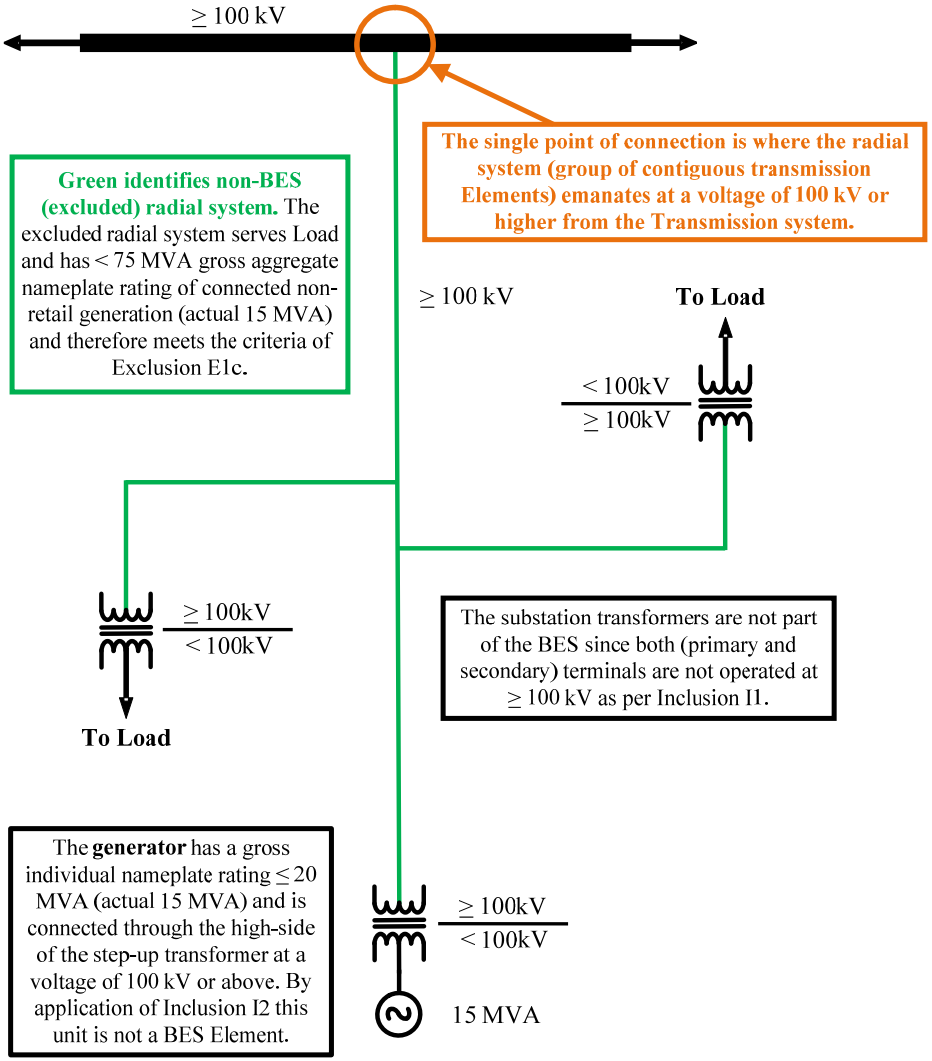


Figure E1-12: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

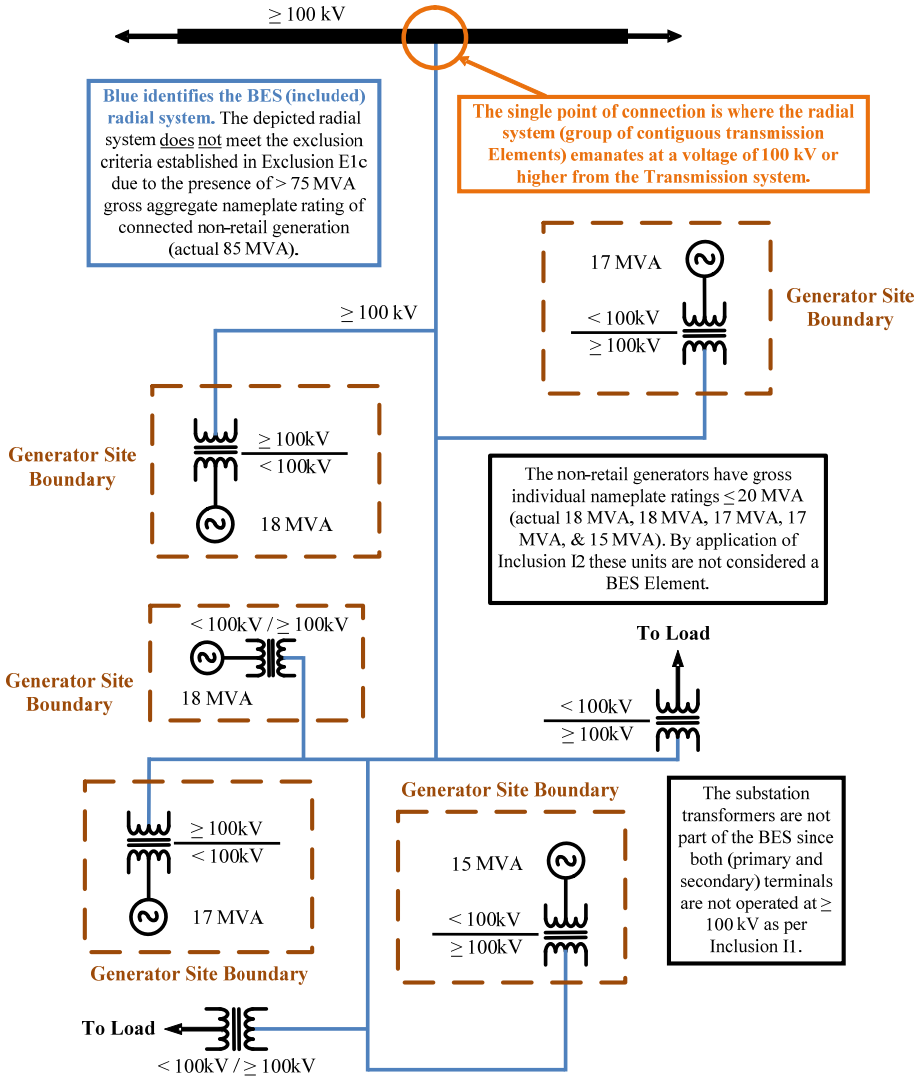


Figure E1-13: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

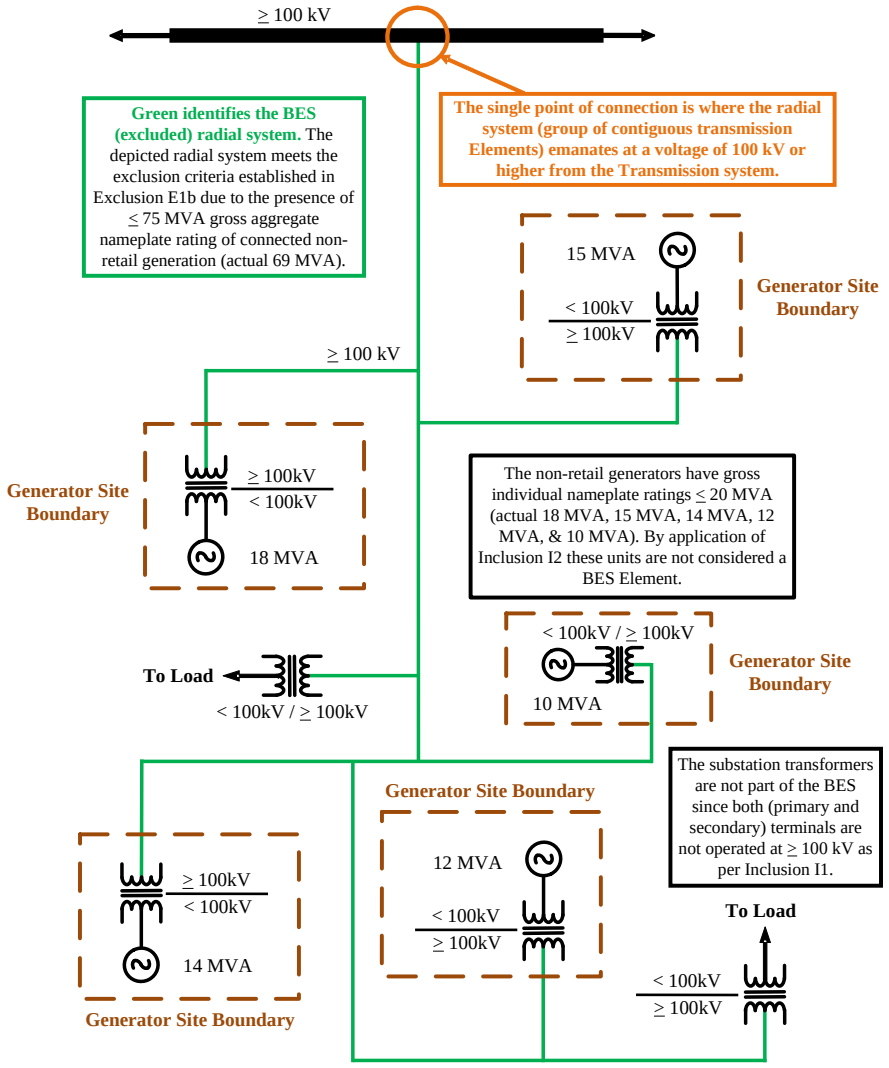


Figure E1-14: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

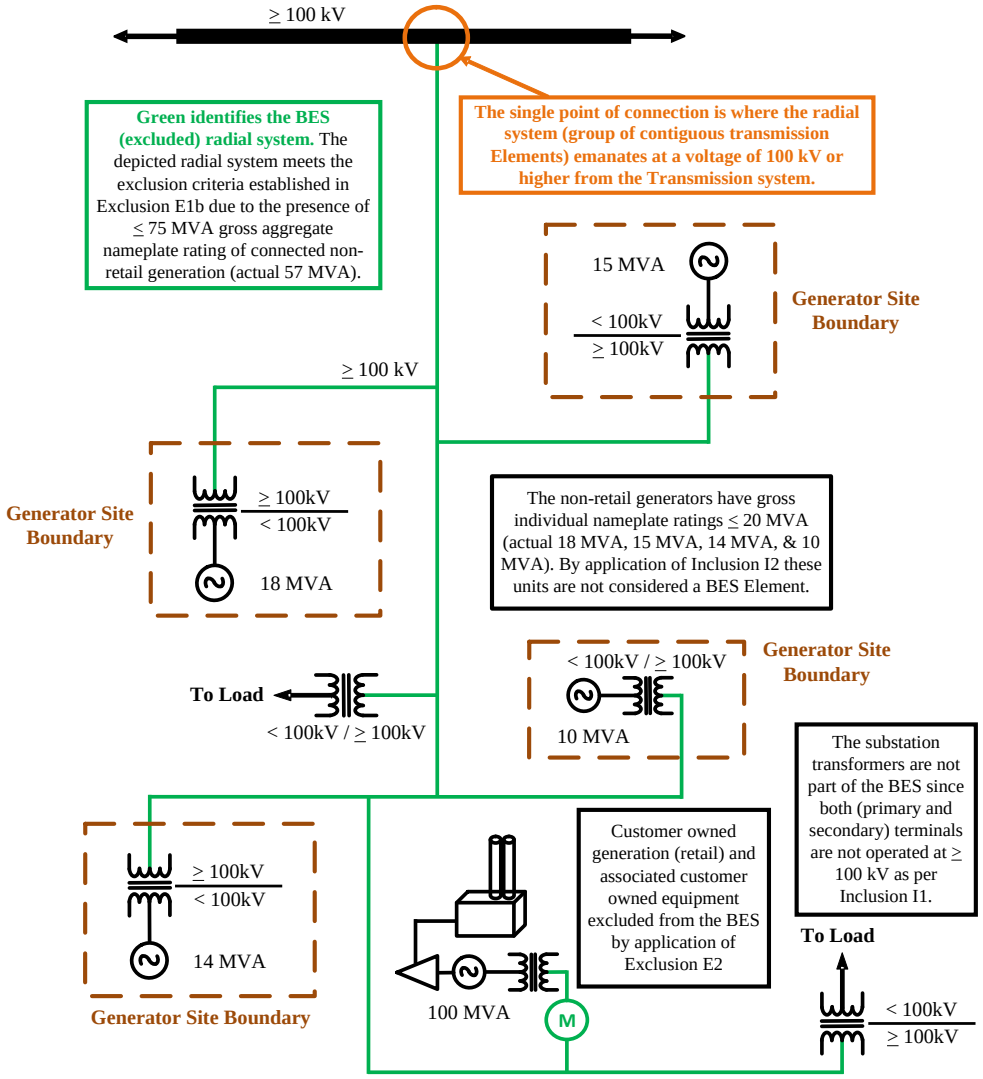


Figure E1-15: Radial System: Generation Resource (Retail & Non-Retail) & Serving Load

Exclusion E1 Radial Systems Normally OPEN Switching Device

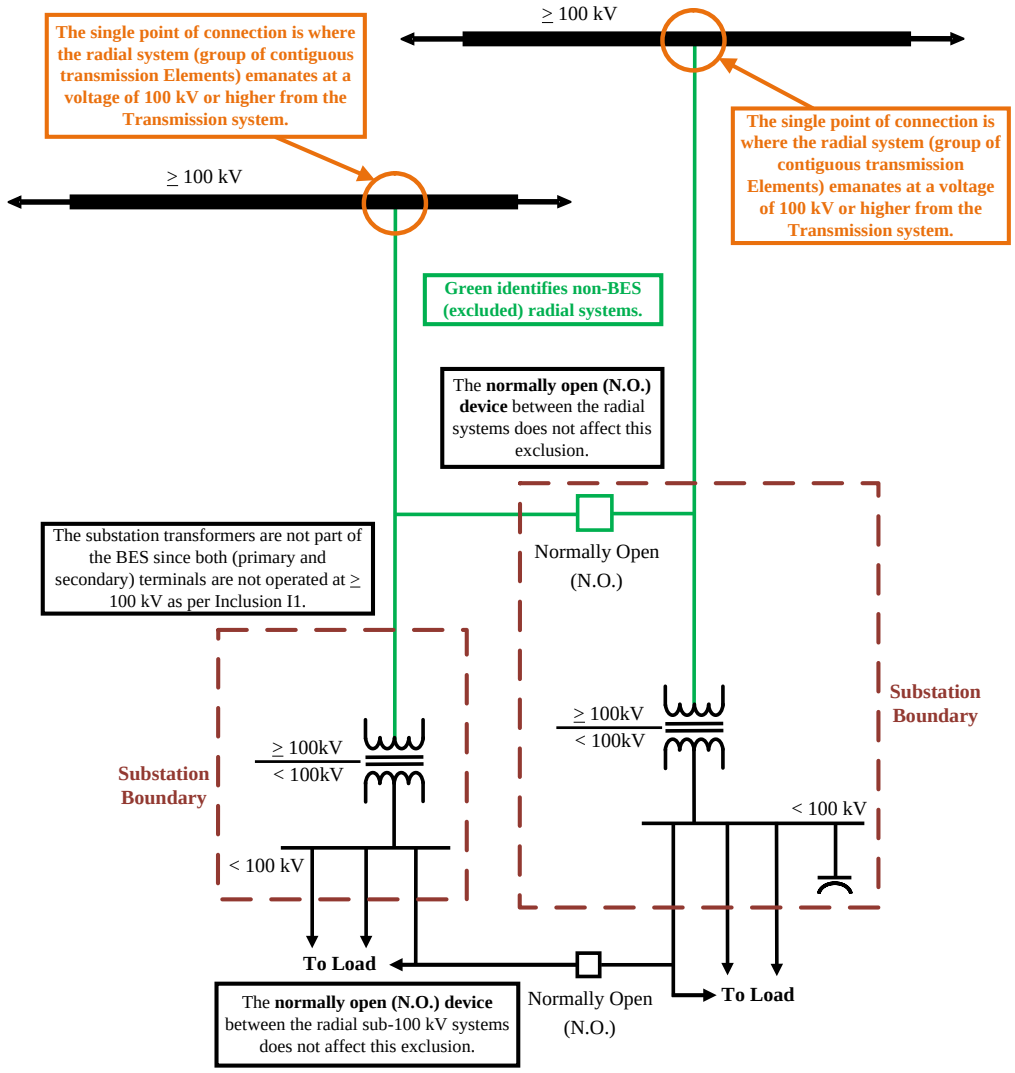


Figure E1-16: Radial System: Normally Open Switching Device between Load Serving Radial Systems

Exclusion E1 Radial Systems Underlying Loops

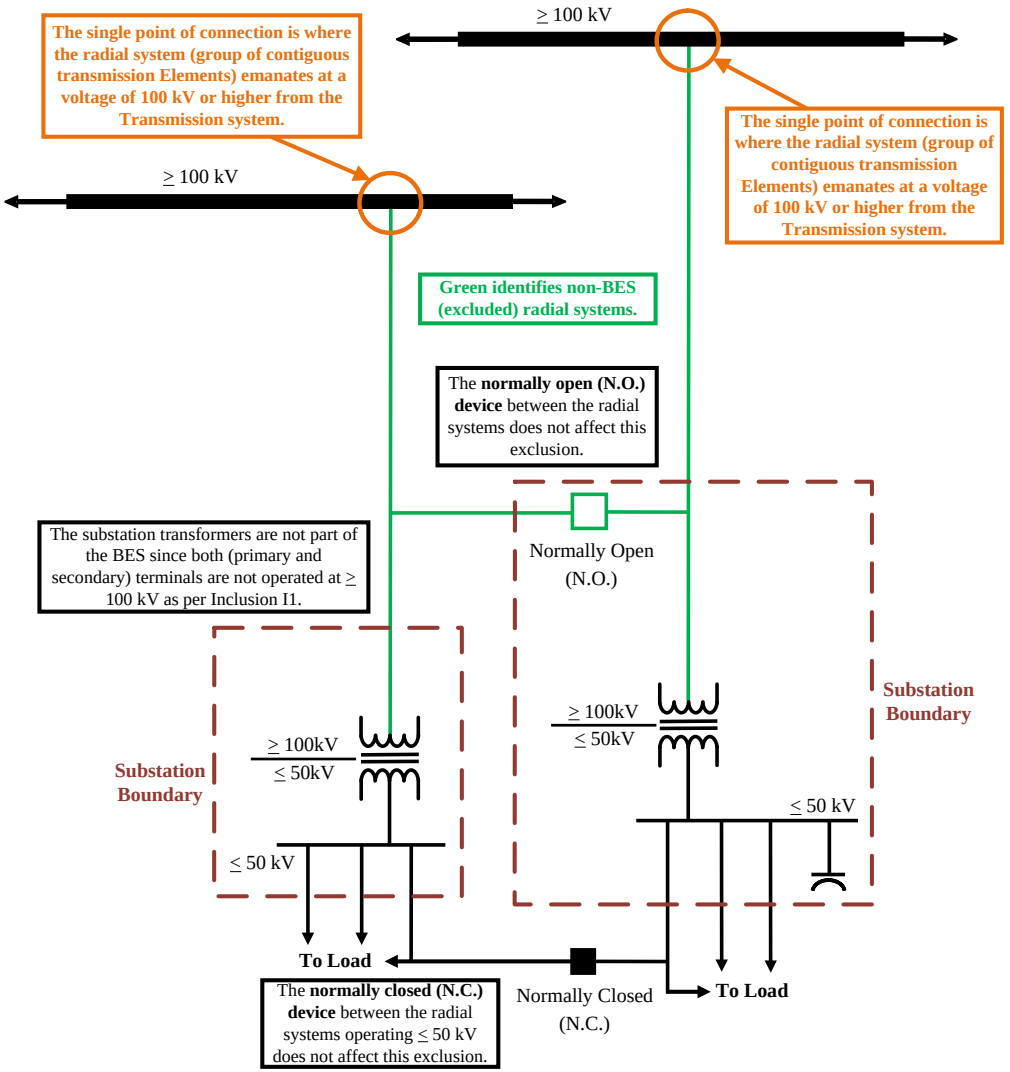


Figure E1-17: Radial System: Normally Open Switching Device between Load Serving Radial Systems with a < 50 kV Loop

Exclusion E1 Radial Systems Underlying Loops

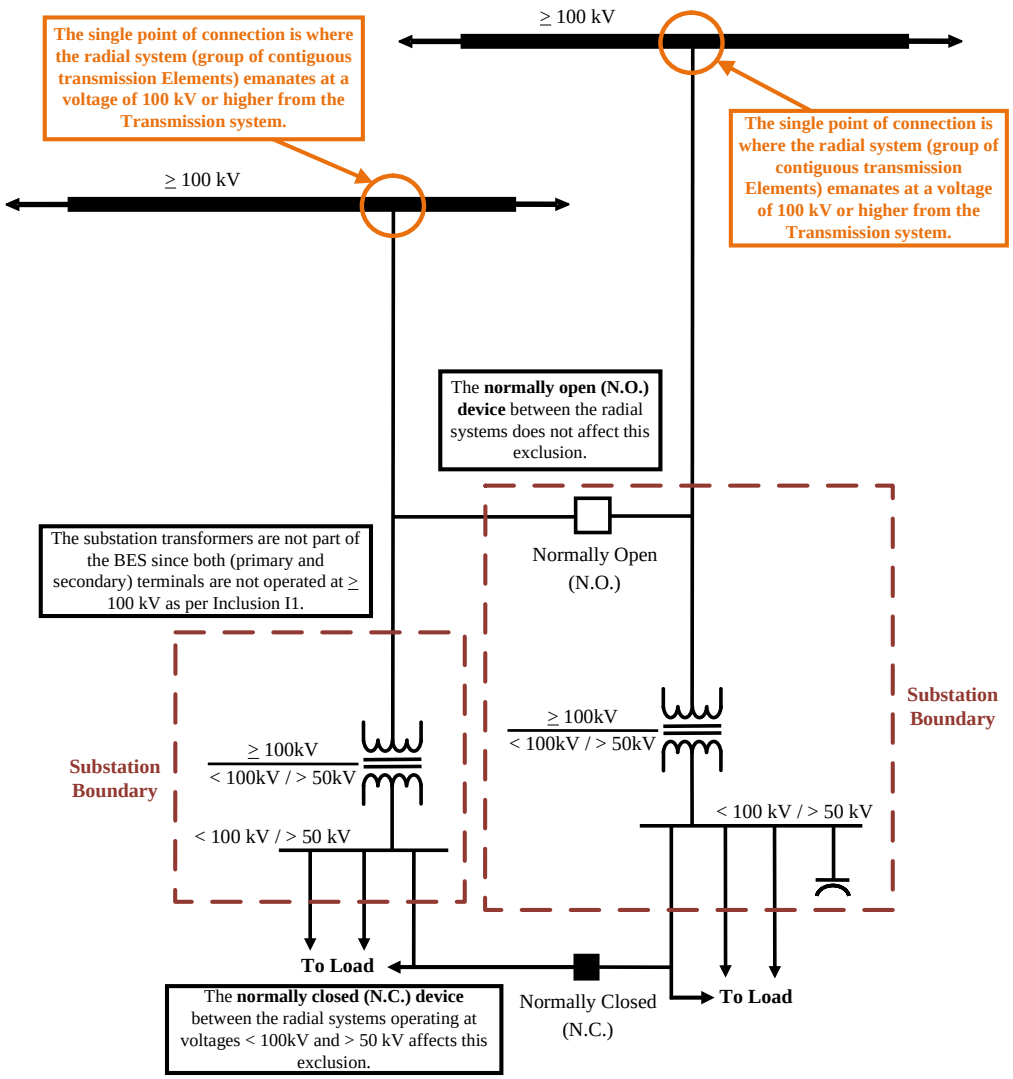


Figure E1-18: Impact of Sub-100 kV Looped Facilities (Switching Devices Identified N.O. > 100 kV & N.C. < 100 kV & > 50 kV)

Exclusion E1 Radial Systems Underlying Loops

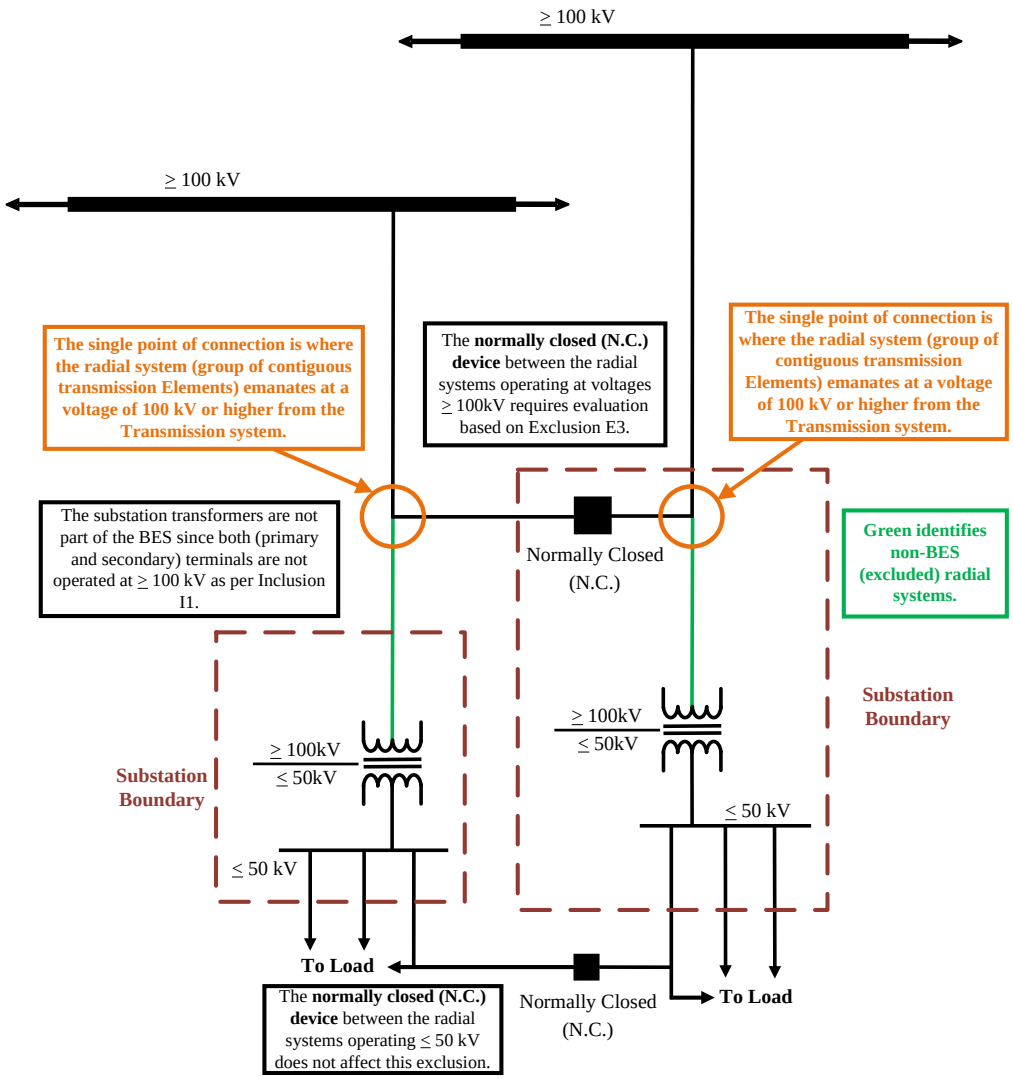


Figure E1-19: Radial System: Normally Closed Switching Device (> 100 kV) between Load Serving Radial Systems with a < 50 kV Loop

Exclusion E1 Radial Systems Underlying Loops

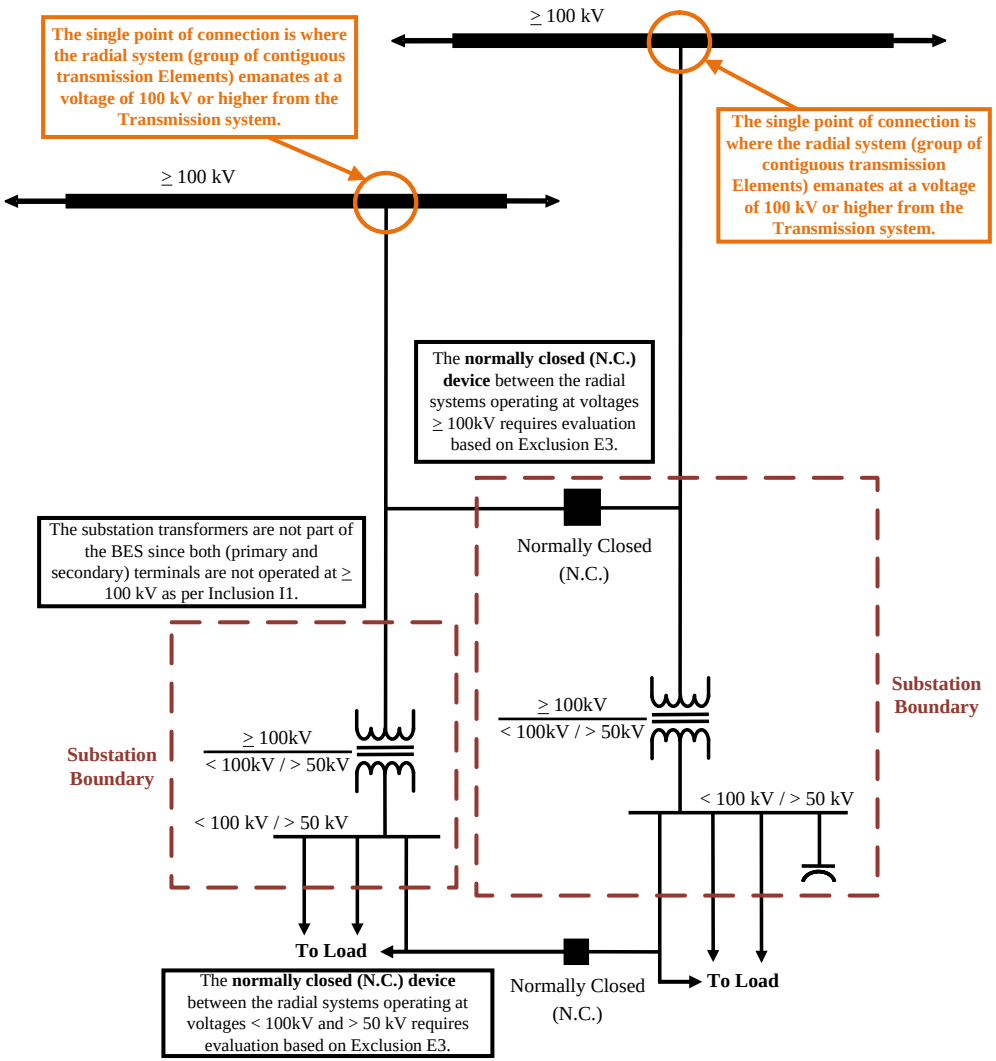


Figure E1-20: Impact of Sub-100 kV Looped Facilities (Switching Devices Identified N.C. > 100 kV & N.C. < 100 kV & > 50 kV)

EXCLUSIONS
E2

Exclusion E2 Behind-the-Meter Industrial Generation

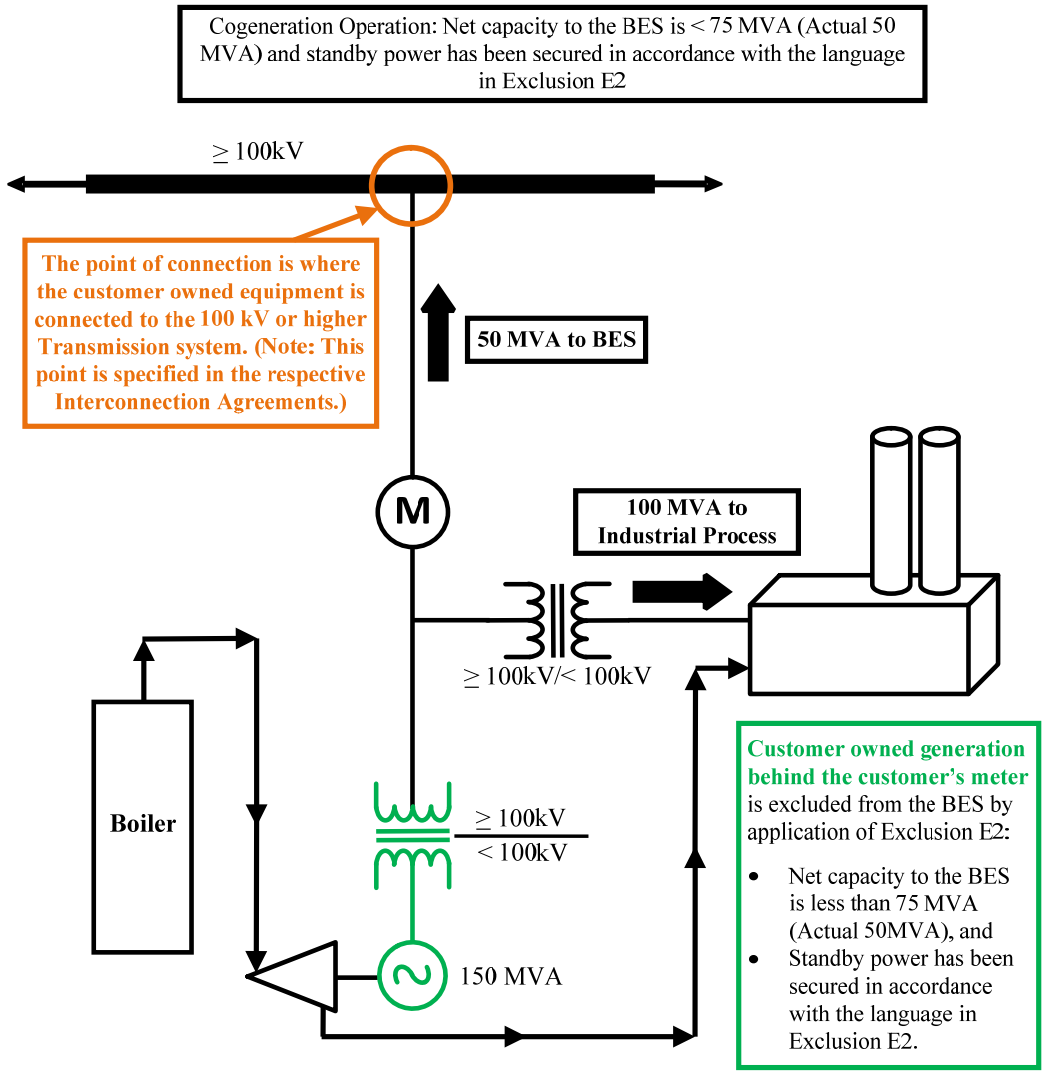


Figure E2-1: Behind-the-Meter Generation: Net Capacity to the BES Less Than 75 MVA

Exclusion E2 Behind-the-Meter Industrial Generation

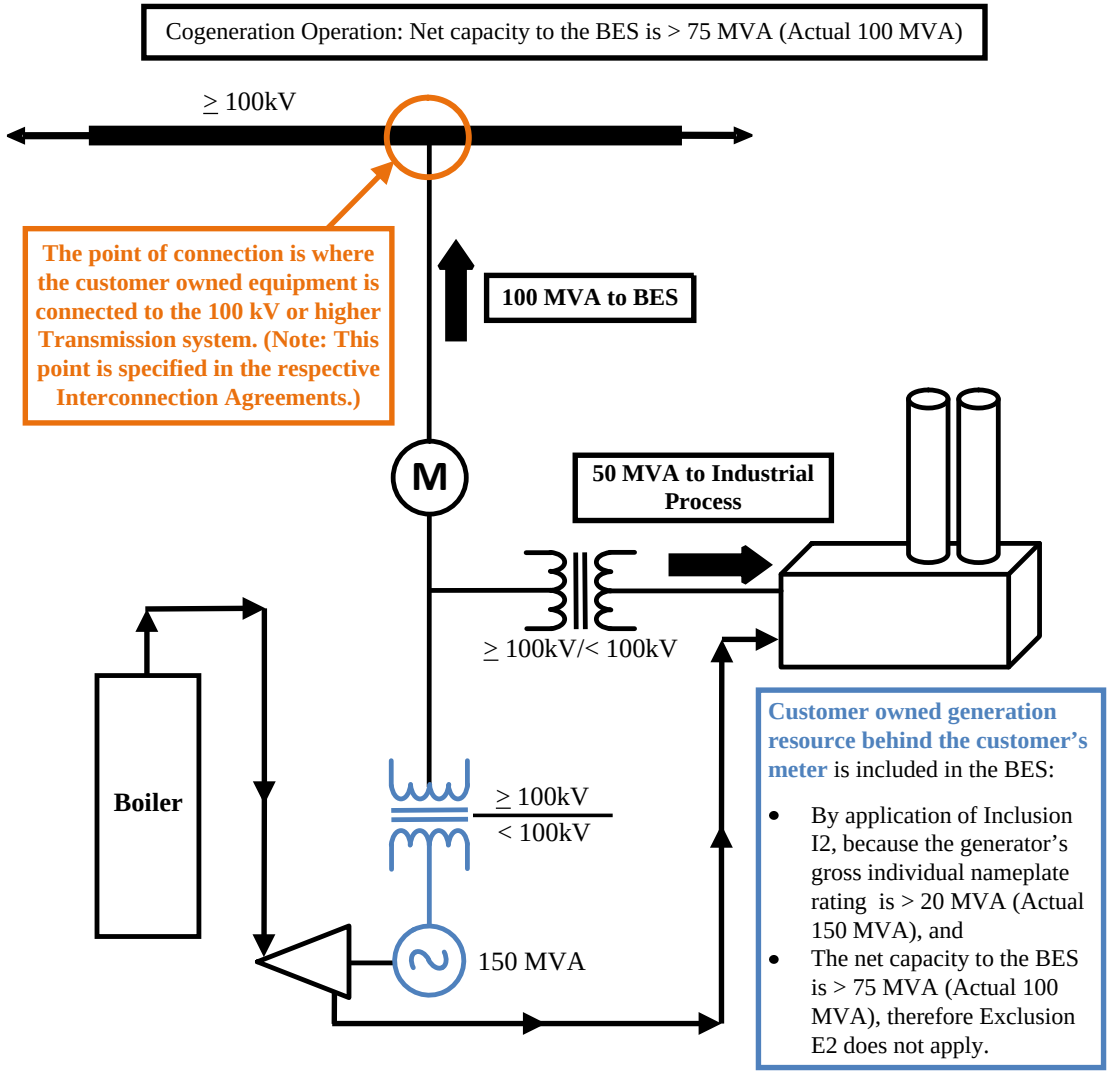


Figure E2-2: Behind-the-Meter Generation: Net Capacity to the BES Greater Than 75 MVA

EXCLUSIONS
E3

Exclusion E3 Local Networks

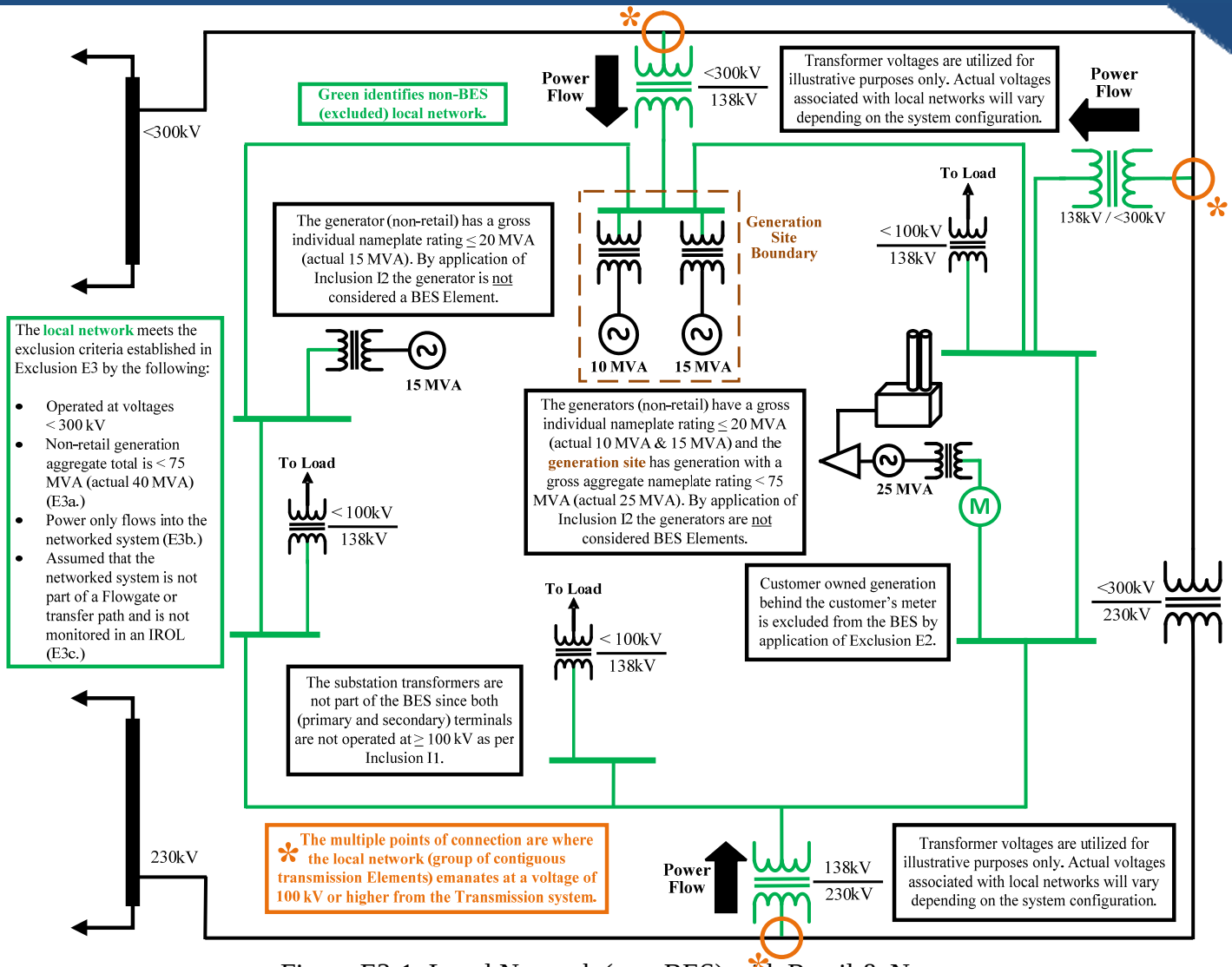
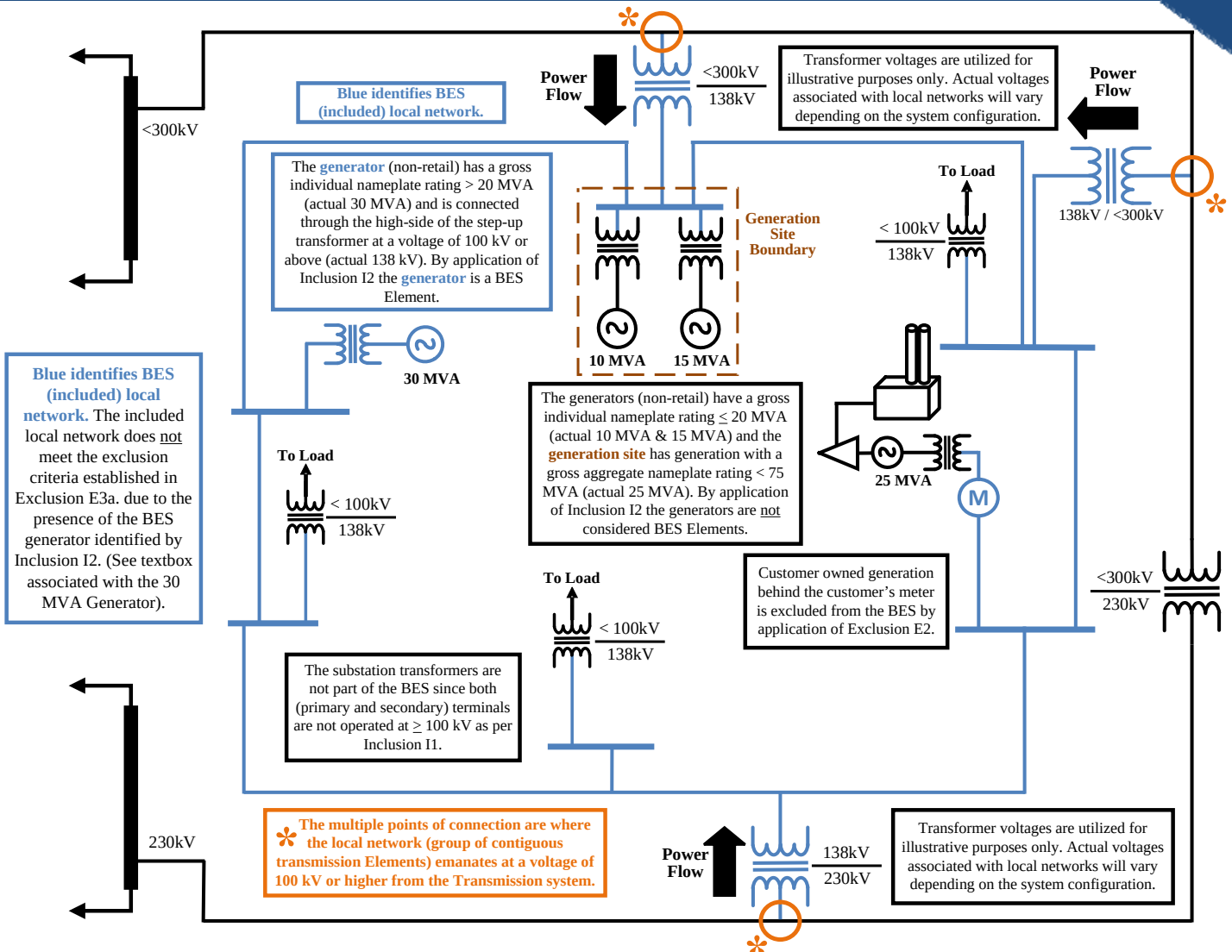


Figure E3-1: Local Network (non-BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks



E3-2: Local Network (BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks

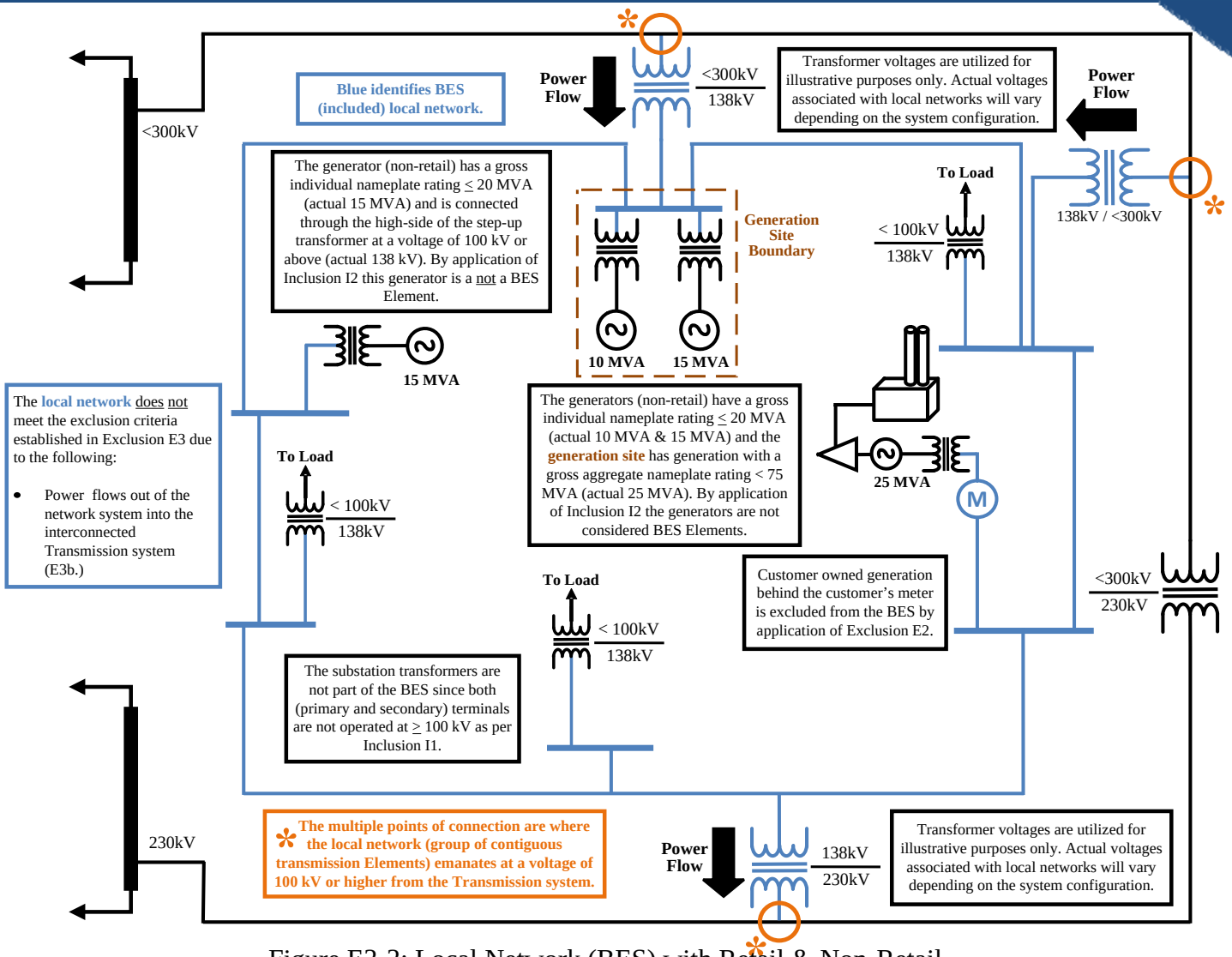


Figure E3-3: Local Network (BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks

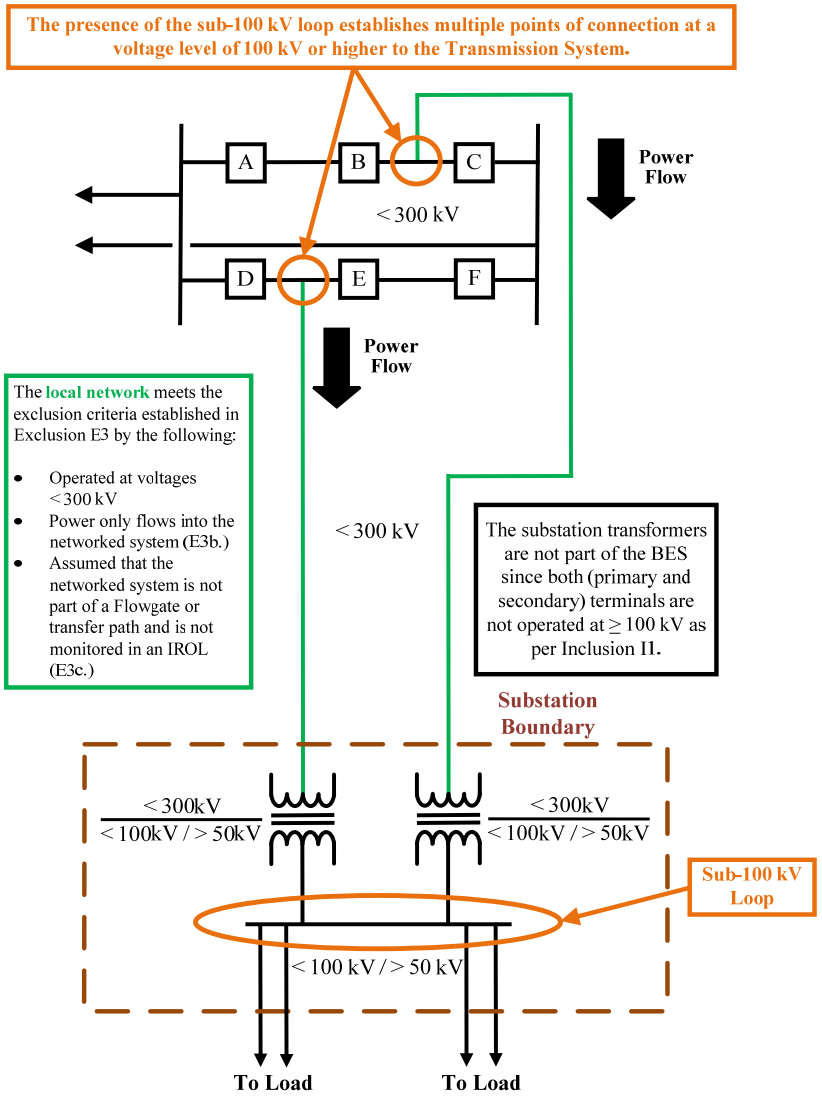


Figure E3-4: Local Network (non-BES) with Sub-100 kV Loop

Exclusion E3 Local Networks

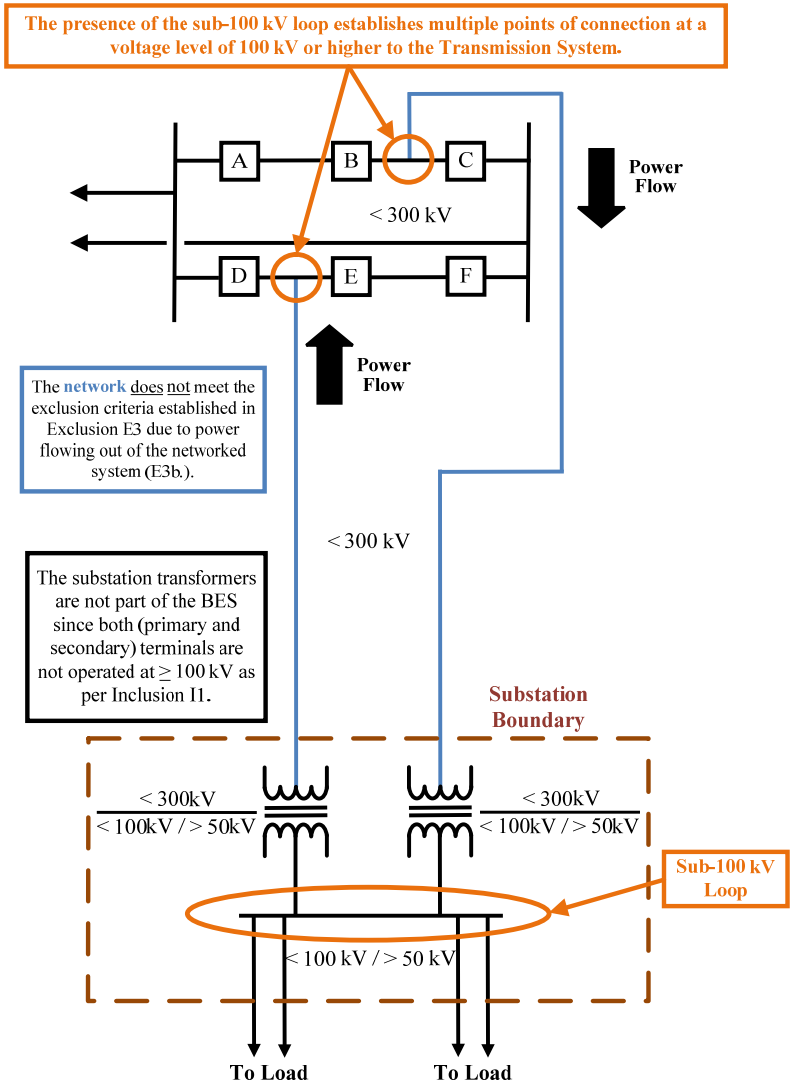


Figure E3-5: Local Network (BES) with Sub-100 kV Loop

Exclusion E3 Local Networks

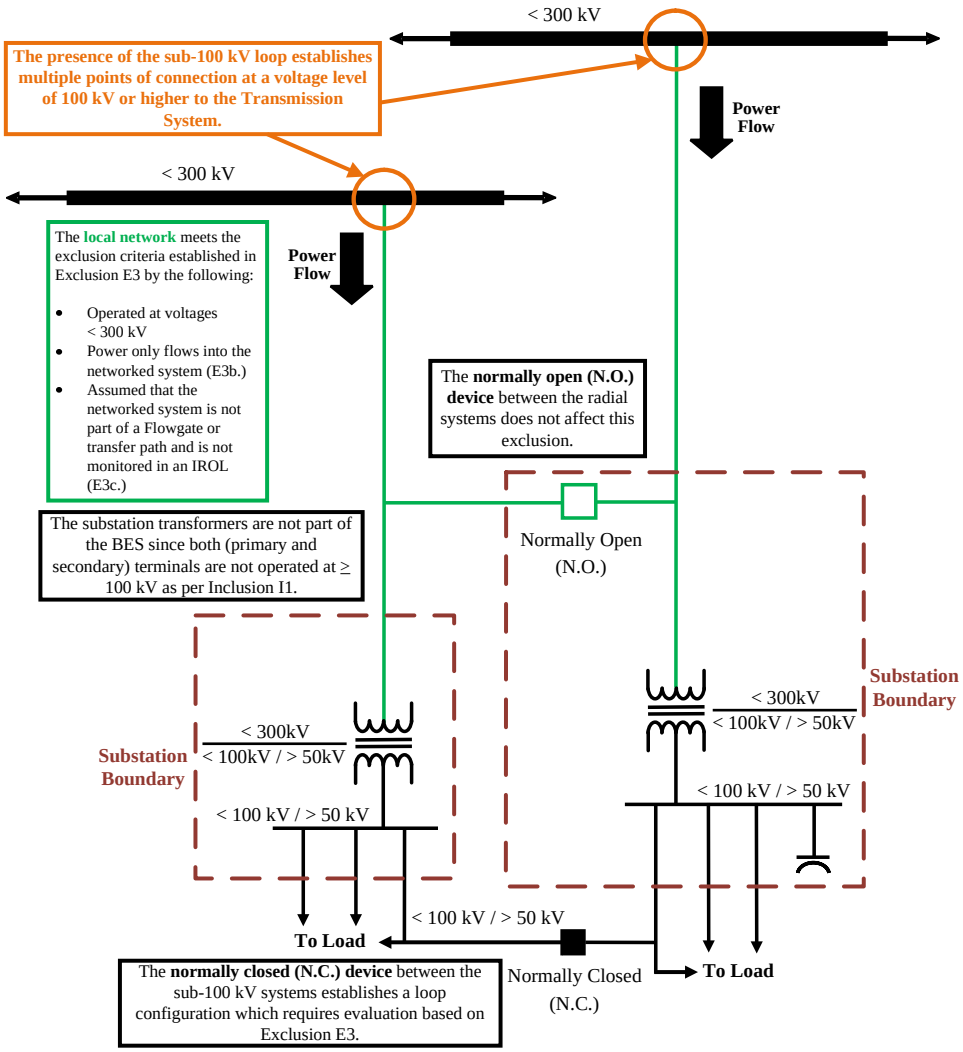


Figure E3-6: Local Network (non-BES) with Sub-100 kV Looped Facilities
(Switching Devices Identified: N.O. > 100 kV & N.C. < 100 kV/> 50 kV)

Exclusion E3 Local Networks

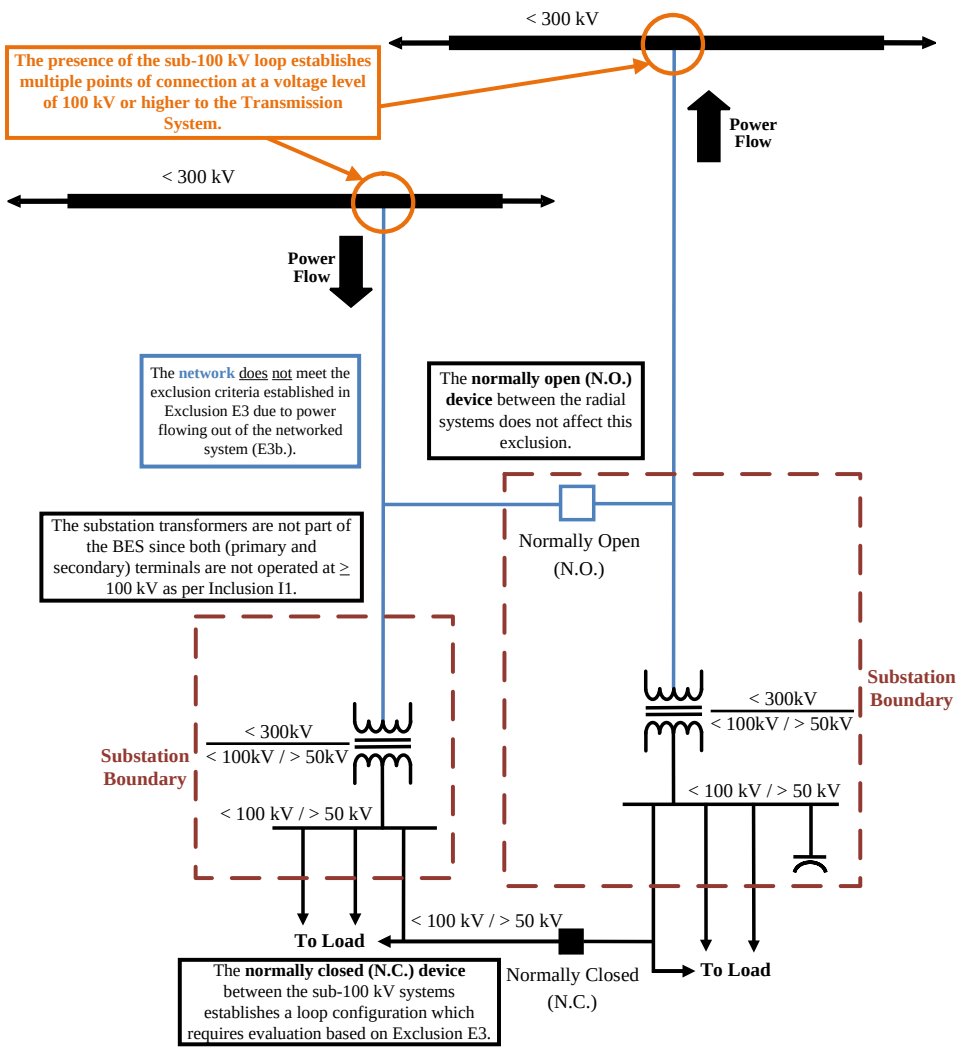


Figure E3-7: Local Network (BES) with Sub-100 kV Looped Facilities
(Switching Devices Identified: N.O. > 100 kV & N.C. < 100 kV/< 50 kV)

Exclusion E3 Local Networks

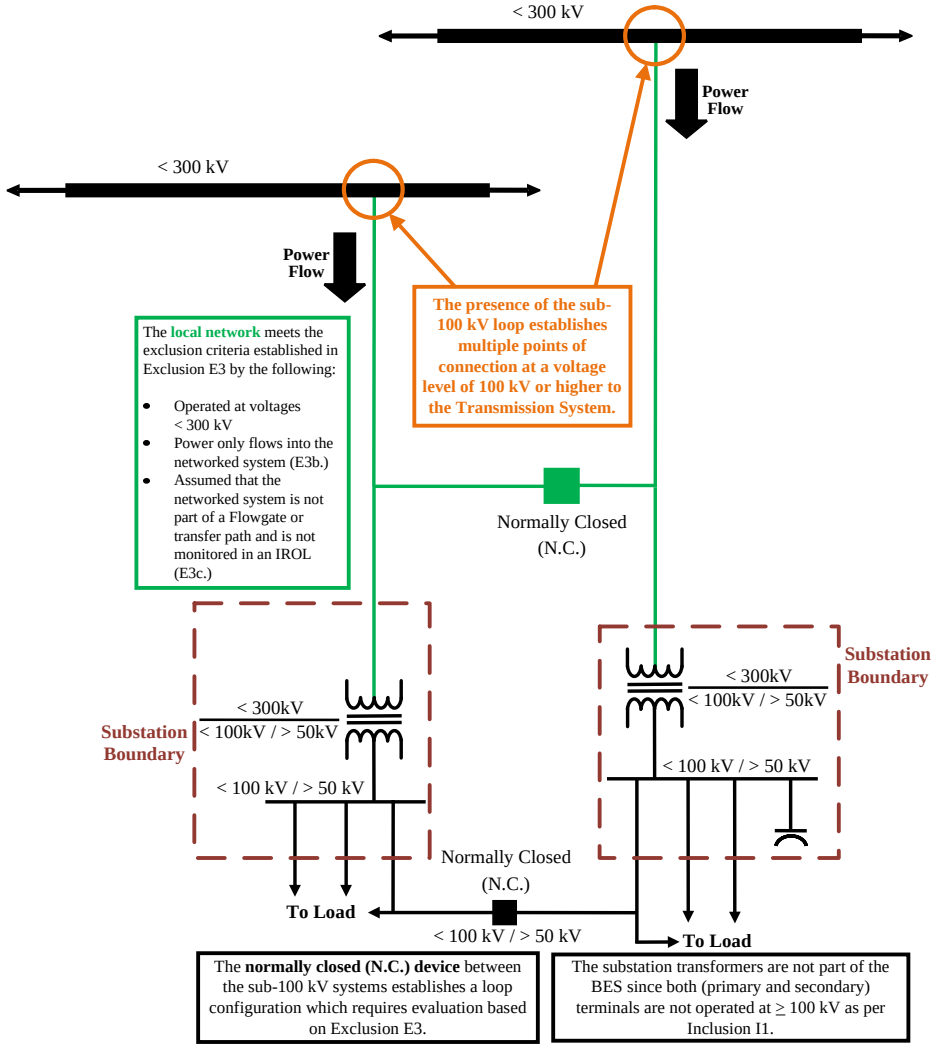


Figure E3-8: Local Network (non-BES) with Sub-100 kV Looped Facilities (Switching Devices Identified: N.C. > 100 kV & N.C. < 100 kV/> 50 kV)

Exclusion E3 Local Networks

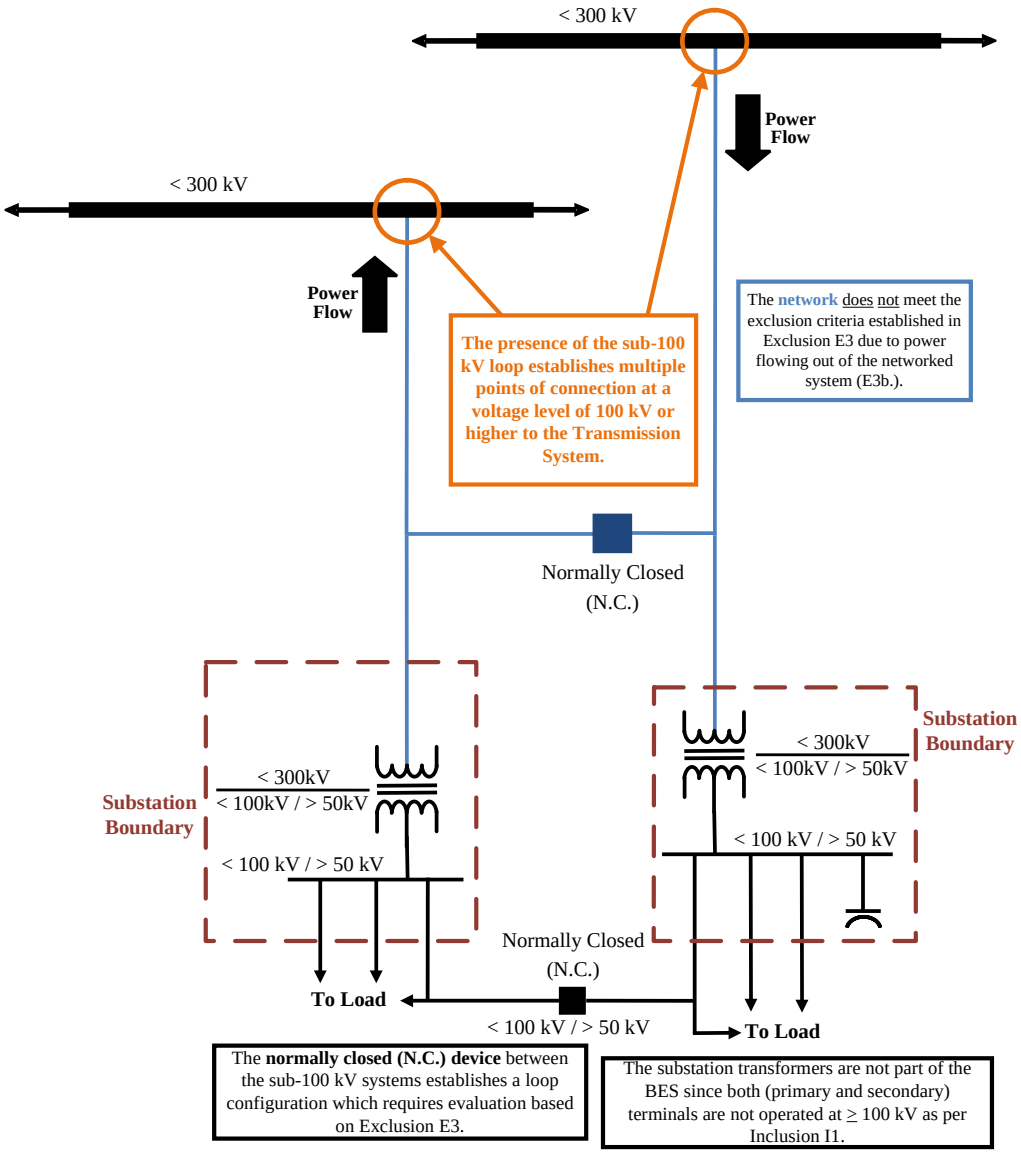


Figure E3-9: Local Network (BES) with Sub-100 kV Looped Facilities
(Switching Devices Identified: N.C. > 100 kV & N.C. < 100 kV/> 50 kV)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Bulk Electric System Definition

Question and Answer Sessions
Intro and Supporting Diagrams

PLEASE WAIT
WE WILL BEGIN SHORTLY

RELIABILITY | ACCOUNTABILITY



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Bulk Electric System Definition

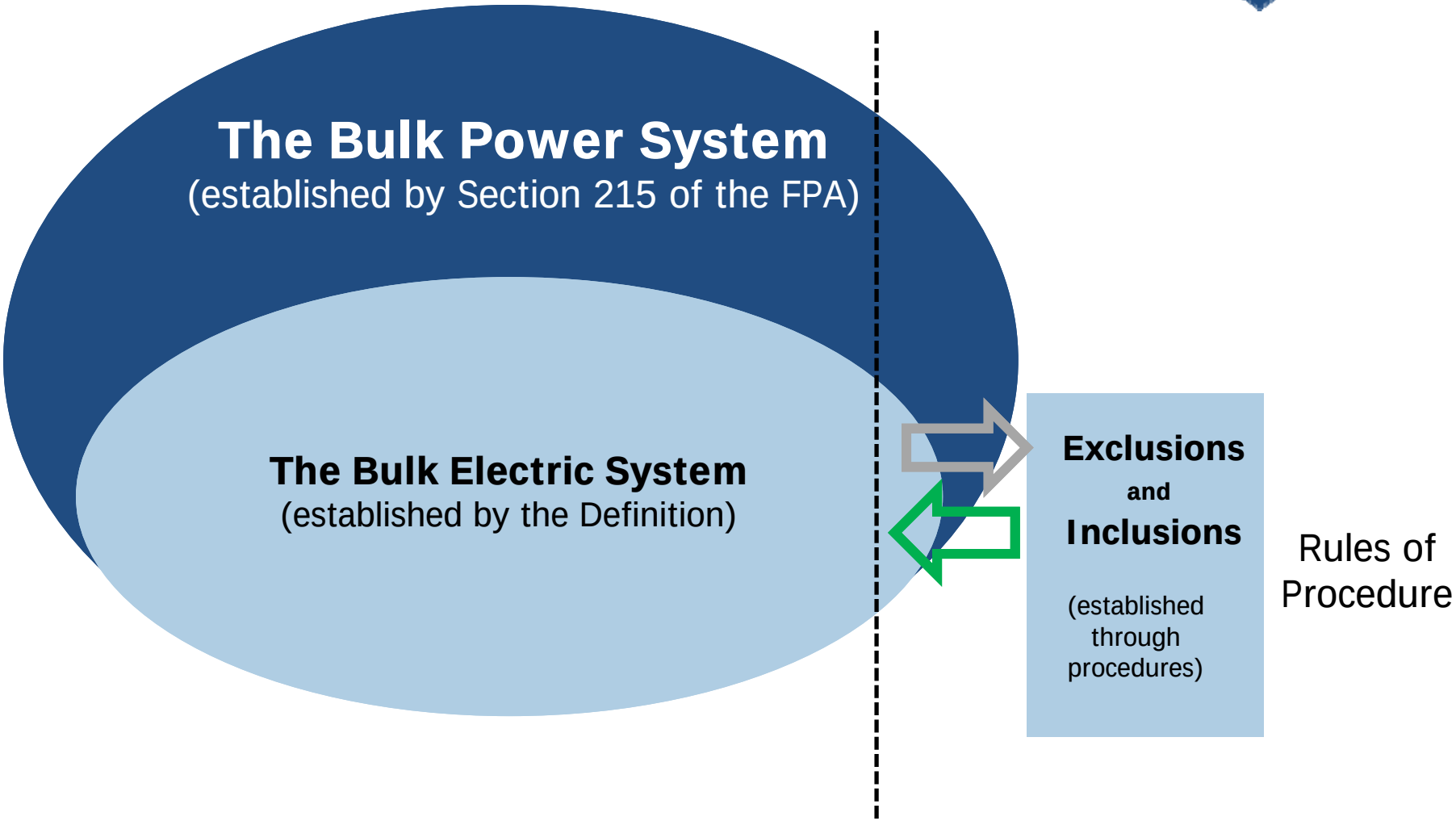
Question and Answer Sessions
Intro and Supporting Diagrams

RELIABILITY | ACCOUNTABILITY






What is the Bulk Electric System?



Many Resources to Assist You

- **Bulk Electric System Definition Reference Document**

  Describes the application of the BES Definition

- **BES Notification Review Guidelines**

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

- **BES Exception Request Evaluation Guidelines**

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

- **BES Implementation Guidance Document (pending)**

  Outlines standards applicability and registration expectations

Many Resources to Assist You

- **BESnet Application Users Guide**

  Manual for the online BESnet application

- **Frequently Asked Questions (FAQ)**

  Explains application, submittal, and process for BES Definition implementation

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

  Regulations approving modified BES definition

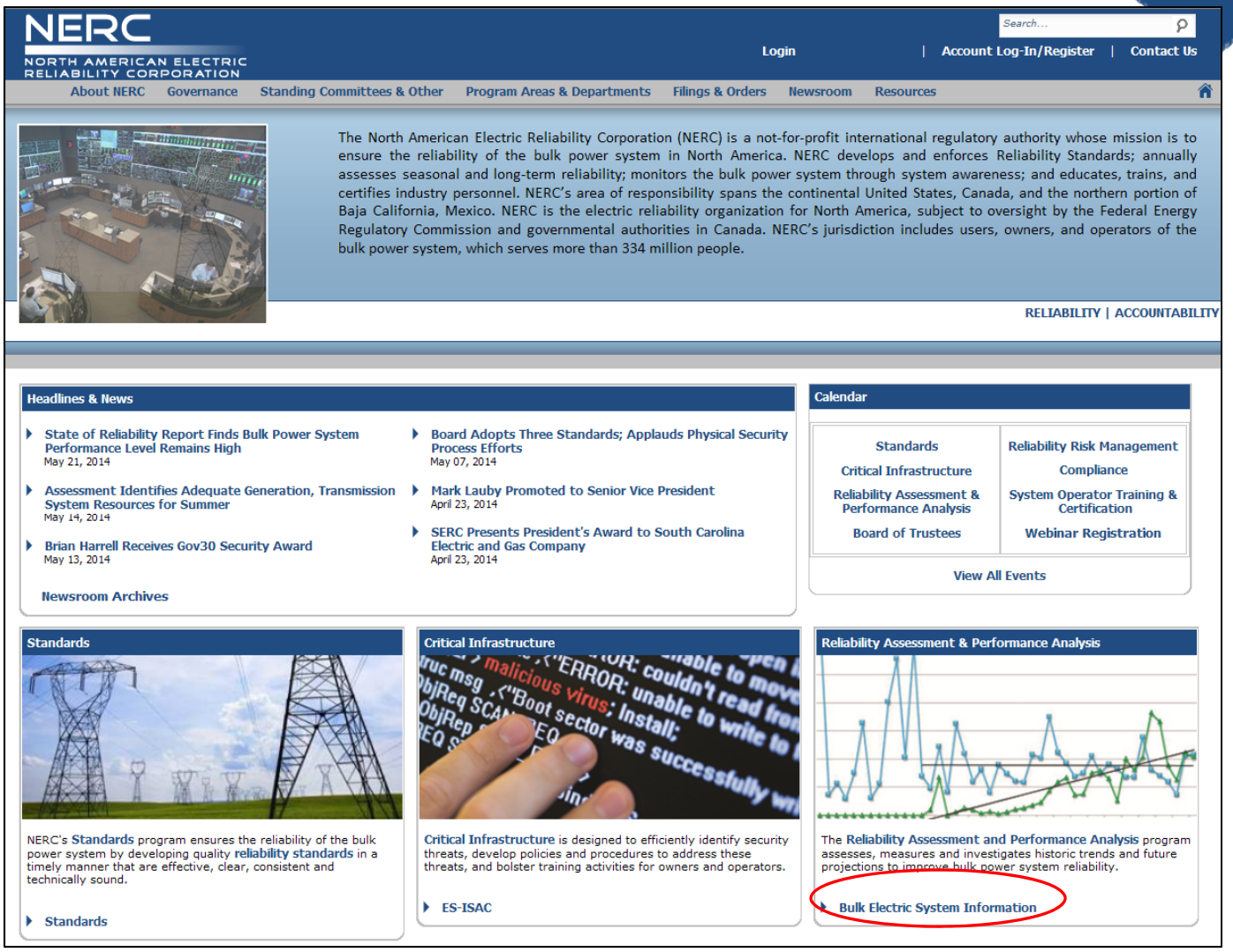
- **NERC Rules of Procedure**

  Section 500 and Appendix 5C

- **Various White Papers**

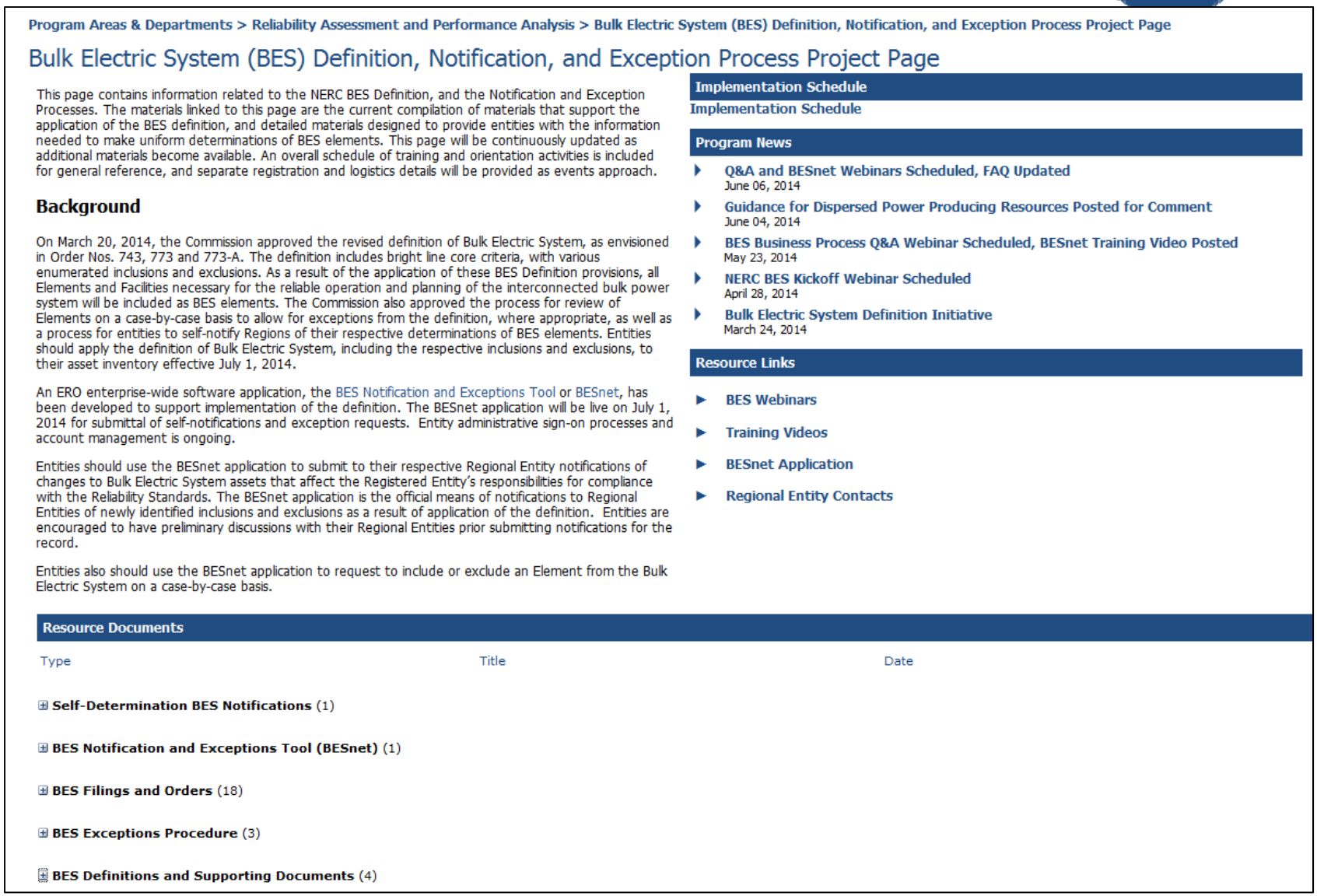
  Providing Technical Justification

For Additional Information



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

BES Project Web Site



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

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

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

Background

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

An ERO enterprise-wide software application, the BES Notification and Exceptions Tool or BESnet, has been developed to support implementation of the definition. The BESnet application will be live on July 1, 2014 for submittal of self-notifications and exception requests. Entity administrative sign-on processes and account management is ongoing.

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

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

Implementation Schedule

Implementation Schedule

Program News

- Q&A and BESnet Webinars Scheduled, FAQ Updated
  June 06, 2014
- Guidance for Dispersed Power Producing Resources Posted for Comment
  June 04, 2014
- BES Business Process Q&A Webinar Scheduled, BESnet Training Video Posted
  May 23, 2014
- NERC BES Kickoff Webinar Scheduled
  April 28, 2014
- Bulk Electric System Definition Initiative
  March 24, 2014

Resource Links

- BES Webinars
- Training Videos
- BESnet Application
- Regional Entity Contacts

Resource Documents

Type	Title	Date
⊞ **Self-Determination BES Notifications** (1)		
⊞ **BES Notification and Exceptions Tool (BESnet)** (1)		
⊞ **BES Filings and Orders** (18)		
⊞ **BES Exceptions Procedure** (3)		
⊞ **BES Definitions and Supporting Documents** (4)		

Training Webinars and Activities

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

BES Business Process Q&A Webinars

June 5
June 11 (with PC/OC meetings in Orlando)
June 16
June 23
June 30

NERC BESnet Training Webinars

June 17
June 18
June 19
June 20
June 24
June 25
June 27

Refer to Implementation Schedule on Website for schedule details

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Questions?

INCLUSIONS I1

Inclusion I1 - Transformers

The **transformer's** primary and secondary terminals are operated at 100 kV or above, and therefore the transformer is included in the BES by application of Inclusion I1.

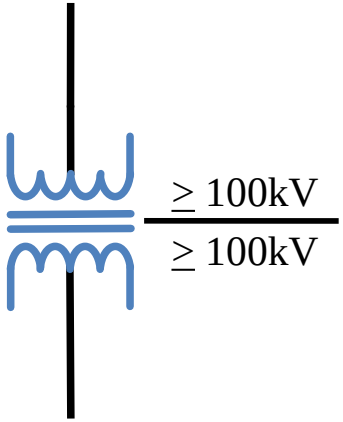


Figure I1-1: Typical Two Winding Transformer (BES)

The **transformer's** primary terminal is operated at 100 kV or above, however the secondary terminal is <u>not</u> operated at a voltage of 100 kV or above. Therefore the transformer is <u>not</u> included in the BES by application of Inclusion I1.

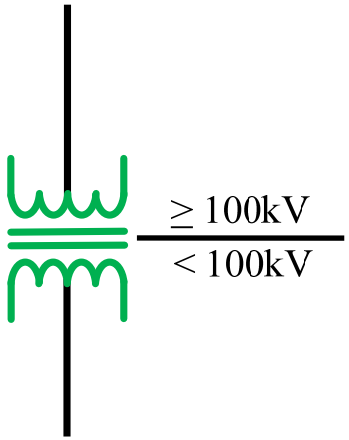
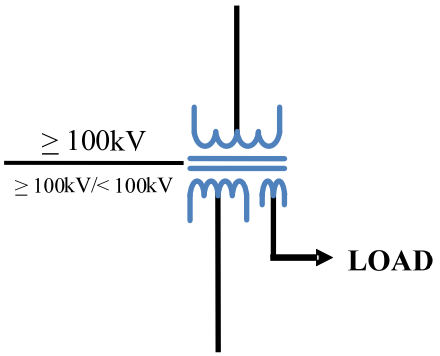


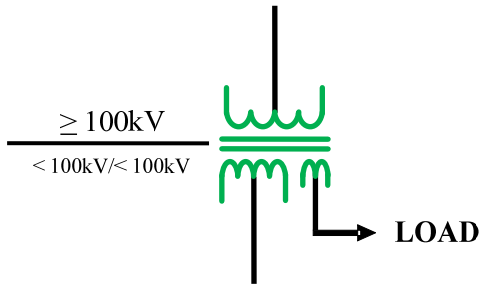
Figure I1-3: Typical Two Winding Transformer (non-BES)

Inclusion I1 - Transformers



The **transformer's** primary terminal and one secondary terminal are operated at 100 kV or above, and therefore the transformer is included in the BES by application of Inclusion I1. Since the transformer is one Element, all windings internal to the transformer (including the tertiary winding) would be included in the BES. The Load and the connection to the tertiary winding, indicated in the diagram, are non-BES as they are connected at a voltage < 100 kV.

Figure I1-2: Typical Three Winding Transformer (BES)



The **transformer's** primary terminal is operated at 100 kV or above, however neither of the secondary terminals are operated at a voltage of 100 kV or above. Therefore the transformer is not included in the BES by application of Inclusion I1. The Load and the connection to the tertiary winding, indicated in the diagram, are non-BES as they are connected at a voltage < 100 kV.

Figure I1-4: Typical Three Winding Transformer (non-BES)

INCLUSIONS I2

Inclusion I2 – Generating Resources

The **generator** has a gross individual nameplate rating > 20 MVA and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 the **generator including the generator terminals through the high-side of the step-up transformer** is included in the BES.

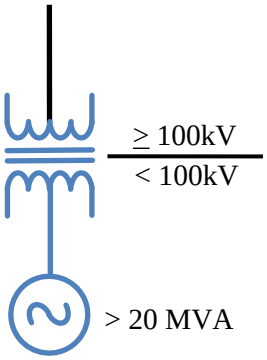


Figure I2-1: Single Generator (BES)

The **generator** has a gross individual nameplate rating ≤ 20 MVA (actual 19 MVA) and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 the **generator including the generator terminals through the high-side of the step-up transformer** is not included in the BES.

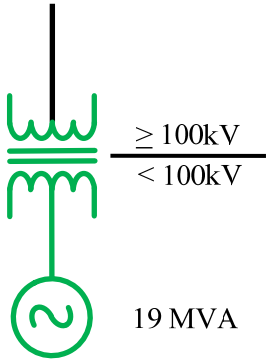
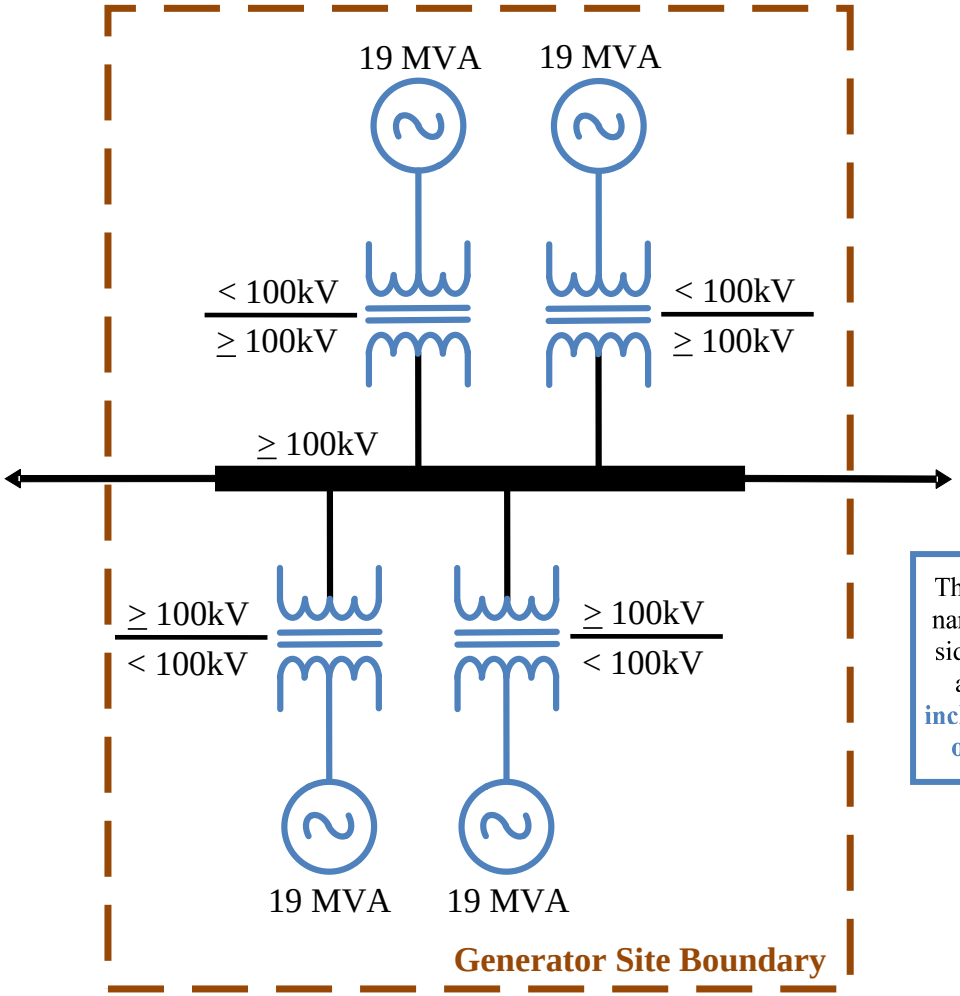


Figure I2-2: Single Generator (non-BES)

Inclusion I2 – Generating Resources



The generation site has generation with a gross aggregate nameplate rating of 76 MVA connected through the high-side of the step-up transformers at a voltage of 100 kV or above. By application of Inclusion I2, the **generators including the generator terminals through the high-side of the step-up transformers** are included in the BES.

Figure I2-3: Multiple Generators at a Single Site (BES)

Inclusion I2 – Generating Resources

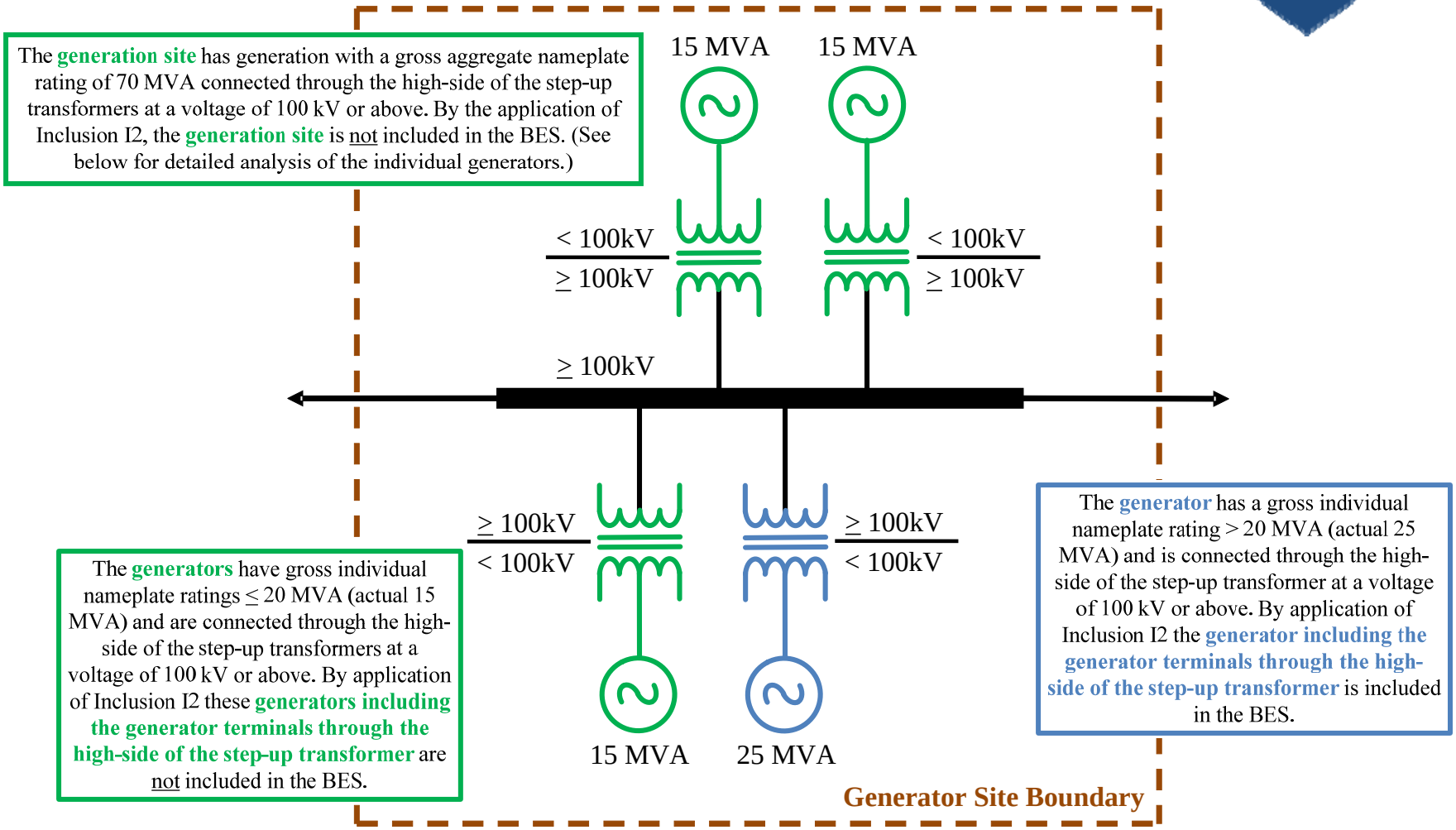
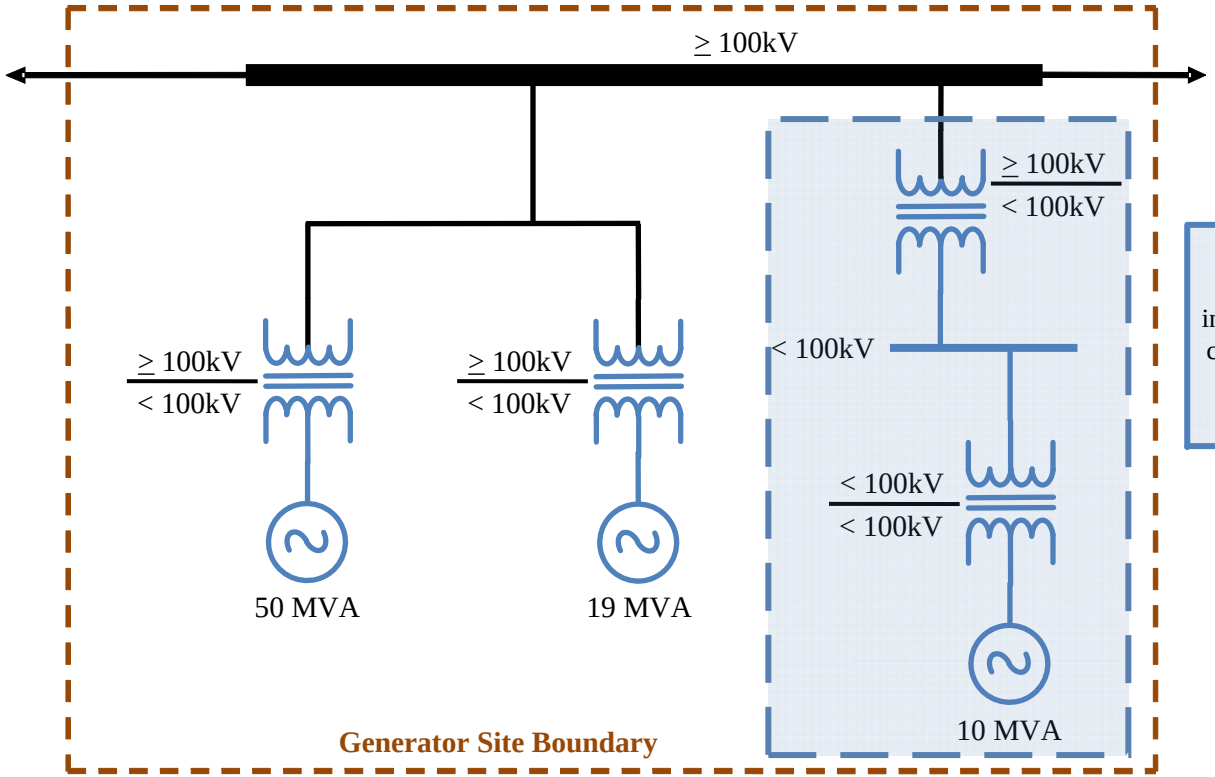


Figure I2-4: Multiple Generators at a Single Site (BES & non-BES)

Inclusion I2 – Generating Resources

The **generation site** has generation with a gross aggregate nameplate rating greater than 75 MVA (actual 79 MVA) connected through the high-side of the step-up transformers at a voltage of 100 kV or above. By the application of Inclusion I2, the **generation site** is included in the BES.

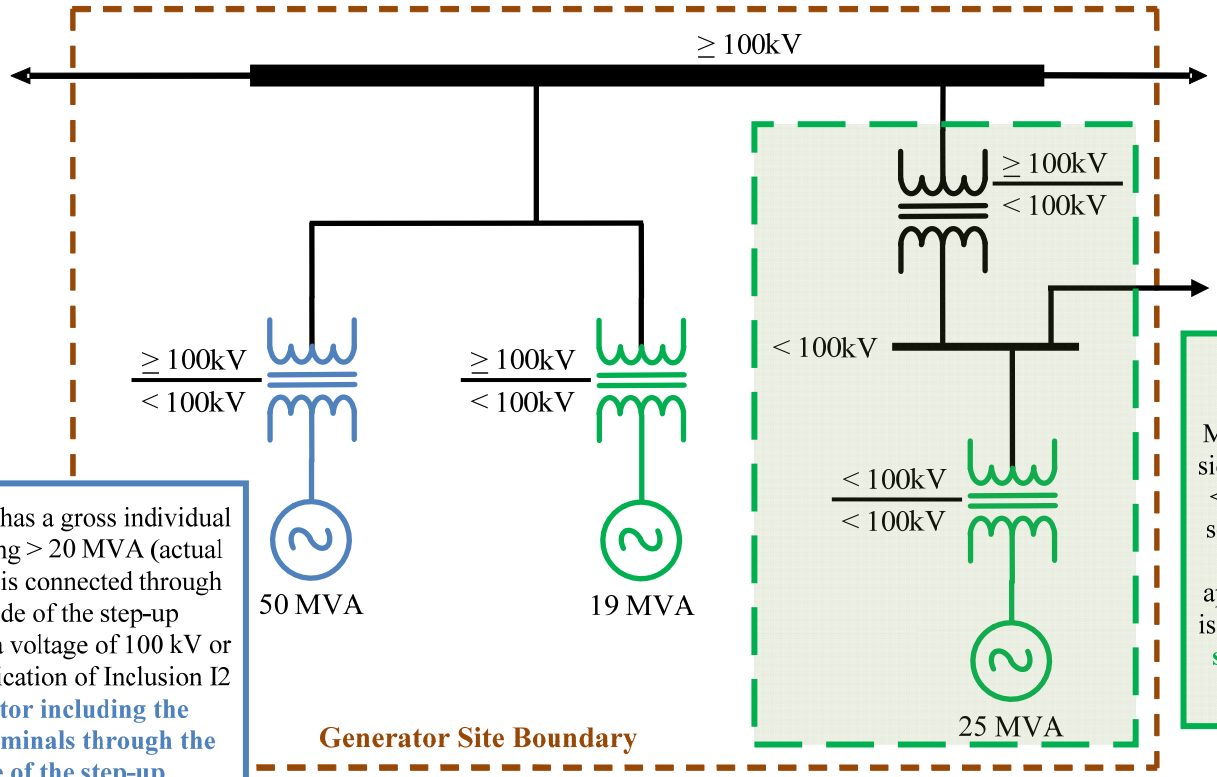


The **generator step-up transformers,** associated with the 10 MVA generator, including the interconnecting bus work are considered a BES Element. The generator contributes to the gross aggregate nameplate rating of the site.

Figure I2-5: Multiple Generators at a Single Site (BES)

Inclusion I2 – Generating Resources

The **generation site** has generation with a gross aggregate nameplate rating of less than 75 MVA (actual 69 MVA (50 + 19 MVA)) connected through the high-side of the step-up transformers at a voltage of 100 kV or above. The 25 MVA generator is not included in the gross aggregate calculation, see textbox on right. By the application of Inclusion I2, the **generation site** is not included in the BES.



The **generator** has a gross individual nameplate rating > 20 MVA (actual 50 MVA) and is connected through the high-side of the step-up transformer at a voltage of 100 kV or above. By application of Inclusion I2 this **generator including the generator terminals through the high-side of the step-up transformer** is included in the BES.

The **generator** has a gross individual nameplate rating > 20 MVA (actual 25 MVA) and is connected through the high-side of the step-up transformer at a voltage < 100 kV. The interconnecting bus work serves Load and provides a connection to sub-100 kV Facilities, therefore by application of Inclusion I2, the **generator** is connected **through the high-side of the step-up transformer** at a voltage < 100 kV and is not included in the BES.

Figure I2-6: Multiple Generators at a Single Site (BES & non-BES)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INCLUSIONS I4

Inclusion I4 – Dispersed Power Producing Resources

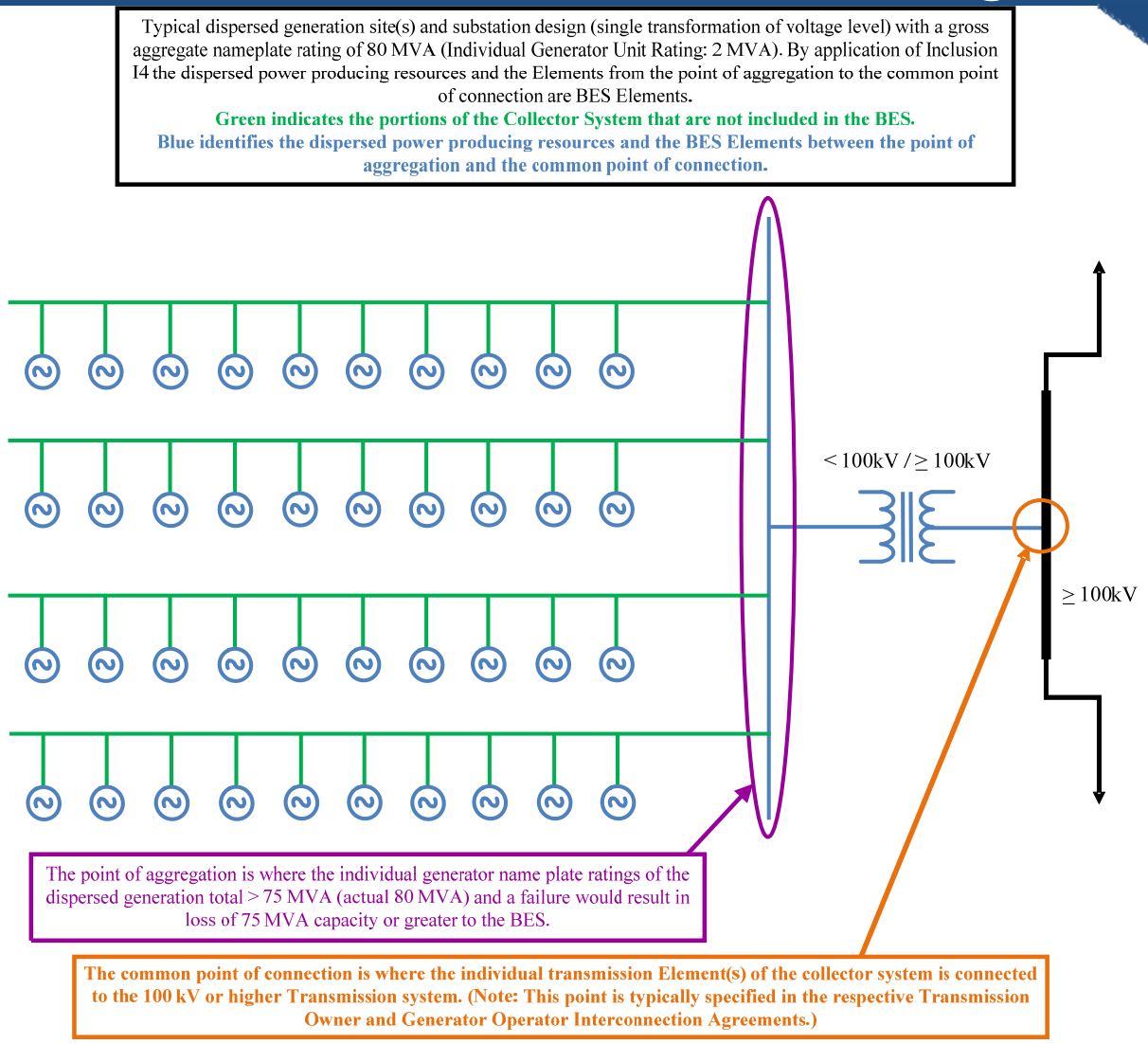


Figure I4-1 Dispersed Generation Site (Single Voltage Transformation) – Wind Farm

Inclusion I4 – Dispersed Power Producing Resources

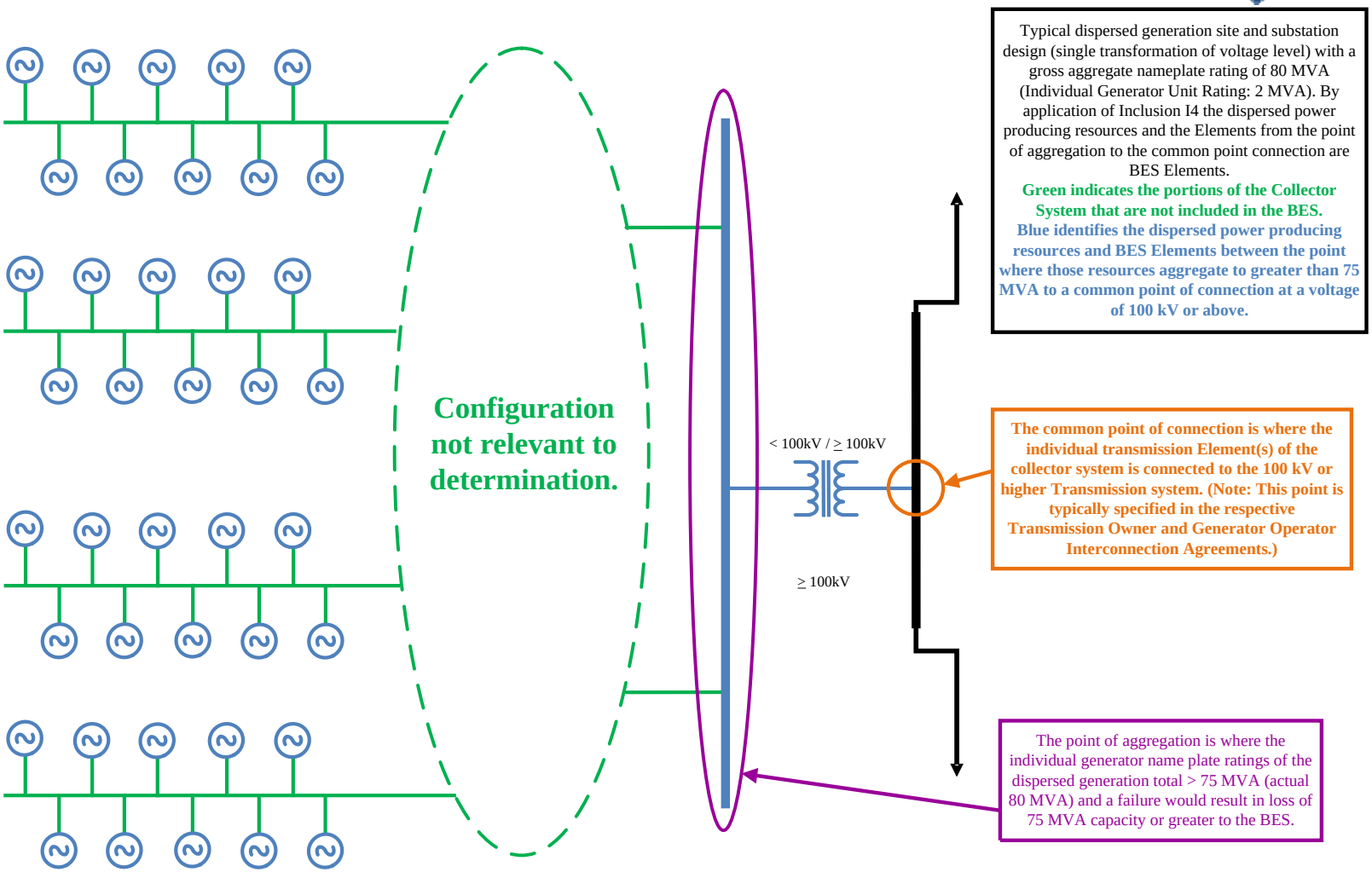


Figure I4-2 Dispersed Generation Site (Unknown Collector System Configuration) – Wind Farm

Inclusion I4 – Dispersed Power Producing Resources

Dispersed generation site and substation design (single transformation of voltage level) with a gross aggregate nameplate rating of 80 MVA (Individual Photovoltaic Bank Rating: 20 MVA). By application of Inclusion I4 the Photovoltaic Cells & Inverters (generators) are included in the BES.

Green indicates the portions of the Collector System that are not included in the BES.

Blue identifies BES dispersed power producing resources (Photovoltaic Cells & Inverters) and the BES Elements between the point of aggregation and the common point of connection.

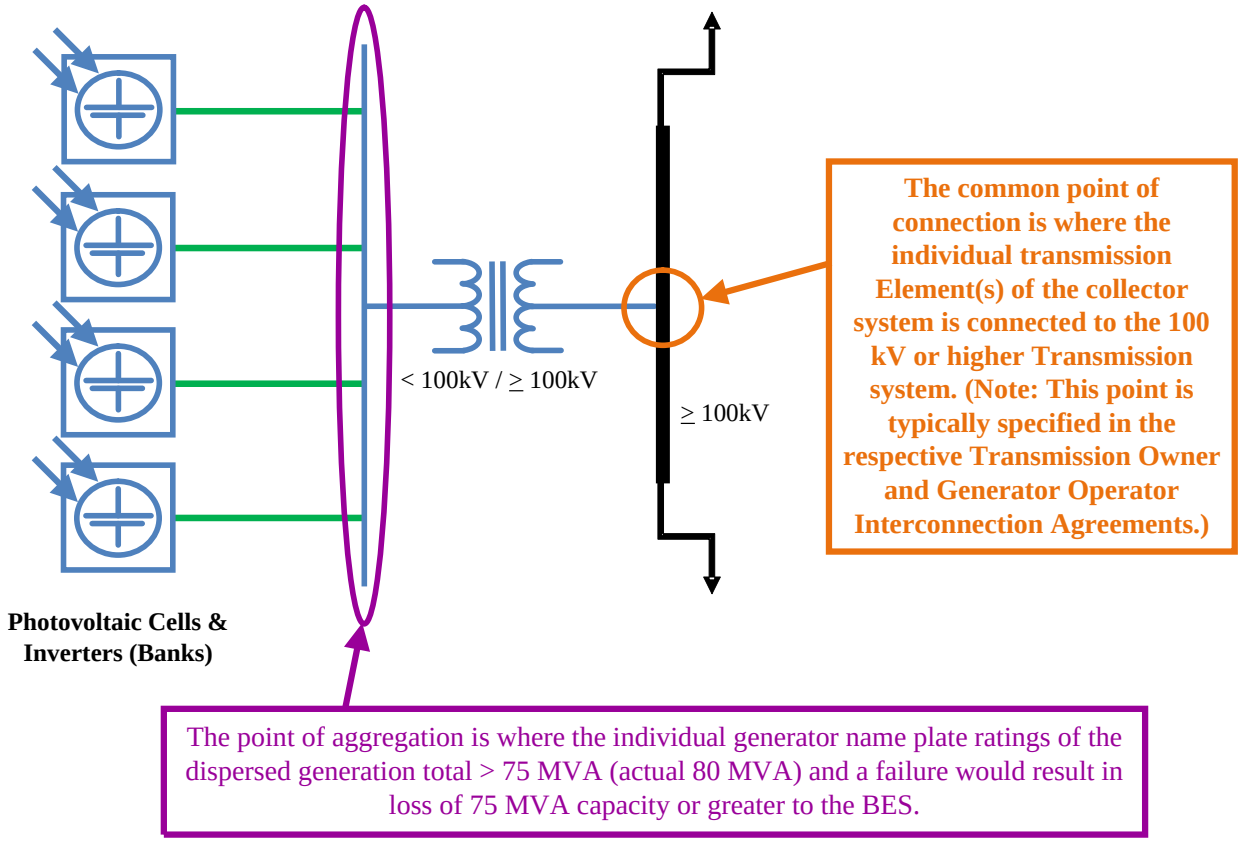


Figure I4-3 Dispersed Generation Site (Single Voltage Transformation) – Solar Array

Inclusion I4 – Dispersed Power Producing Resources

Dispersed generation site and substation design (multiple transformations of voltage level) with a gross aggregate nameplate rating of 80 MVA (Individual Photovoltaic Bank Rating: 20 MVA). By application of Inclusion I4 the Photovoltaic Cells & Inverters (generator units) are included in the BES.

Green indicates the portions of the Collector System that are not included in the BES.

Blue identifies BES dispersed power producing resources (Photovoltaic Cells & Inverters) and the BES Elements between the point of aggregation and the common point of connection.

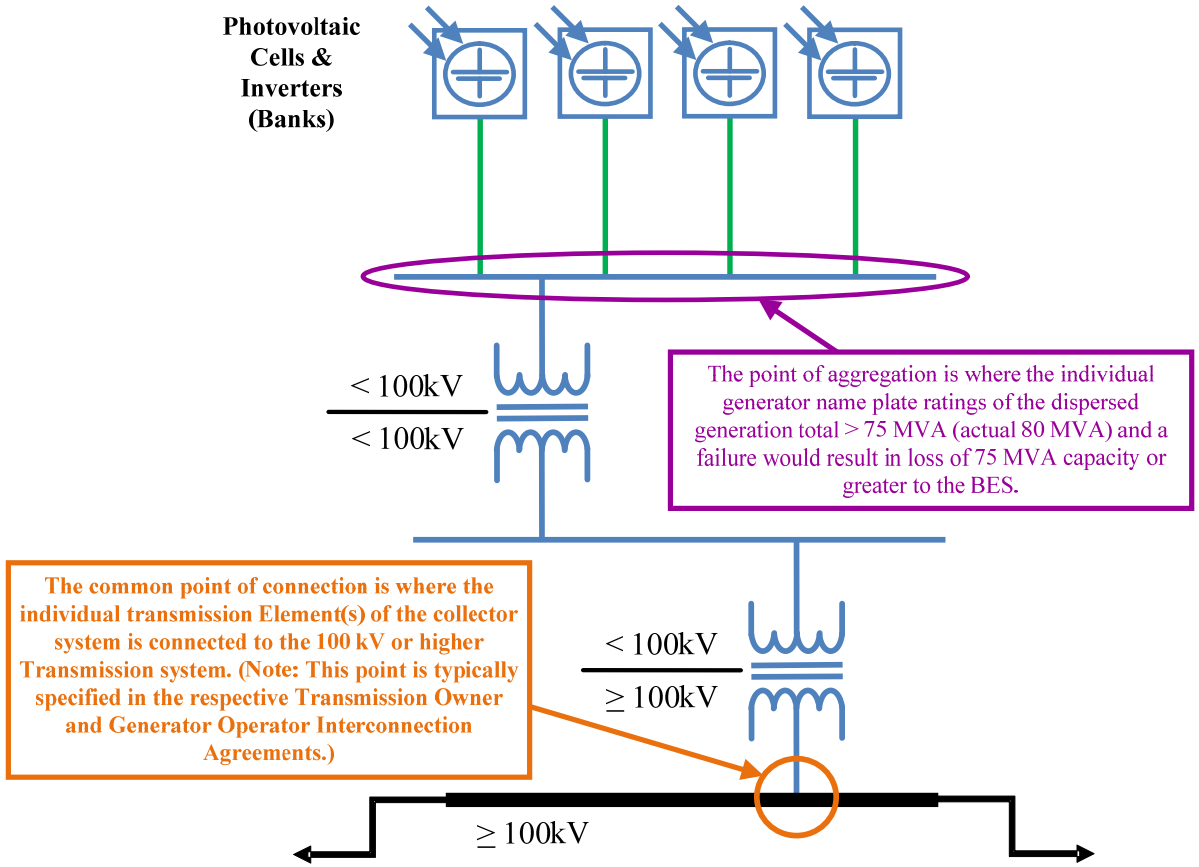


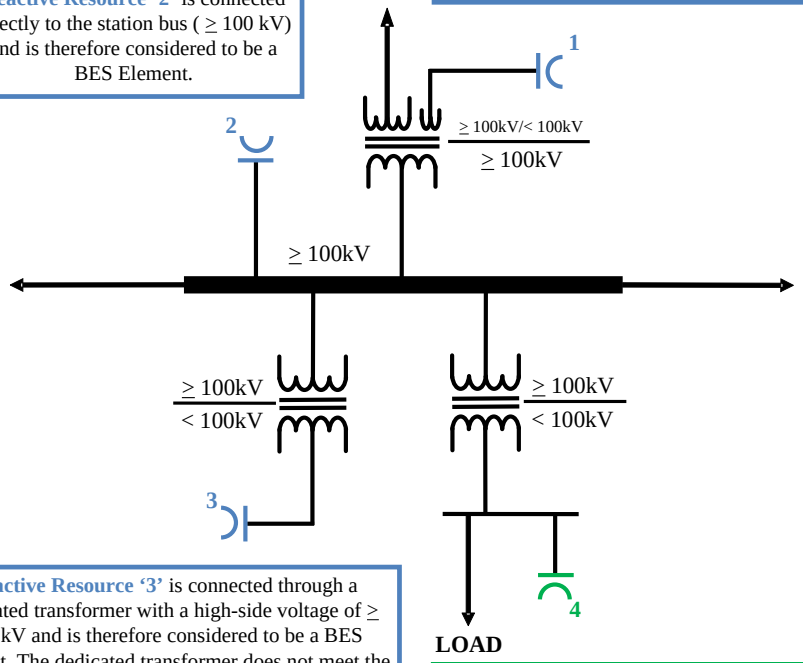
Figure I4-4 Dispersed Generation Site (Multiple Voltage Transformations) – Solar Array

INCLUSIONS I5

Inclusion I5 – Reactive Power Devices

Reactive Resource '1' is connected through the tertiary winding of a transformer that meets the inclusion criteria established by Inclusion I5 (i.e., through a transformer that is designated in Inclusion I1) and is therefore considered to be a BES Element.

Reactive Resource '2' is connected directly to the station bus (≥ 100 kV) and is therefore considered to be a BES Element.



Reactive Resource '3' is connected through a dedicated transformer with a high-side voltage of ≥ 100 kV and is therefore considered to be a BES Element. The dedicated transformer does not meet the inclusion criteria established by Inclusion I1 and is therefore not considered to be a BES Element.

Reactive Resource '4' is connected directly to the station bus (< 100 kV), and is not connected through a dedicated transformer with a high-side voltage of 100 kV or higher or through a transformer that is designated in Inclusion I1, and is therefore not considered to be a BES Element.

EXCLUSIONS
E1

Exclusion E1 Radial Systems
E1.a Serves Load Only

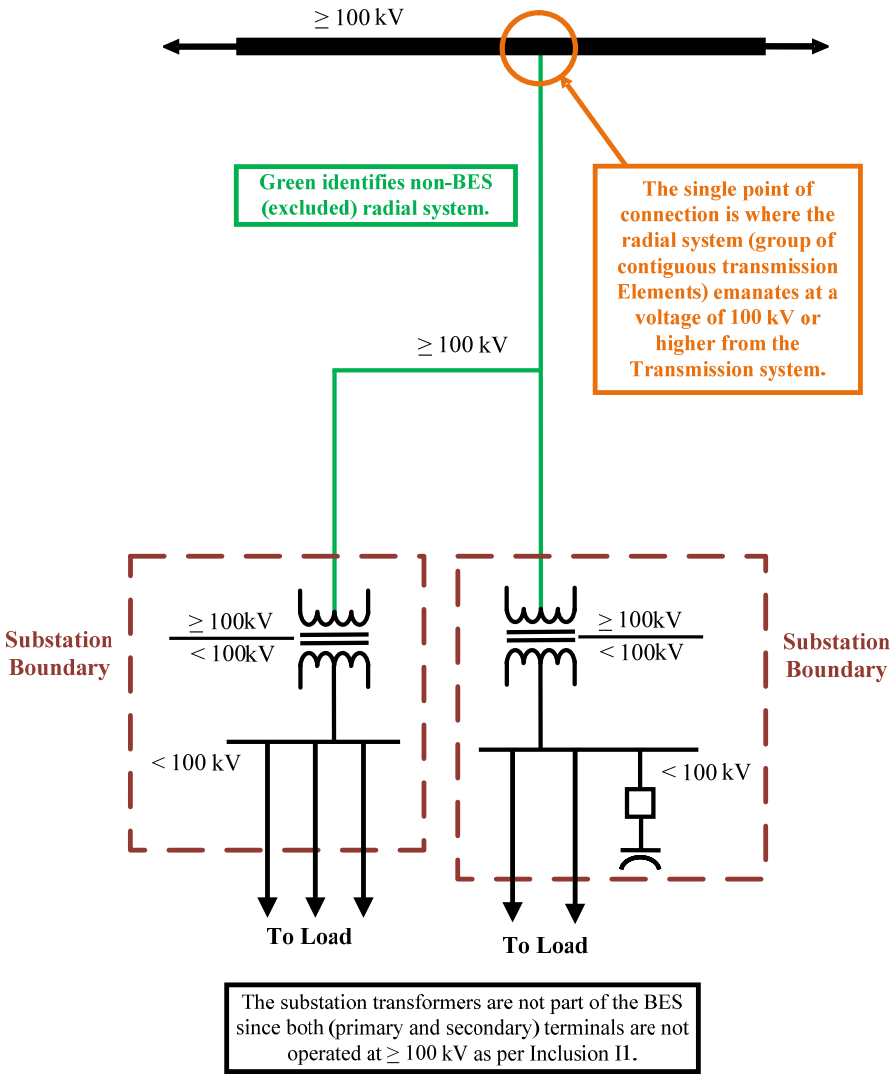


Figure E1-1: Radial System: Serving Only Load

Exclusion E1 Radial Systems
E1.a Serves Load Only

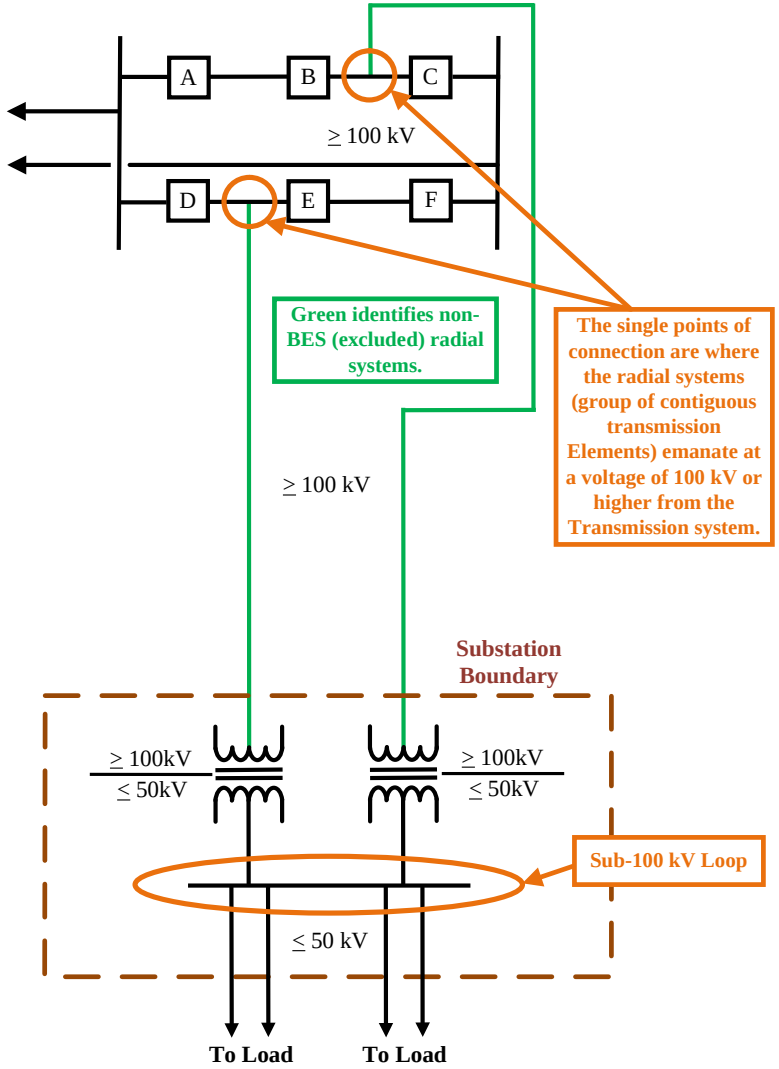


Figure E1-2: Multiple Radial Systems (Underlying Loop Facilities < 50 kV)

Exclusion E1 Radial Systems
E1.a Serves Load Only

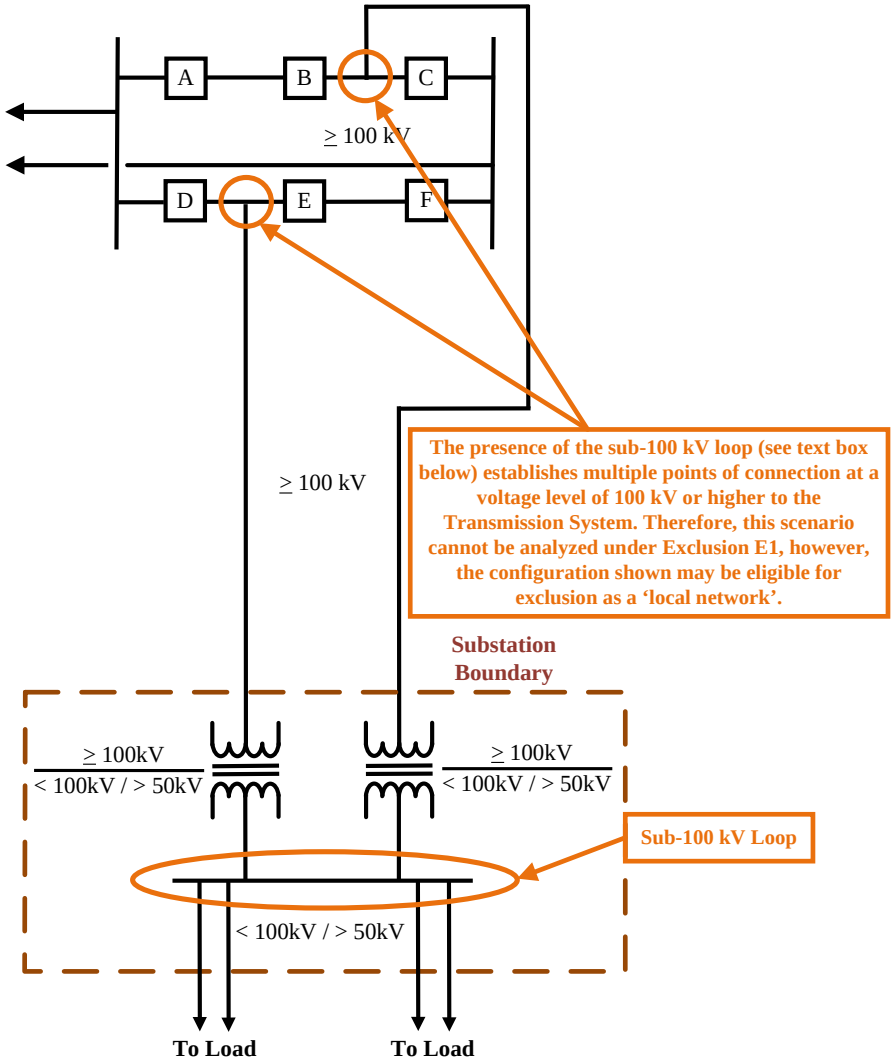


Figure E1-3: Impact of Sub-100 kV Looped Facilities

Exclusion E1 Radial Systems
E1.b Generation Only

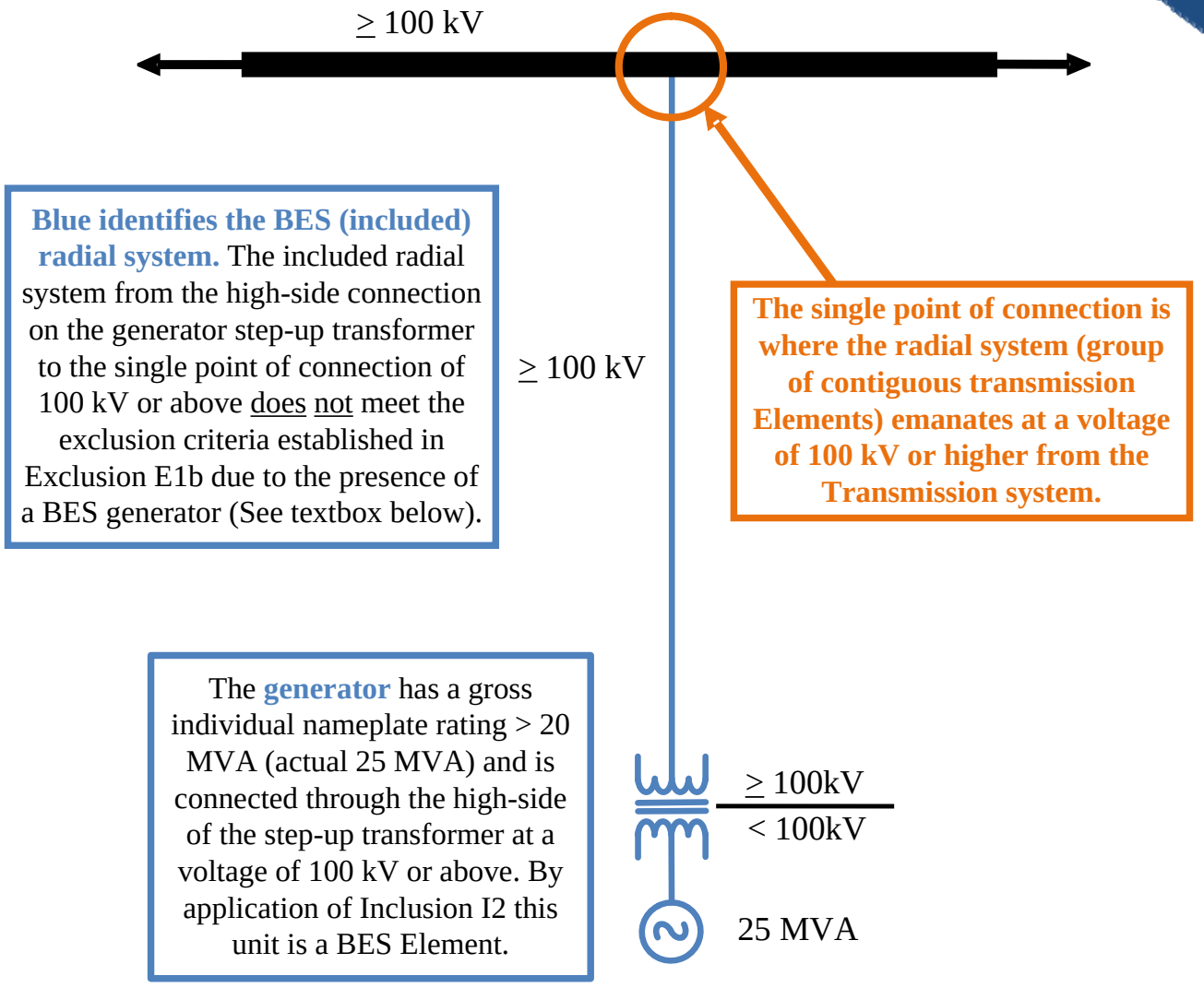


Figure E1-4: Radial System: Single BES Generation Resource

Exclusion E1 Radial Systems
E1.b Generation Only

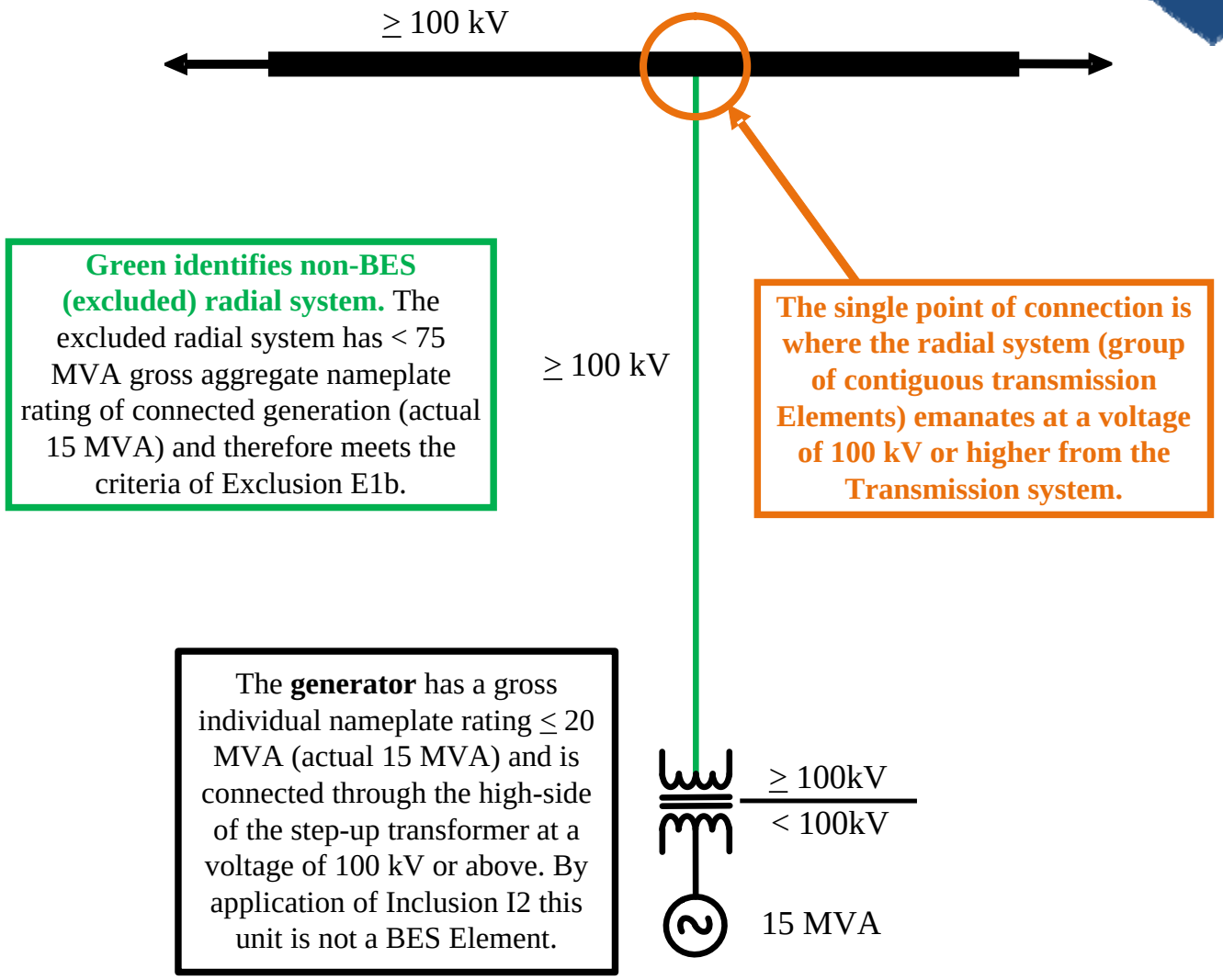


Figure E1-5: Radial System: Single non-BES Generation Resource

Exclusion E1 Radial Systems
E1.b Generation Only

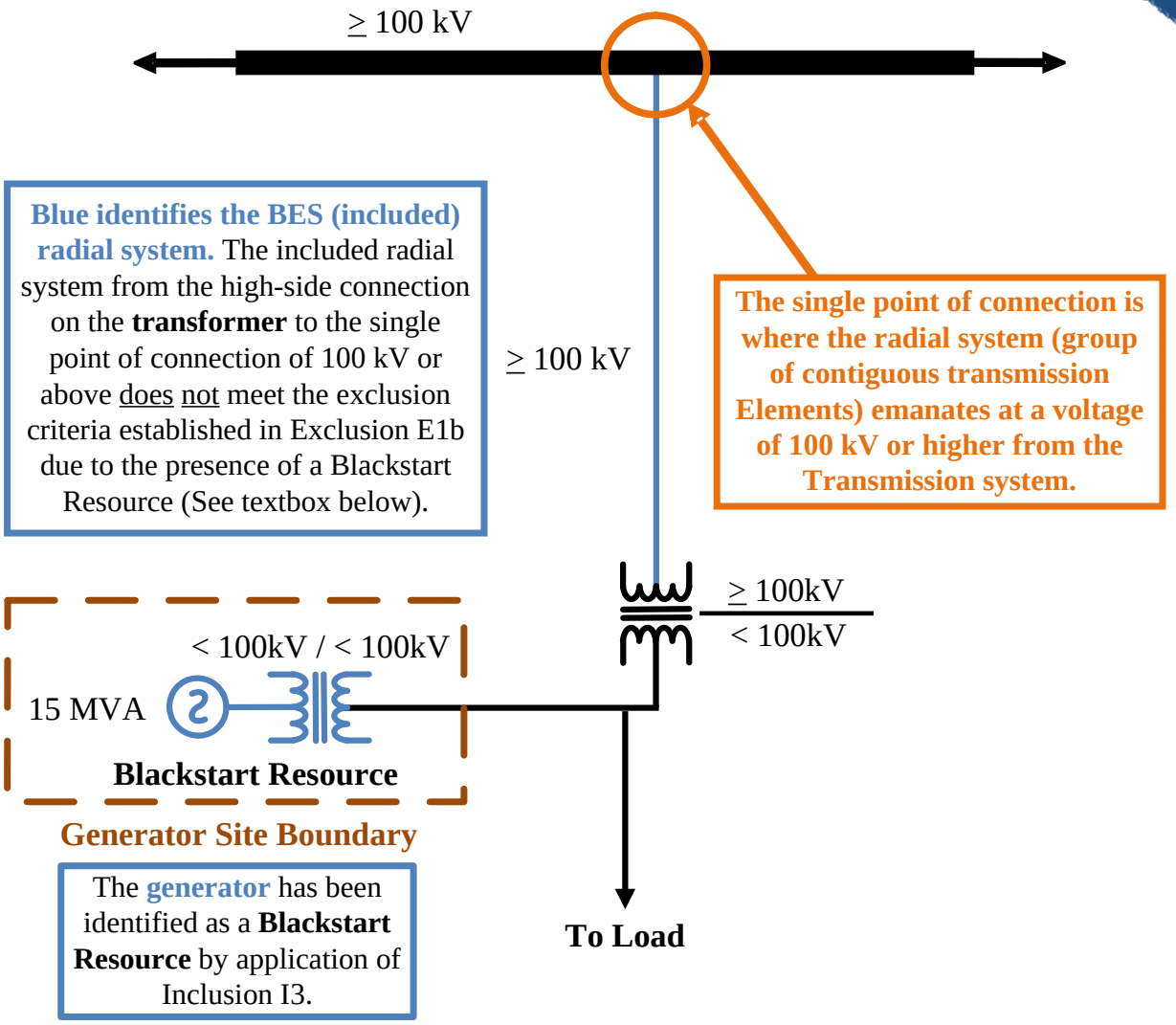


Figure E1-6: Radial System: Blackstart Resource

Exclusion E1 Radial Systems
E1.b Generation Only

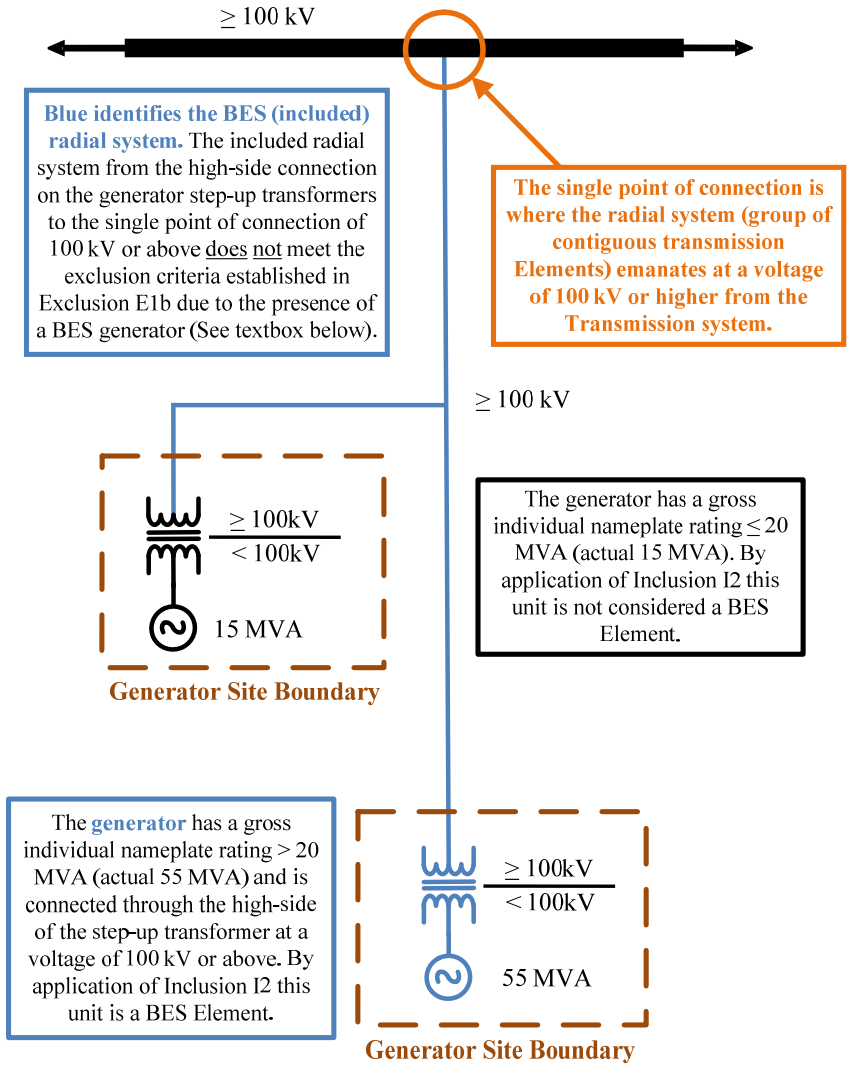


Figure E1-7: Radial System: Multiple (BES & non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.b Generation Only

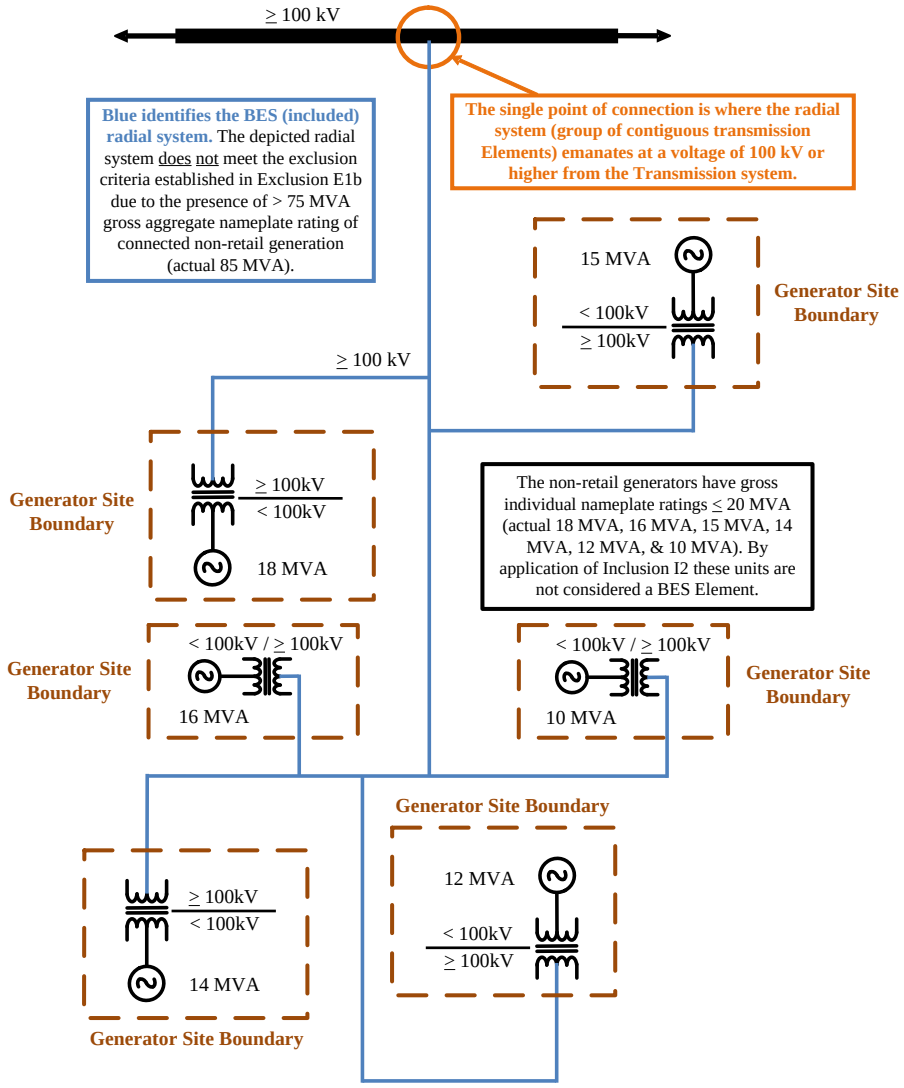


Figure E1-8: Radial System: Multiple (non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.b Generation Only

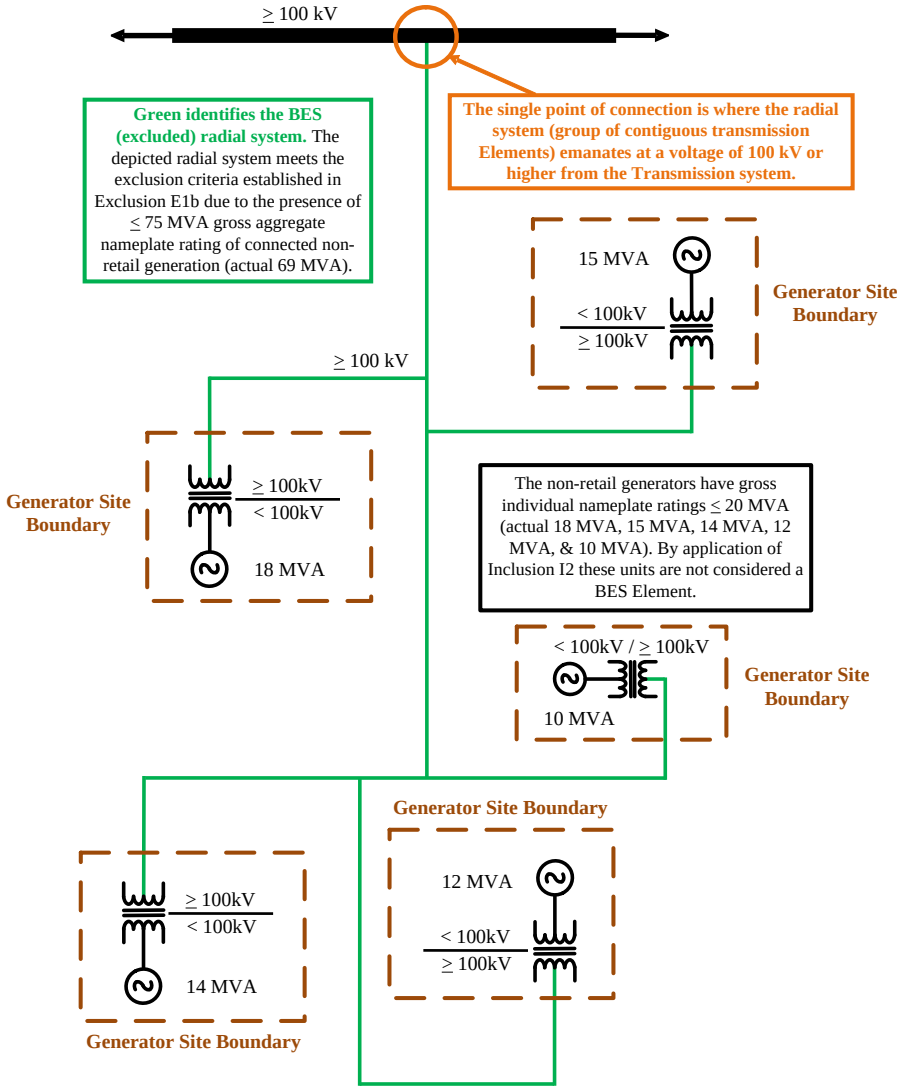


Figure E1-9: Radial System: Multiple (non-BES) Generation Resources (Non-Retail)

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

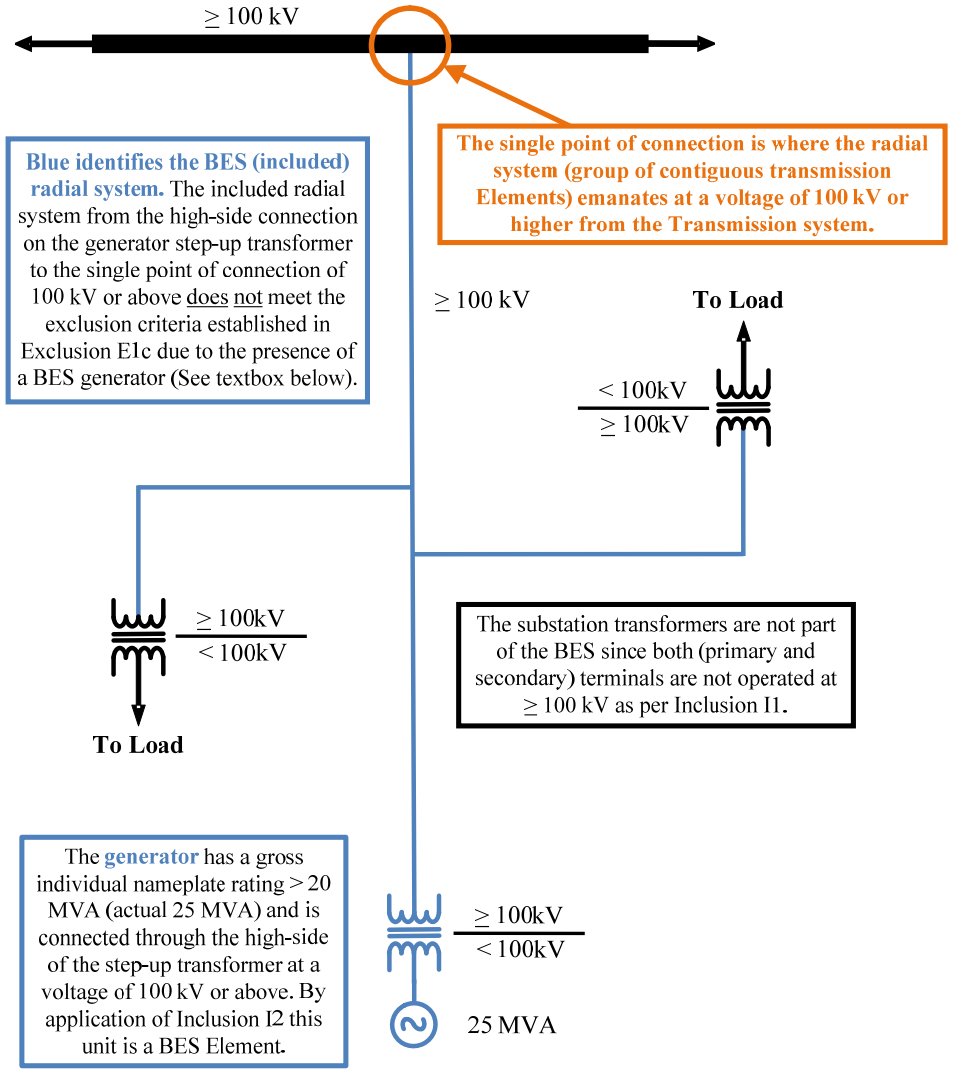


Figure E1-11: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

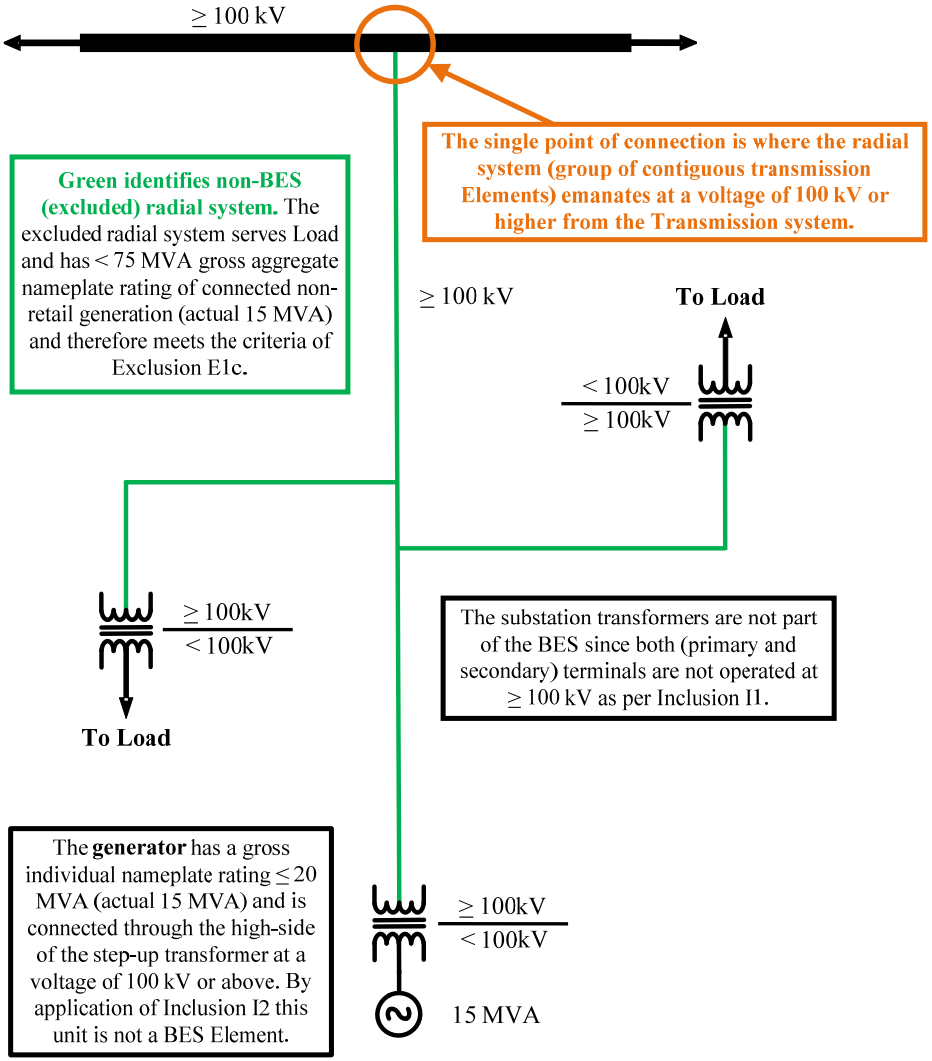


Figure E1-12: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

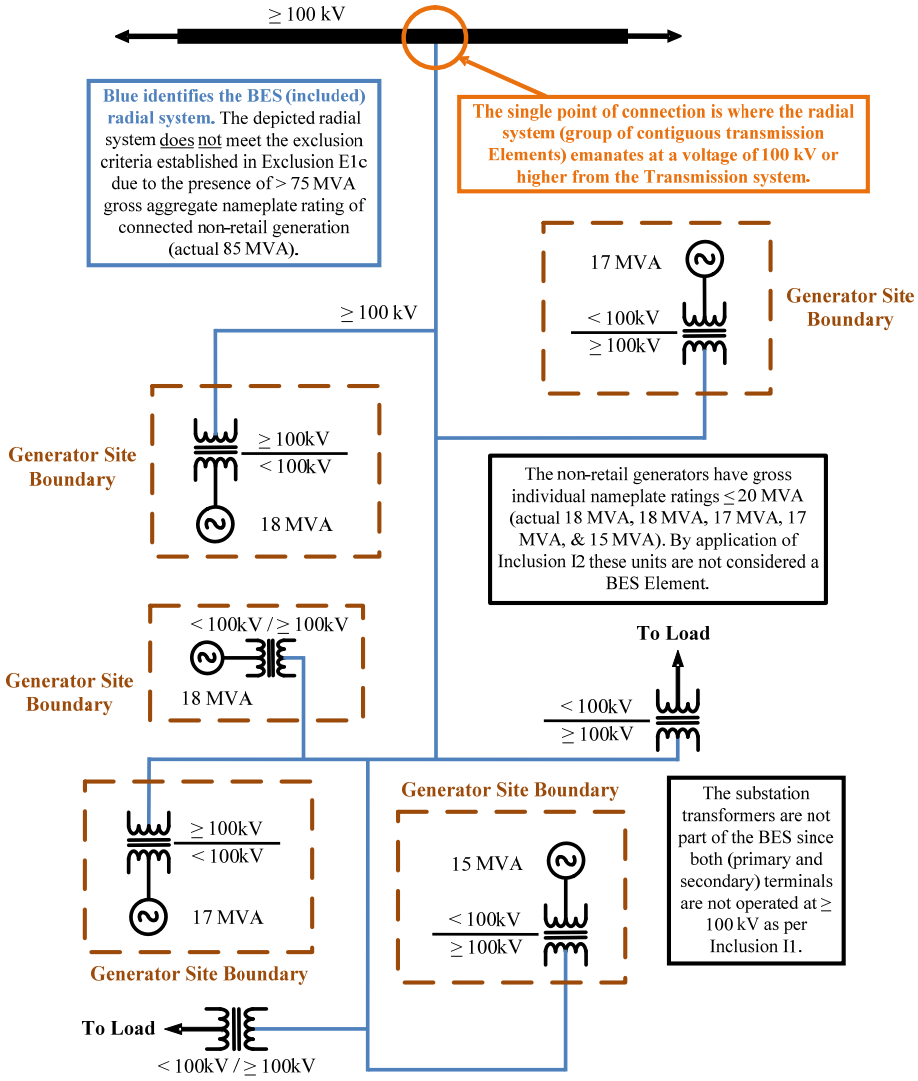


Figure E1-13: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

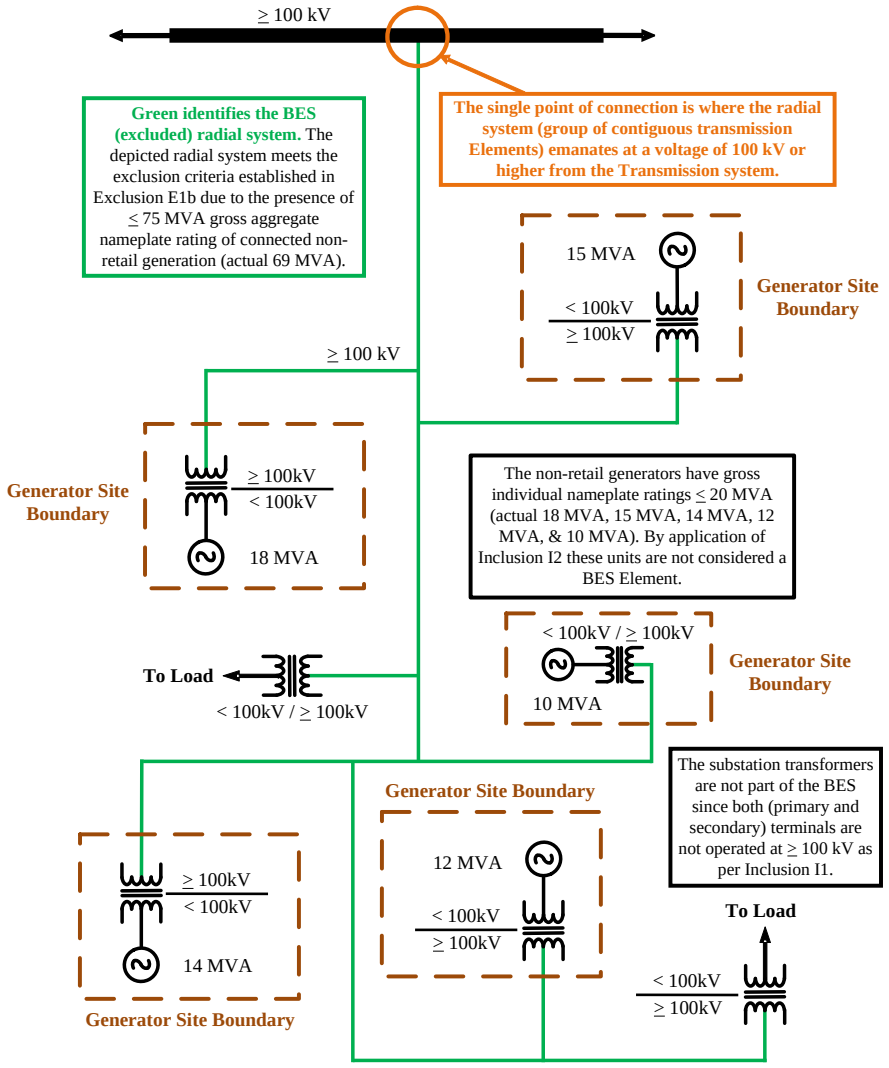


Figure E1-14: Radial System: Generation Resource (Non-Retail) & Serving Load

Exclusion E1 Radial Systems
E1.c Generation and Serves Load

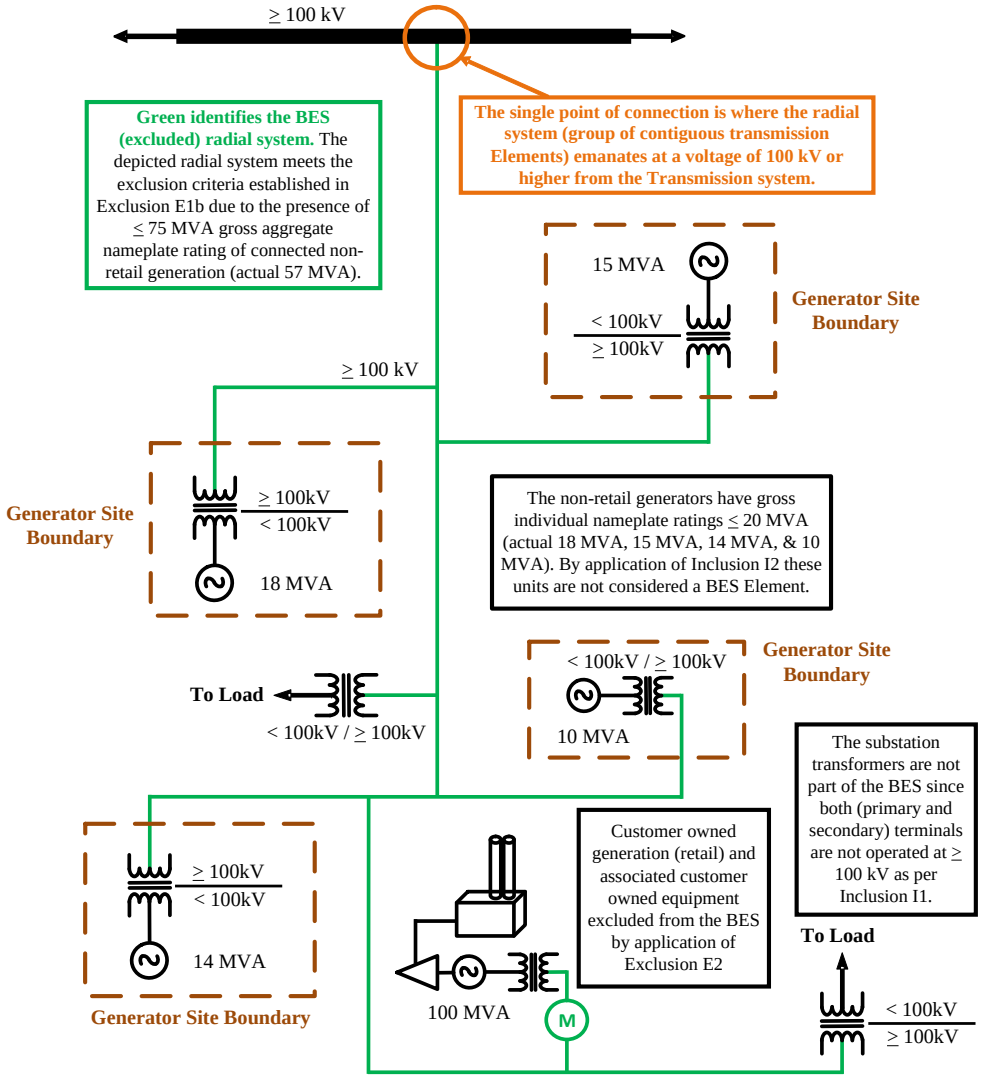


Figure E1-15: Radial System: Generation Resource (Retail & Non-Retail) & Serving Load

Exclusion E1 Radial Systems Normally OPEN Switching Device

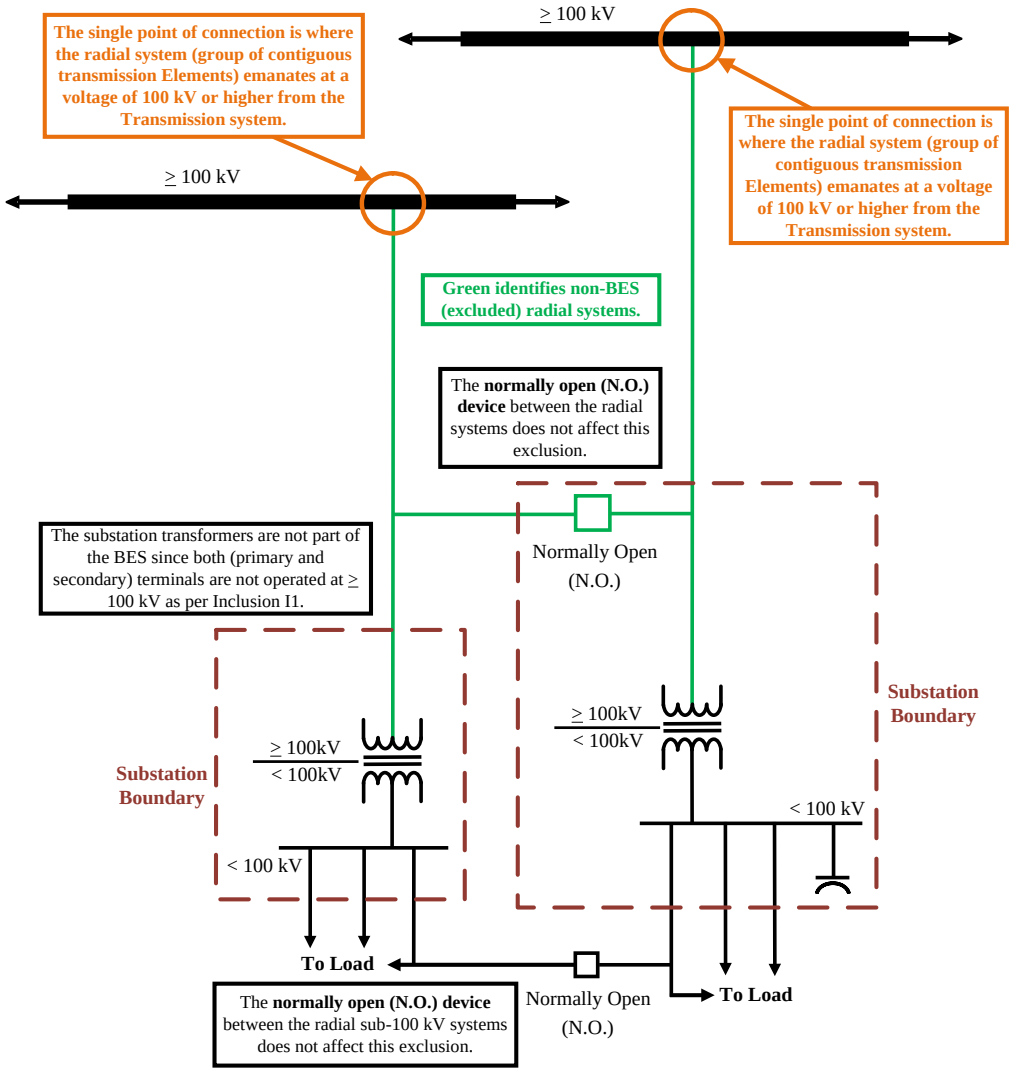


Figure E1-16: Radial System: Normally Open Switching Device between Load Serving Radial Systems

Exclusion E1 Radial Systems Underlying Loops

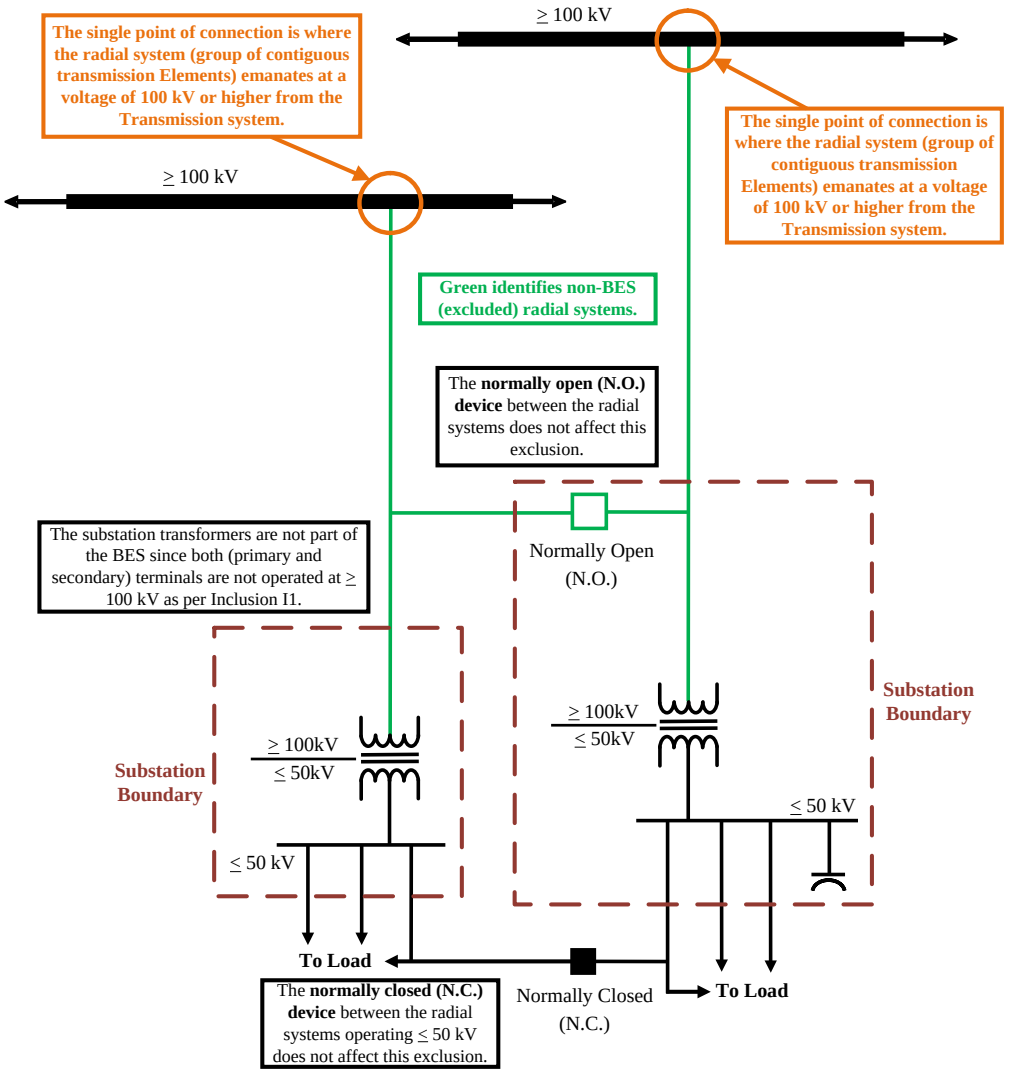


Figure E1-17: Radial System: Normally Open Switching Device between Load Serving Radial Systems with a < 50 kV Loop

Exclusion E1 Radial Systems Underlying Loops

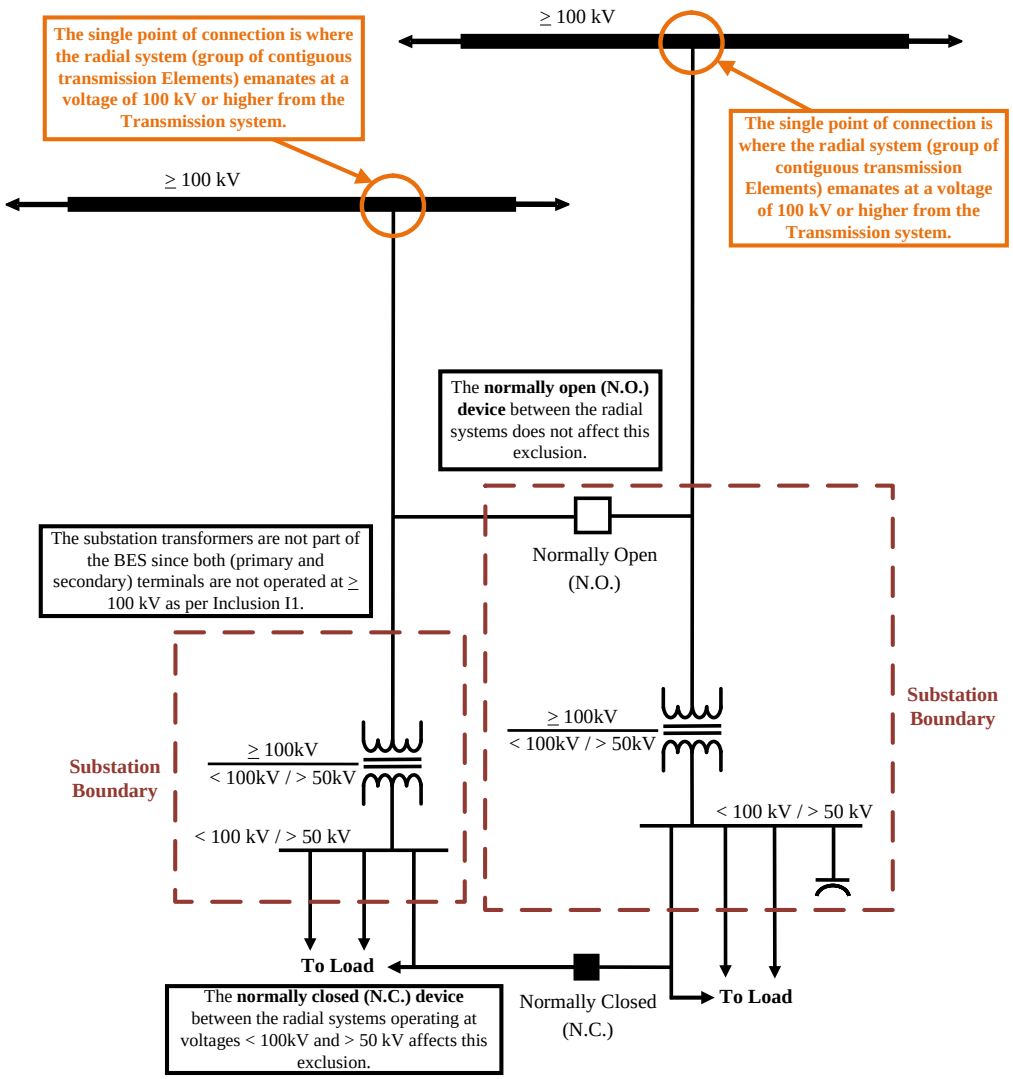


Figure E1-18: Impact of Sub-100 kV Looped Facilities (Switching Devices Identified N.O. > 100 kV & N.C. < 100 kV & > 50 kV)

Exclusion E1 Radial Systems Underlying Loops

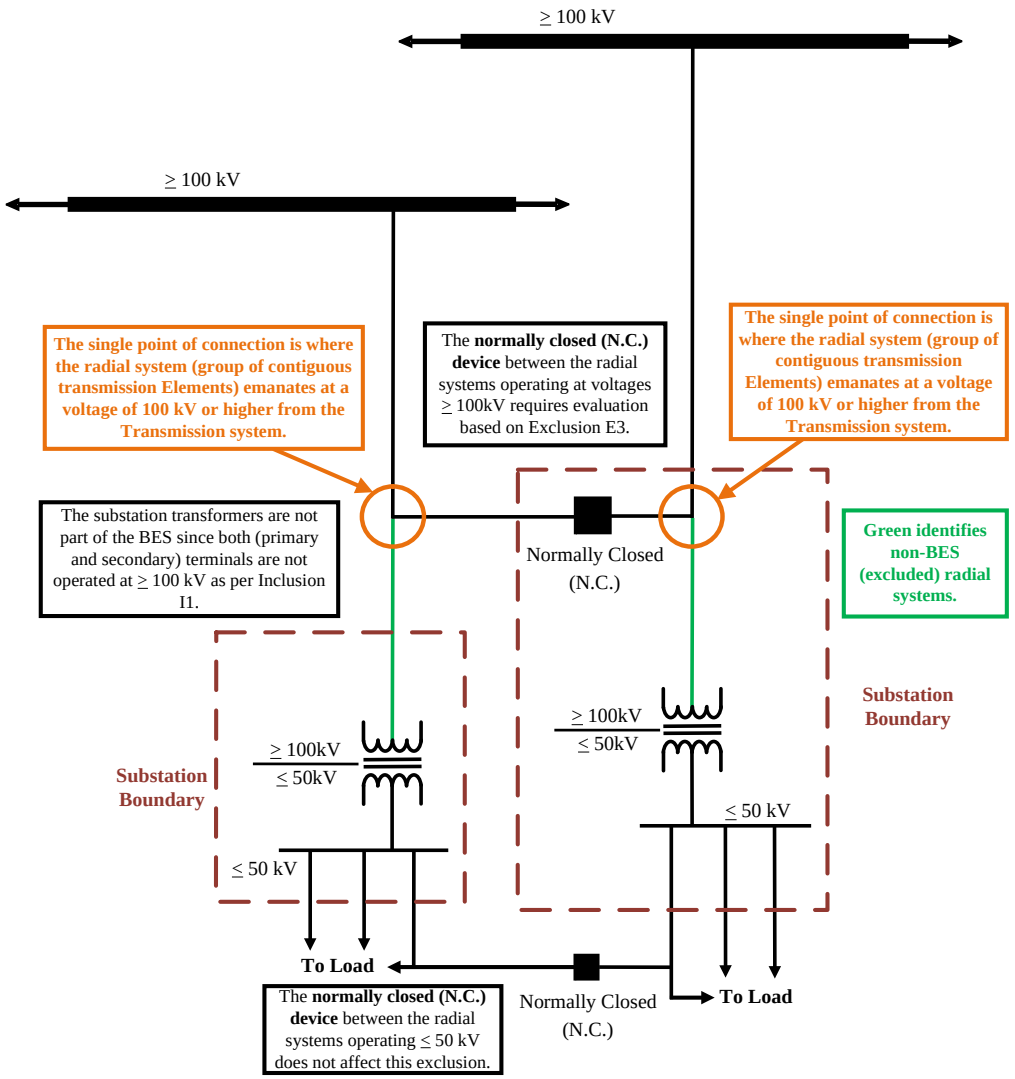


Figure E1-19: Radial System: Normally Closed Switching Device (> 100 kV) between Load Serving Radial Systems with a < 50 kV Loop

Exclusion E1 Radial Systems Underlying Loops

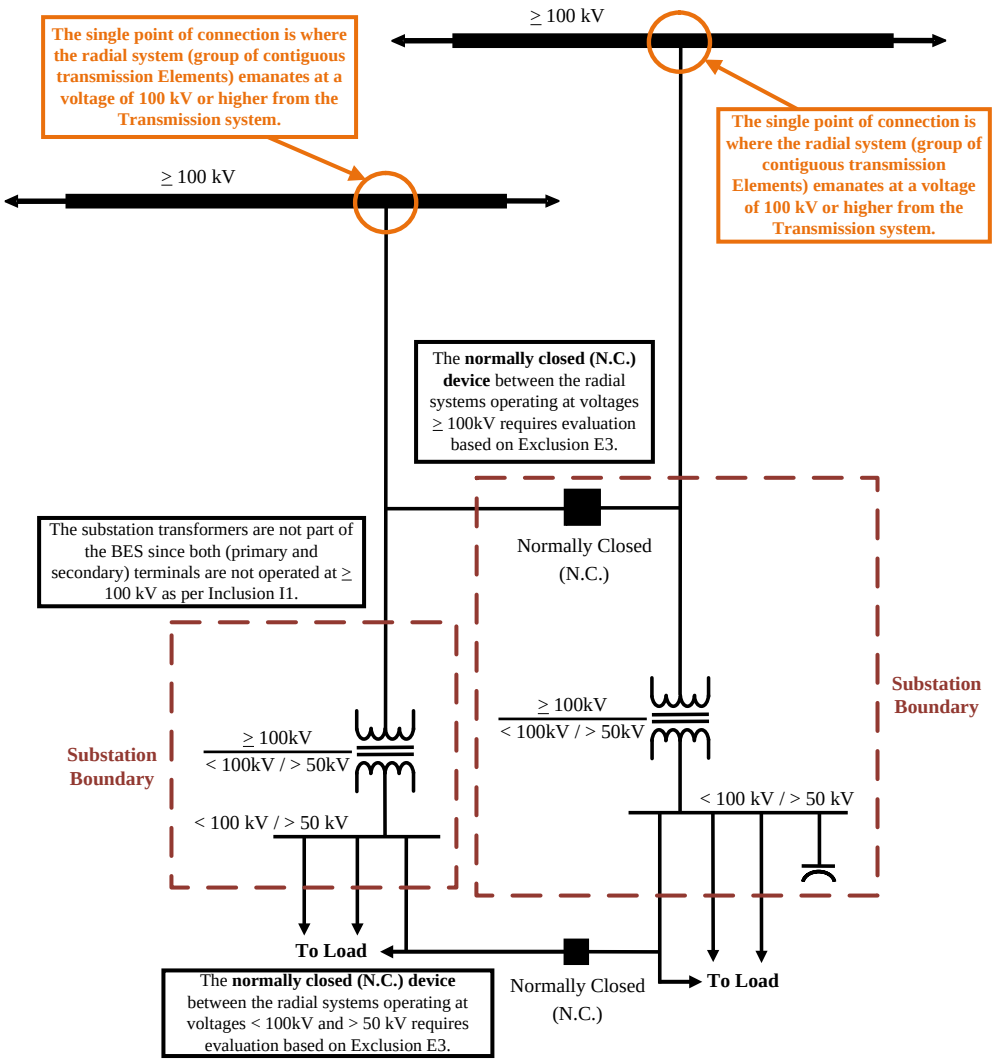


Figure E1-20: Impact of Sub-100 kV Looped Facilities (Switching Devices Identified N.C. > 100 kV & N.C. < 100 kV & > 50 kV)

EXCLUSIONS
E2

Exclusion E2 Behind-the-Meter Industrial Generation

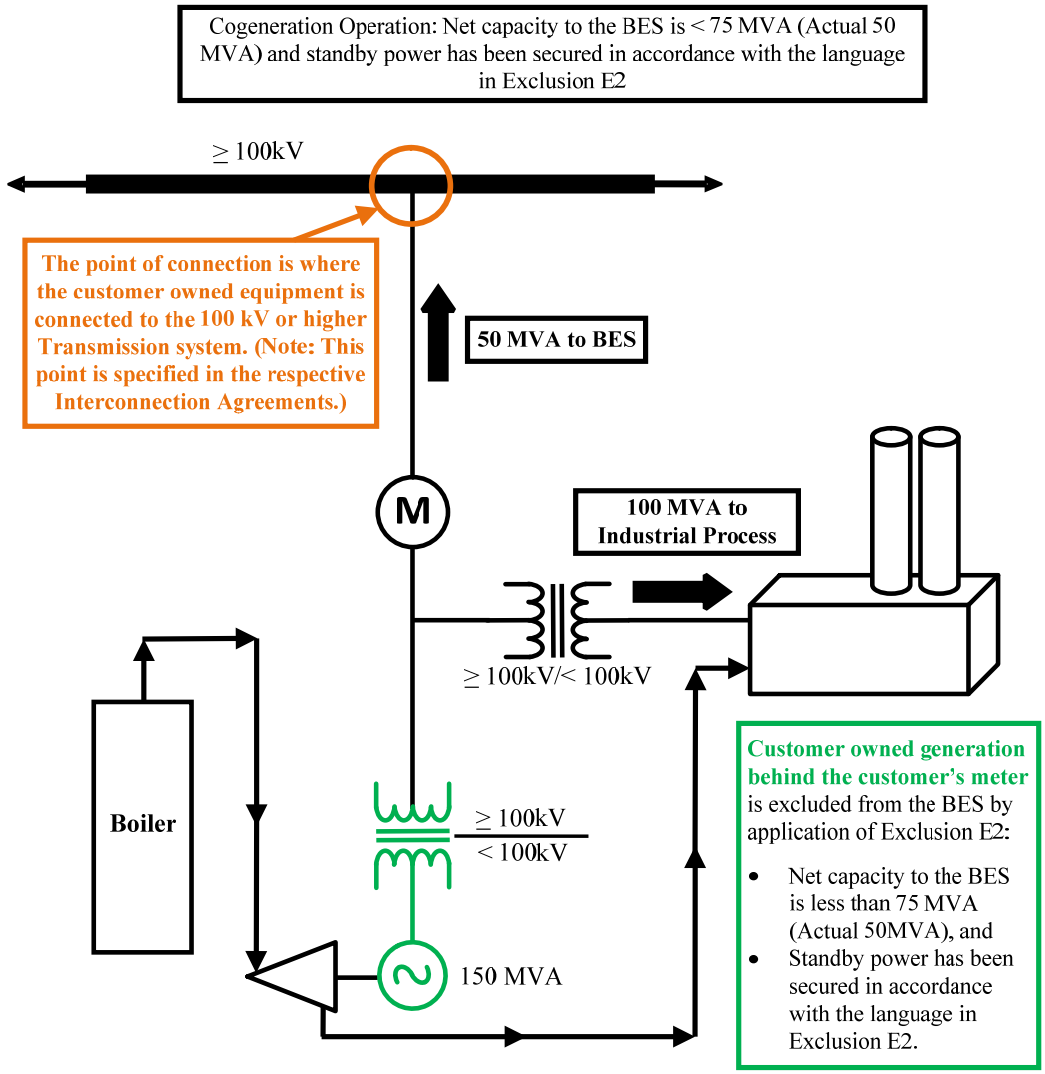


Figure E2-1: Behind-the-Meter Generation: Net Capacity to the BES Less Than 75 MVA

Exclusion E2 Behind-the-Meter Industrial Generation

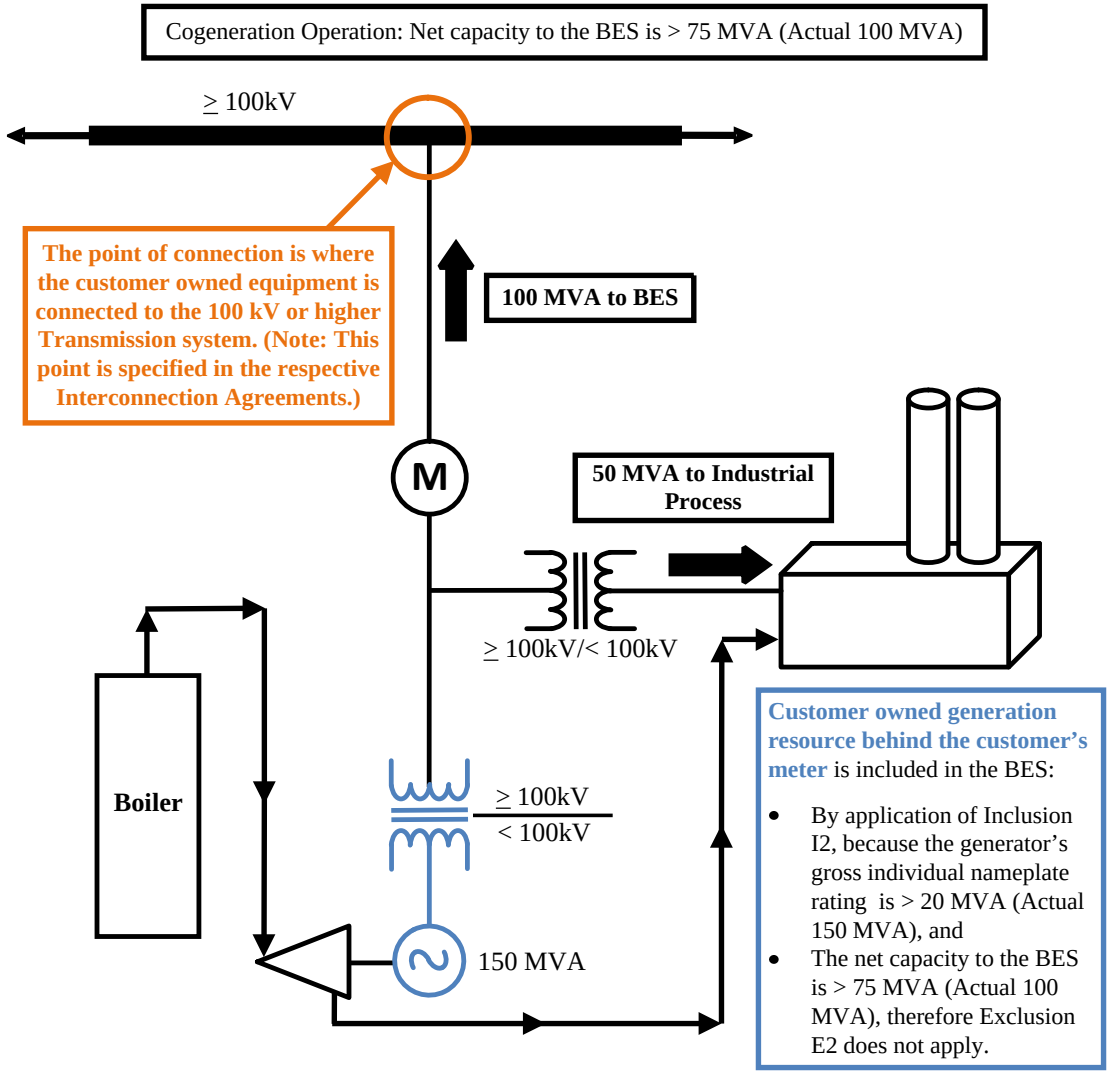


Figure E2-2: Behind-the-Meter Generation: Net Capacity to the BES Greater Than 75 MVA

EXCLUSIONS
E3

Exclusion E3 Local Networks

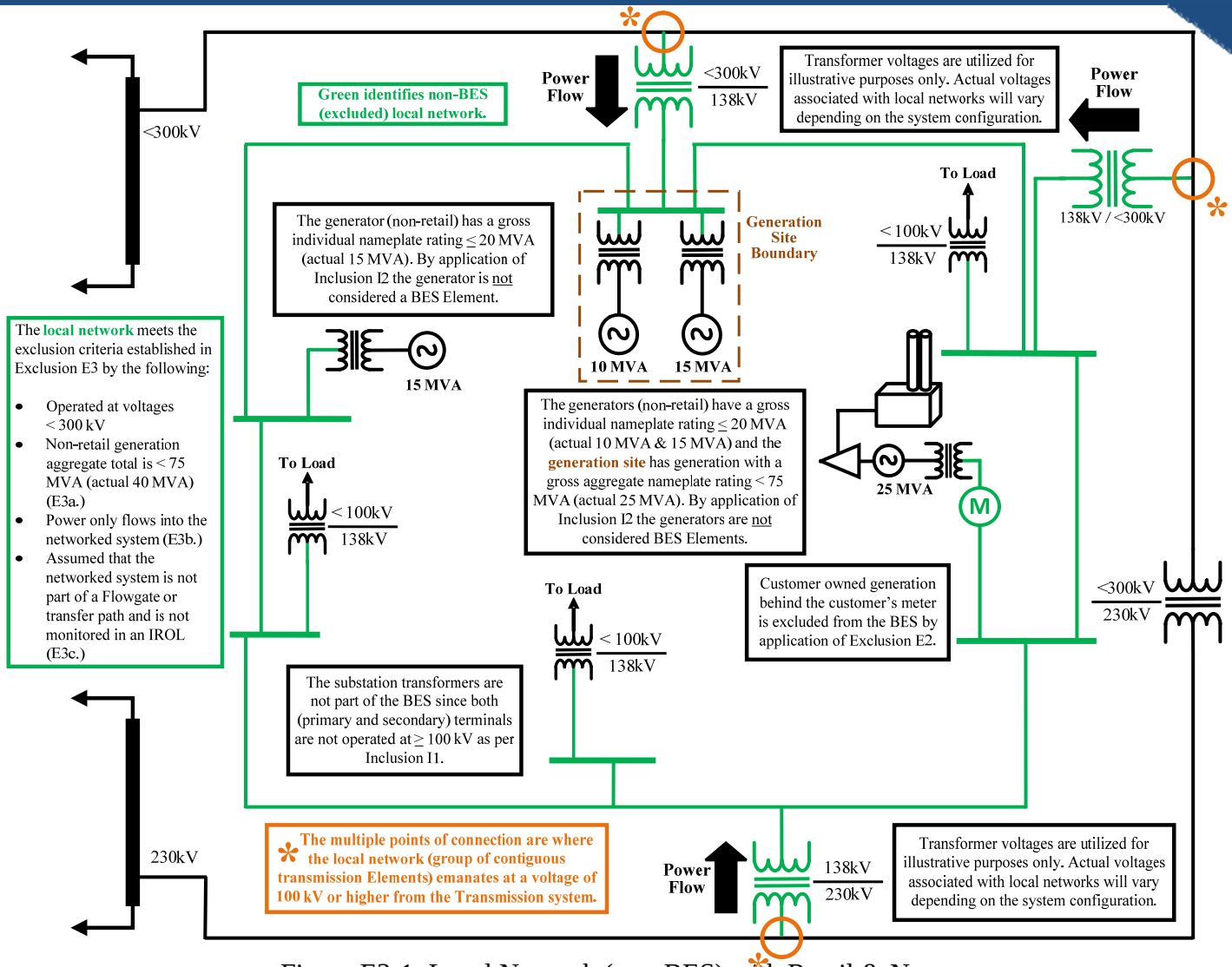
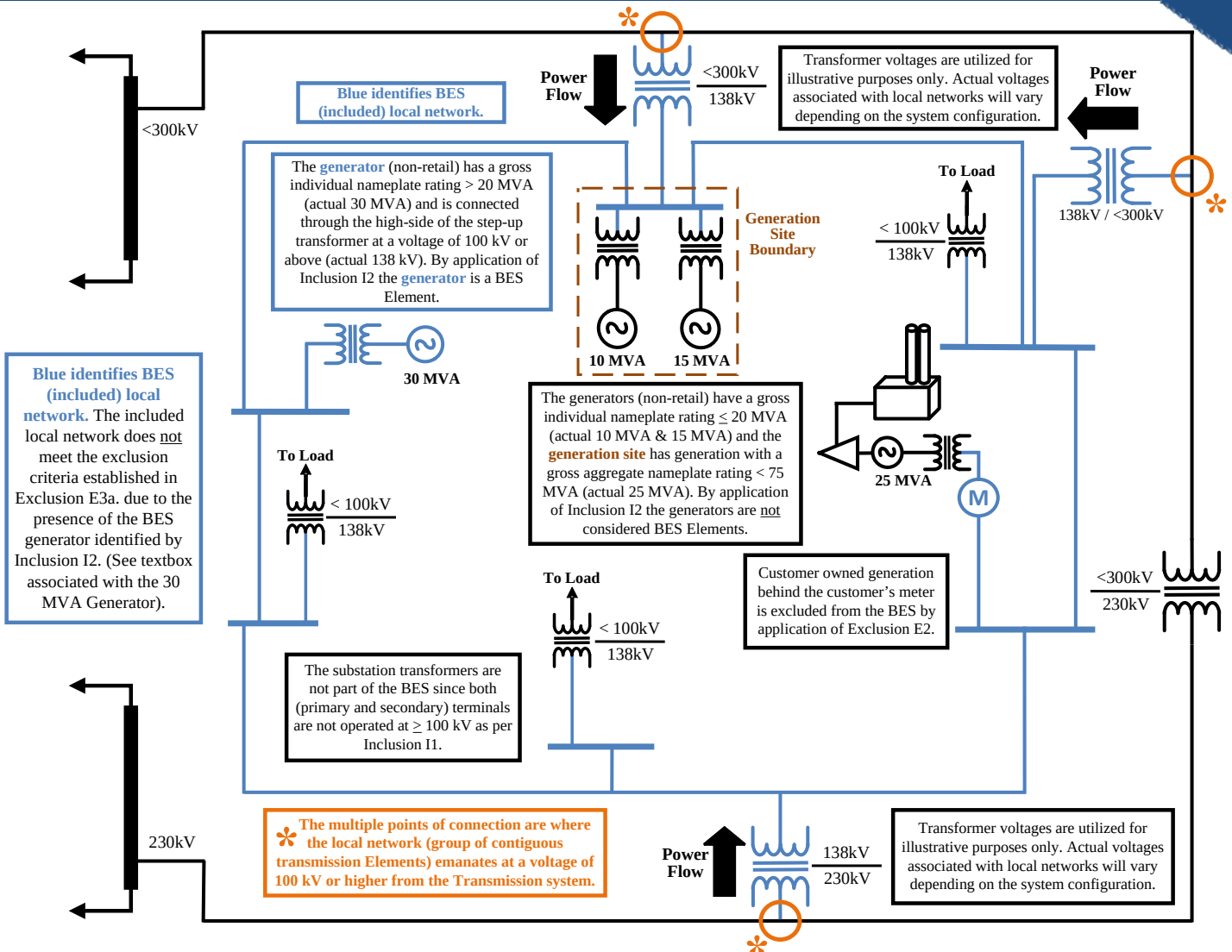


Figure E3-1: Local Network (non-BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks



E3-2: Local Network (BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks

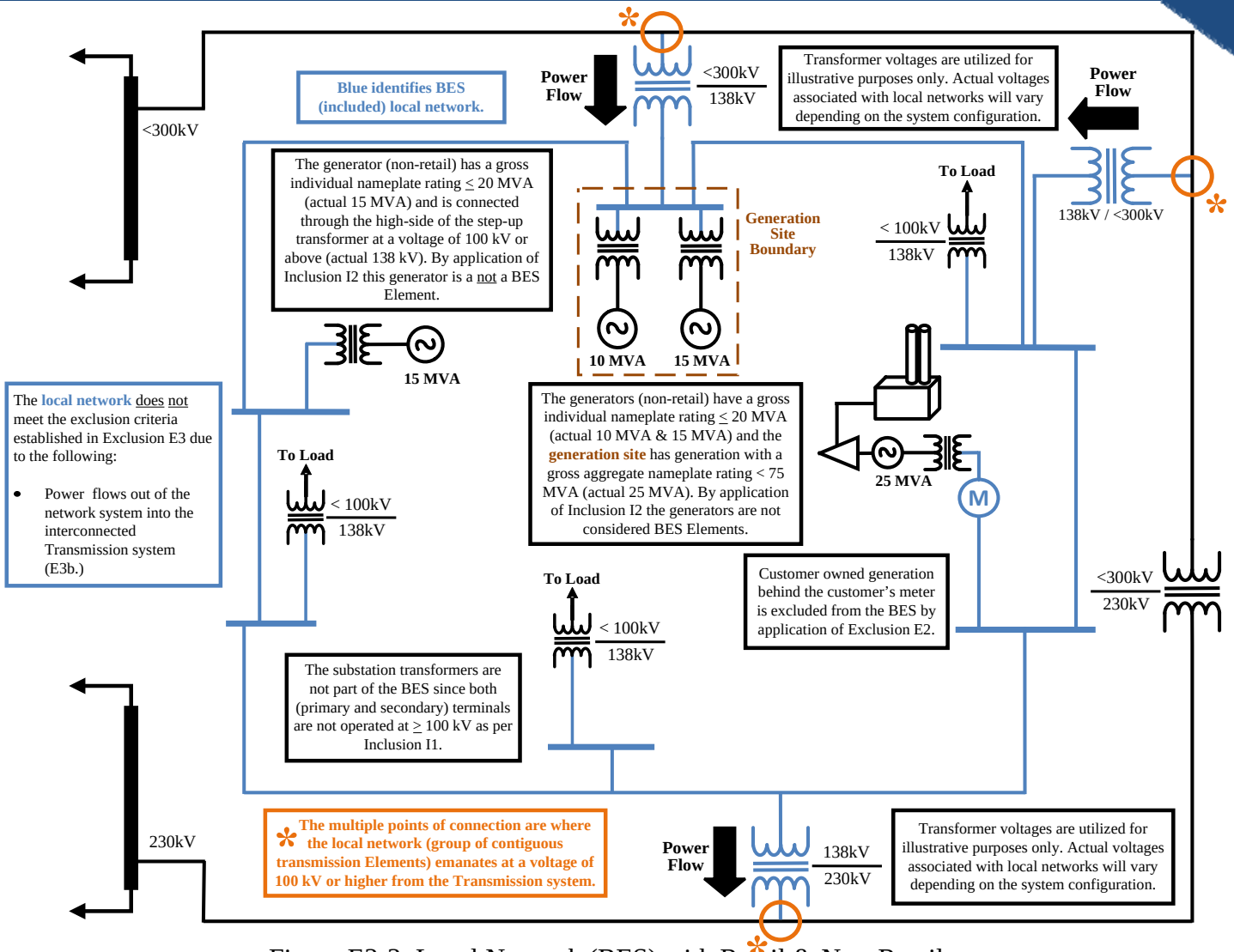


Figure E3-3: Local Network (BES) with Retail & Non-Retail Generation Resources & Serving Load

Exclusion E3 Local Networks

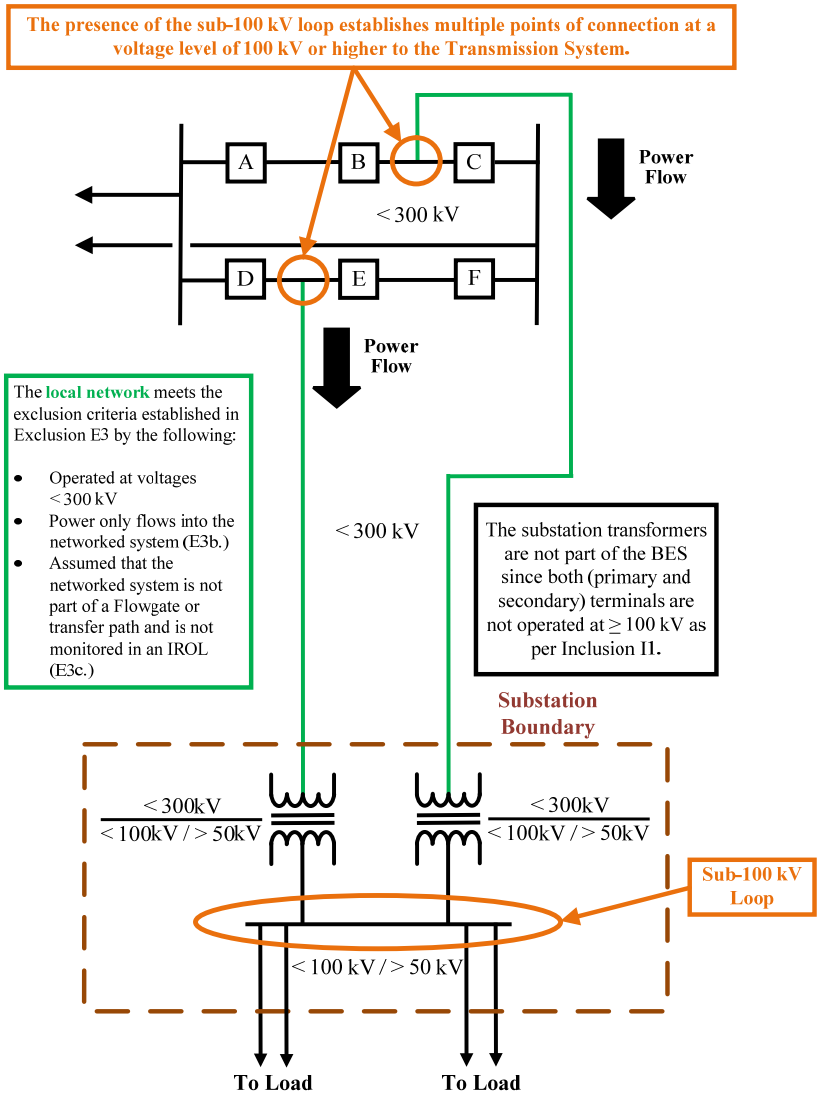


Figure E3-4: Local Network (non-BES) with Sub-100 kV Loop

Exclusion E3 Local Networks

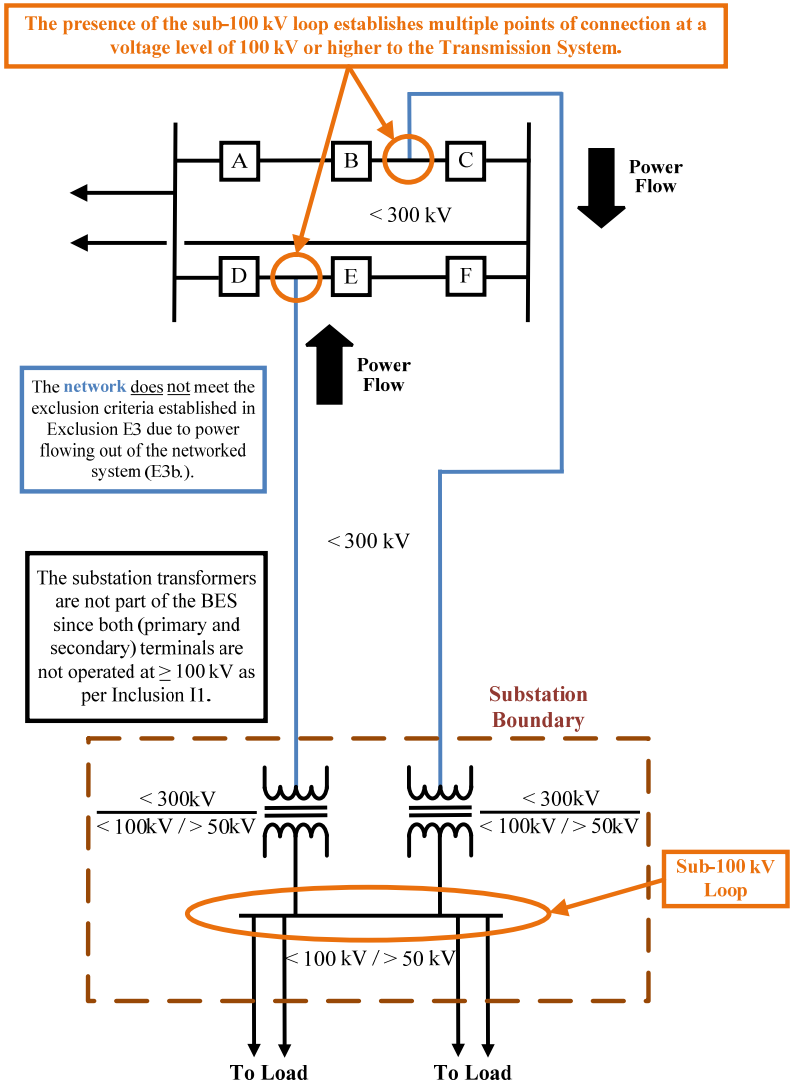


Figure E3-5: Local Network (BES) with Sub-100 kV Loop

Exclusion E3 Local Networks

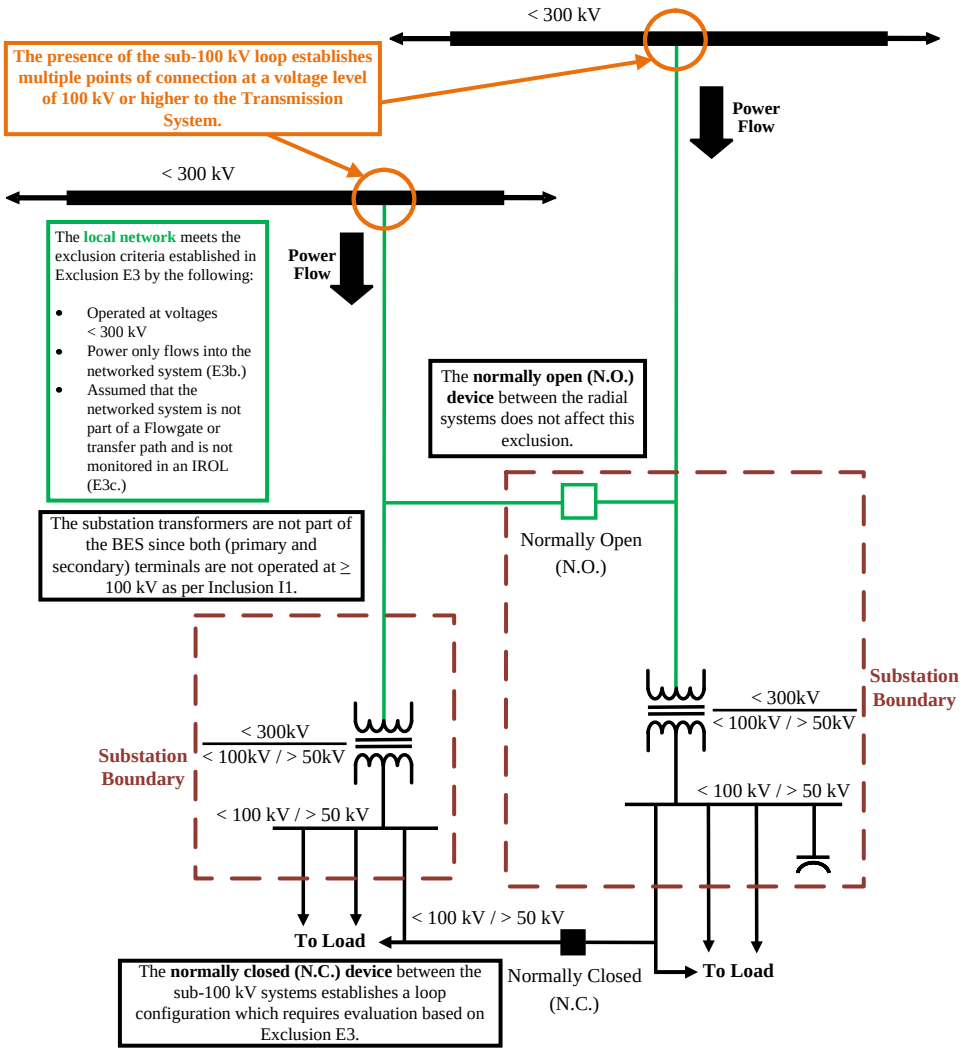


Figure E3-6: Local Network (non-BES) with Sub-100 kV Looped Facilities
(Switching Devices Identified: N.O. > 100 kV & N.C. < 100 kV/> 50 kV)

Exclusion E3 Local Networks

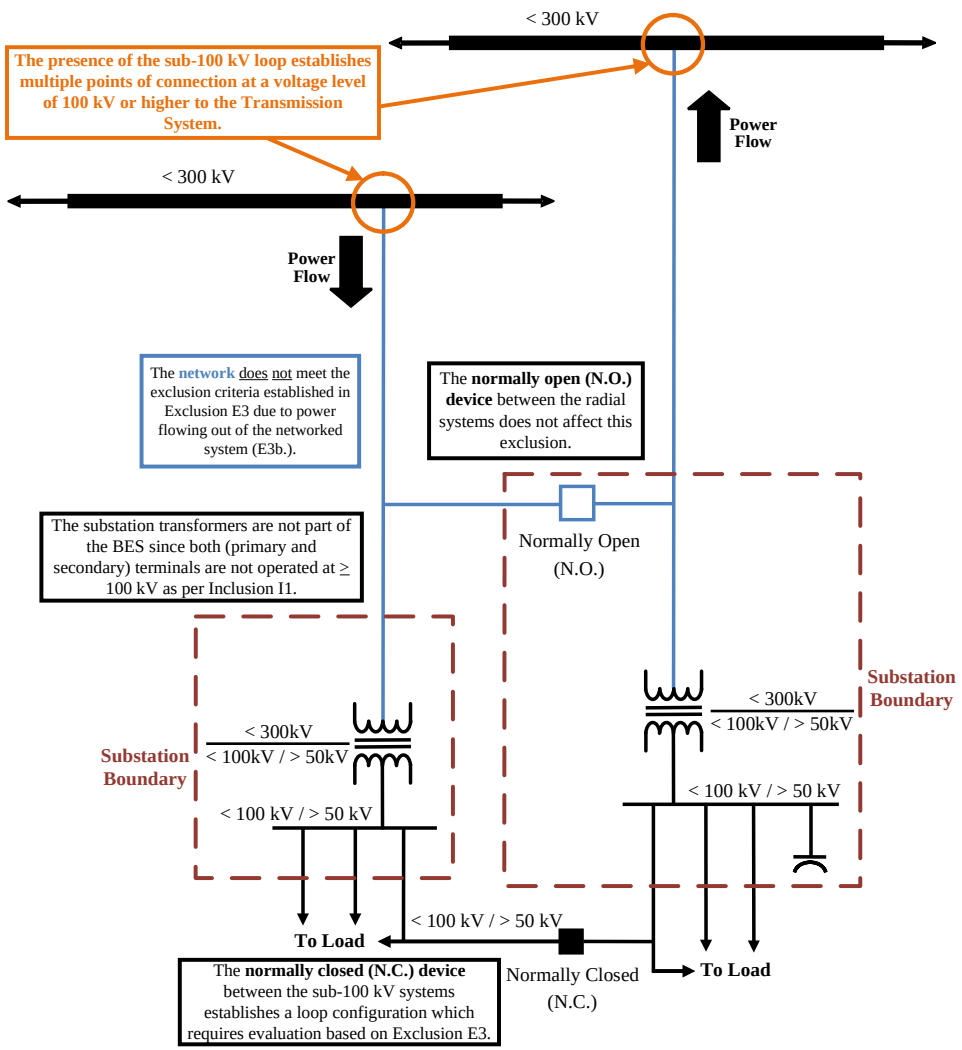


Figure E3-7: Local Network (BES) with Sub-100 kV Looped Facilities
(Switching Devices Identified: N.O. > 100 kV & N.C. < 100 kV/< 50 kV)

Exclusion E3 Local Networks

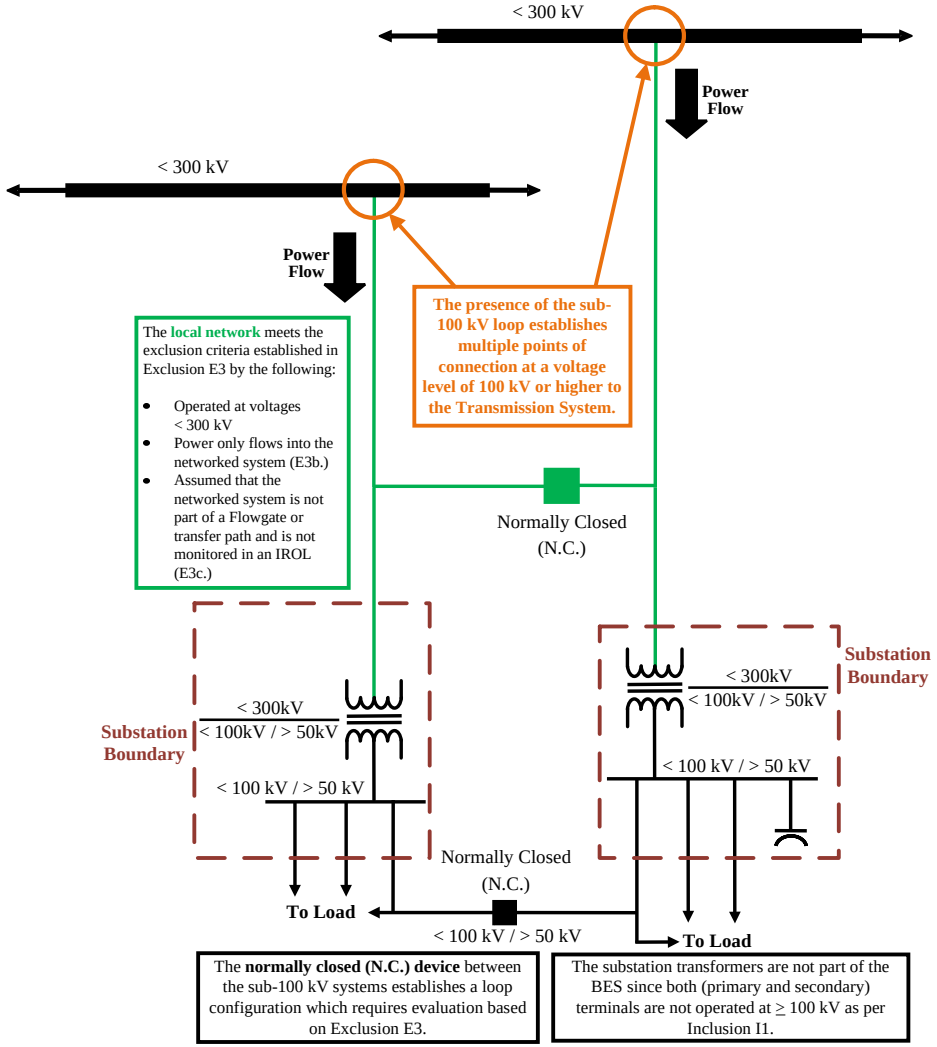


Figure E3-8: Local Network (non-BES) with Sub-100 kV Looped Facilities (Switching Devices Identified: N.C. > 100 kV & N.C. < 100 kV/> 50 kV)

Exclusion E3 Local Networks

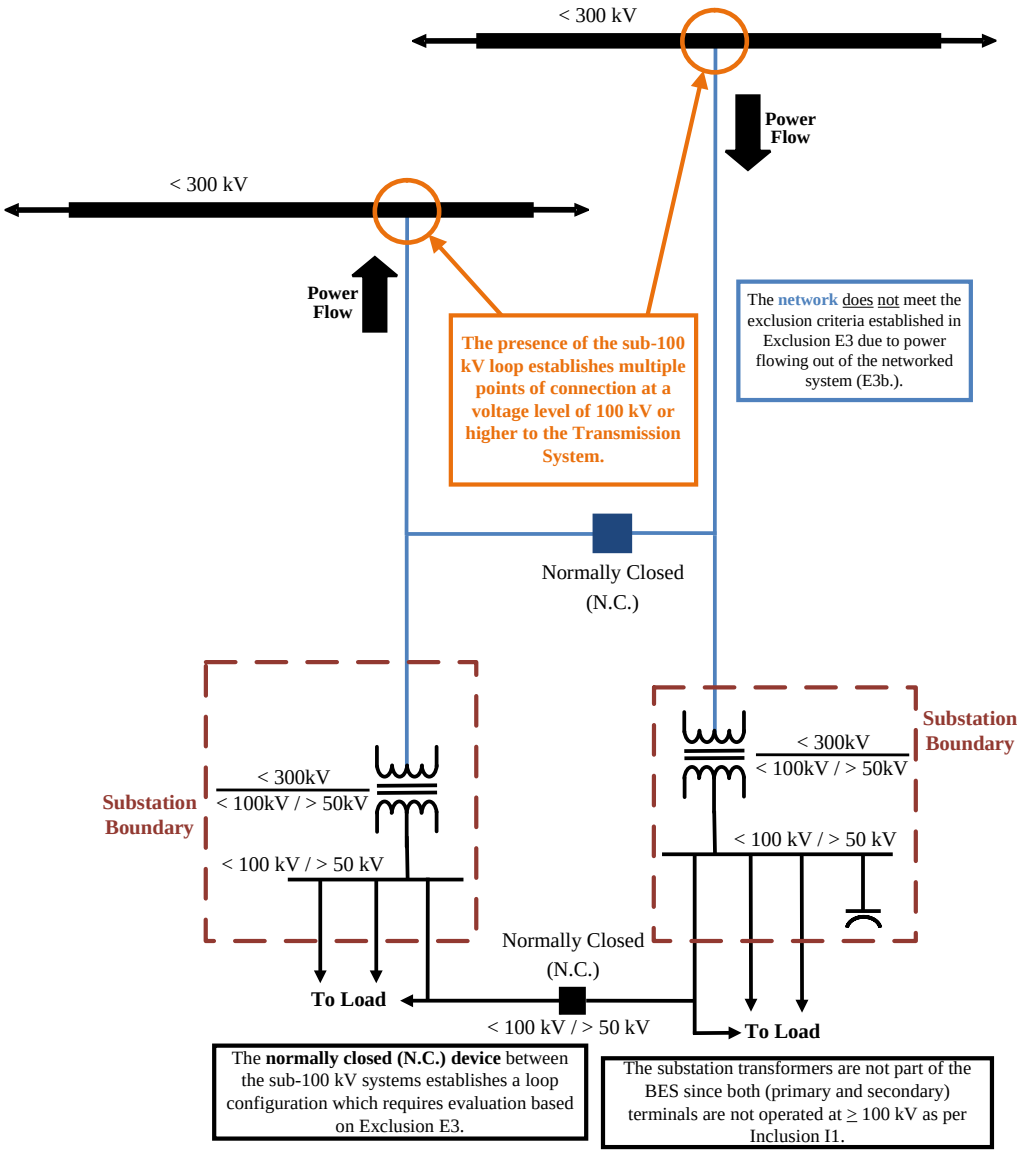


Figure E3-9: Local Network (BES) with Sub-100 kV Looped Facilities (Switching Devices Identified: N.C. > 100 kV & N.C. < 100 kV/> 50 kV)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BESnet

Tool Training for Registered Entities

Justin Lofquist
NERC Project Manager

RELIABILITY | ACCOUNTABILITY






Actions



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

Actions (cont.)



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

Agenda

- Application Overview (:05 - :15)
- Exception Requests (1:20 – 1:00)
  - Creation (:20 – :30)
  - Initial Review and Appeal (:30 – :35)
  - Substantive Review (:35 – :45)
  - Proposed and Final Decisions (:45 – :50)
  - Challenges, Certification and Change (:50 – 1:00)
- Break (1:00 – 1:10)
- Notifications of Self-Determination (1:10 – 1:30)
  - Submission (1:10 – 1:20)
  - Regional Review (1:20 – 1:30)
- Questions and Answers (1:30 – 2:00)

Resources

- BESnet Registered Entity User Guide
  - http://www.nerc.com/pa/rapa/pages/bes.aspx -> Resource Documents -> BES Notification and Exceptions Tool (BESnet)
- Support
  - http://www.nerc.com/pa/rapa/pages/bes.aspx -> Resource Links -> Regional Entity Contacts
- BESnet Training videos
  - http://www.nerc.com/pa/rapa/pages/bes.aspx -> Resource Links -> Training Videos
    - *User Account Management*
    - *Creating an Exception Request*
    - *Appealing a Rejected Exception Request*
    - *Substantive Review Process*
    - *User Account Management*
    - *Proposed and Final Decisions*
    - *Exception Request in Certification*
    - *Notification of Self-Determination*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Questions?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BESnet Release Notes August 8, 2014 and August 13, 2014

Introduction

The list below contains a list of known defects for the August 8, 2014 and August 13 releases of BESnet.

Known Defects

Known Defects			
ID	**Area**	**Description**	**Work-Around**
252	**Create Entity-Submitting Entity Role**	When creating an ER under section 1 there is an option of **YES** or **NO** in regard to if the Submitting entity is the owner of the elements. Once the **NO** option is selected a search option is displayed to select the owner and choose the submitting entity's role. If no owner is selected during the search, or if Submitting Entity Role(s) is chosen before the Owner, the selection will revert back to YES.	Click on the NO option again. All information (e.g. Submitting Entity Role) will be retained and displayed.
351	**ER - details**	When creating a SDN the "primary name" that gets populated in the Section 2 of the Notification gets automatically grabbed from the "From Point Name" field of the Edit Element screen? It would be more appropriate and user friendly to utilize either the "Common Element Name" or the "Circuit ID". This change has not been consistently applied throughout the UI.	No work around needed; will be cleaned up in a future release.
395	**Reports**	The export report Stage column is not showing text in all cases; in some, it is displaying a numerical value.	No work around needed at this time; will be cleaned up in a future release.
401	**Reports**	In several reports, Primary voltage and secondary voltage is showing 'HVDCxxx' where 'xxx' is the actual voltage.	For numerical voltages, ignore or trim the HVDC from the front of the value.
414	**ER Creation**	When the user removes the Associated Entity, the NCR shows up in a pull-down box. This text should be static.	No impact; will be addressed in a future release.

420	**Substantive Review**	The display strips CRLFs from the comments (e.g., if I enter 'Comment 1 <crlf> comment 2, 'it retains that when in a text box, but when displayed as 'label' text, it displays as 'Comment1 comment 2' (all on one line).	No work around needed.
422	**ER**	When adding a SOR, when you click back from the entity selection screen, the system takes you to the dashboard-not to the ER.	Manually go back into the ER
423	**ER**	If the phone number is not filled in correctly, the ER will not save.	Enter phone number correctly in the field provided.
485	**Initial Review-Rejected**	Once an ER is created and it is rejected by the region, the Initial Review documents cannot be read on the Decision tab (i.e. the hyperlink is disabled) for the Submitting Entity or the Owning Entity. The hyperlink is available to the Lead Region.	Initial Review Documents are not available on the Docs tab when the ER is in a **Reject** status. Submit an **Appeal** (this sends the ER to **Reject-under appeal**) and the docs are then available under the Docs tab.

Bug Fixes / Enhancements since the Initial Release into Production

The list below contains the Bug Fixes and Enhancements since the first release of BESnet into Production.

Resolved Issues			
ID	**Area**	**Description**	**Additional Notes**
146	ER - Create	Added a question regarding Black Start service.	
208	**Challenge Response-UI**	When taking an action to approve/disapprove a challenge, the radial button popped up with 'OK' and 'Cancel' instead of the wording in the question. The pop up has been changed to reflect the following: *'Are you sure you approve/disapprove the challenge? 'Ok' and 'Cancel' button*	
267	**TRP - UI**	Changed label "There are no TRP's that can be assigned to this ER' to 'There are no TRP candidates available to be assigned to this exception Request'	

286	**Dashboard-next action**	When the next action = 'Challenge' is reflected; the date shown is the date for re-certification. The date has been corrected to reflect the 'Challenge' date.	
329	**Entity Management**	BESnet was not allowing Canadian zip codes to be reflected in the application. This issue has been corrected and Canadian zip codes are being reflected in the application.	
330	**Entity Management**	Unable to modify entity role (e.g. submitting, BA). This has been corrected.	
332	**User Management-Vetting**	When adding an entity to a user's profile, a success message was returned when the check box to add entity is not checked and the **Save** button is clicked (meaning no entity was selected to be added). A validation rule was added to catch this error.	
356	**ER-Create**	Incorrect text when removing BES Definition Basis. The statement has been updated to reflect the following: 'Remove BES Definition Basis'	
368	**Dashboard**	The status of an ER (approved or disapproved) is being concatenated to the 'Stage' but not to the 'Status'. Overall changes to clarify state, status, and the use of filters were applied.	
376	**Reports**	The 'back' button on reports was not working. This has been corrected.	
377	**SDN**	NEW FUNCTIONALITY: SDNs cannot be submitted (review completed) by the Region or NERC unless all the elements are in the same state (for regions, accepted or rejected; for NERC concurred or conflicted). In cases where they are not in the same state, a validation rule will tell the user they must split them to make each SDN only contain elements in the same state.	
378	**SDN**	NEW FUNCTIONALITY: At the element level there is now a "pass" button next to 'concur' or 'conflict' to indicate when NERC elects not to review an SDN. The status can now be 'concur, conflict or pass'.	

379	**SDN**	NEW FUNCTIONALITY: The SDN will drop into SD in NERC review as soon as the region completes their initial review.	
380	**SDN**	NEW FUNCTIONALITY: The SDN is considered 'Archived' if NERC Concurs (Reject-Concur) with the regional rejection of the SDN. The term "Archived" has been be replaced with "Terminated."	
381	**SDN**	NEW FUNCTIONALITY: If NERC Passes (Reject-Pass) on the SDN (by clicking a new 'Pass' button within the SDN screen for NERC users), the SDN is considered 'Archived.' The term "Archived" has been be replaced with "Terminated."	
382	**SDN**	NEW FUNCTIONALITY: If NERC Conflicts (Reject-Conflicted) with the regional rejection of the SDN, the SDN is considered 'Certified'.	
383	**SDN**	NEW FUNCTIONALITY: If NERC Concurs (Accept-Concur) with the regional acceptance of the SDN, the SDN is considered 'Certified'.	
384	**SDN**	NEW FUNCTIONALITY: If NERC Passes (Accept-Pass) on the SDN (by clicking a new 'Pass' button within the SDN screen for NERC users), the SDN is considered 'Certified'	
385	**SDN**	NEW FUNCTIONALITY: If NERC Conflicts (Accept-Conflicted) with the regional acceptance of the SDN, the SDN is considered 'Archived.' The term "Archived" has been be replaced with "Terminated."	
386	**SDN**	NEW FUNCTIONALITY: The system shall have the following Status: NEW RE Review Complete (accepted/rejected); NERC Review Complete + (accepted/rejected, based on concatenation of both RE and NERC review	Overall changes to clarify state, status, and the use of filters were applied.
387	**SDN**	NEW FUNCTIONALITY: The system shall have the following Stages: Regional Review, NERC review and <Blank>.	Overall changes to clarify state, status, and the use of filters were applied.
397	**SDN**	General clean- up of the UI needed to ensure consistency and accuracy- the SDN screen still shows 'Exception Request' labels. These incorrect references were removed.	

398	**SDN Regional Review**	The language under the Elements tag of a SDN was corrected to align with the buttons (the Region Status in the grid should be 'Accepted' not 'Approved'.	
400	**Dashboard**	The dashboard was changed to include abbreviated types to SDN and ER (SDN-I and SDN-E, ER-I and ER-E).	
402	**Reports**	The 'IsRF' flag in the export report has been changed to "IsRFC," and now accurately reflects the status..	
404	**Reports**	The internal and external IDs were added to the Export reports.	
405	**Reports**	The 'Elements' Report was not displaying the 'Current BESnet Definition Status'; this has now been fixed.	
406	**Reports**	The Excel Export report is only exporting 100 characters for text fields. We have expanded this to allow for more data to be shown.	
407	**Reports**	'Is Rejected' and 'Is Approved' values displaying incorrectly in export report. The report was fixed and data is reflecting as needed.	
408	**Splits**	NEW FUNCTIONALITY: The ability to split an SDN in 'NERC Review' was enabled.	
409	**ER, SDN**	The 'Elements' table in the Documents tab was removed. This table was removed as it caused problems for entities including lots of elements in a single submission.	
410	**Reports**	An Administrative version of the Element Export report was created for the NERC admin role.	
411	**SDN Printed Report**	The primary and secondary voltages reported on the summary were incorrect. This has been corrected to display the correct voltages.	Known defect 401 applies; voltage is displayed as HVDCxxx, where xxx is the correct voltage.
412	**ER/SDN**	The Counter used to create the last five digits of the ER identifier was based on record counts, and incorrectly assigned the same number to multiple requests. This resulted in an error display to the user. The counter has been modified to eliminate this problem.	Note that if an SDN or ER is returned to draft, when it is resubmitted, it will be assigned a NEW ID.

413	**Reports**	An Administrative version of the ER Export report was added for the NERC Admin role.	
429 **Z#619**	**Element Export (Production Issue)**	Data reflected in the Element Report was inaccurate. The report has been corrected to ensure the correct data is being displayed.	
432	**Reports**	The System Administrator was given access to view the Full data reports from the UI.	
433	**UI**	The address on the Help Link in BESnet was changed to reflect: http://www.nerc.com/pa/RAPA/Pages/BESnetHelp.aspx	
486 **Z# 640**	**SDN**	An attempt was made to create a notice of Self Determination for Potomac Electric Company which has a Washington DC address. Drop down menu for states did not contain DC as a selection.	The District of Columbia and Canada were added to the drop down menu for address information.
xxx	**Add Element**	Changes were made to the labels related to ratings. MVA Rating- For Element Types, field and optionality was modified as follows: GEN (Gross Nameplate Rating in MVA, Req'd) CKT (Normal Rating in MVA, Req'd DC Conv (Normal Rating in MVA, Req'd) Shunt (Normal Rating in MVAR, Req'd) Network (NA, Not Req'd)	
yyy	**Add Element**	ID- For Element Type Circuit, ID (Circuit ID) was changed to be a required field.	
SSF	**Terminated filter**	Incorrect assignment/filtering of a Challenged ER was corrected.	
SSF2	**Challenge filters**	The UI was adjusted to make 'Challenge' and filter information clear (i.e., show the decisions made during the challenge phase).	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BESNet Training Manual

Pre-Implementation Account Management and Self-Determined Notifications for Registered Entities

June 18, 2014
Version 1-1

RELIABILITY | ACCOUNTABILITY






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

Table of Contents

Introduction 3
BESNet Program Cautions 4
Version History 5
User Account Management 6
Introduction 6
Creating a New Account 6
Creating Account Step 1: User Name and Password 6
Creating Account Step 2: Verify Account 8
Logging Into the BESNet Application 10
Selecting the User's Entity to Use 11
Setting up Your BESNet Application Account 12
Account Setup Step 1: Select Account Type 12
Account Setup Step 2: Association of Account with Entities 13
Editing Your User Profile 16
Password Management 17
Changing User Password 17
Forgot/Resetting the User Password 18
Managing Your User Account Properties 21
Logging Out 22
Administrator User Account Management 23
Administrative User Management 23
Vetting New Users 23
User Role Management 24
BESNet Dashboard Overview 25
Notifications of Self-Determination 27
Creating a Notification of Self-Determination 27
Create Notification of Self-Determination Screen Section 1: General Information 27
Create Notification of Self-Determination Screen Section 2: Detailed Information 30
Adding an Element to a Notification of Self-Determination 31
Add Supporting Documentation for the Element 39
Certifying the Notification of Self-Determination 40
Submitting the Notification of Self-Determination 40

Introduction

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

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

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

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

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

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

BESNet Program Cautions

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

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

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

Version History

The following is the history of changes to this document.

Version	Date	Change(s) Made	Change Tracking
1-0	May 9, 2014	Initial Release – User Account Management Section only	
1-1	June 19, 2014	Incremental Release – Addition of Submittal of Self-Determined Notifications	

User Account Management

Introduction

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

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

When creating accounts, it is essential to make sure your Entity Administrator account is set up before any other accounts. Your Entity Administrator should be the person who is registered with NERC as your Primary Compliance Contact (PCC). Requesting accounts before the Entity Administrator account is set up will result in having to re-register those accounts later.

Creating a New Account

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

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

Creating Account Step 1: User Name and Password

Navigate to the following URL:

https://BESNET.EROENTERPRISE.COM

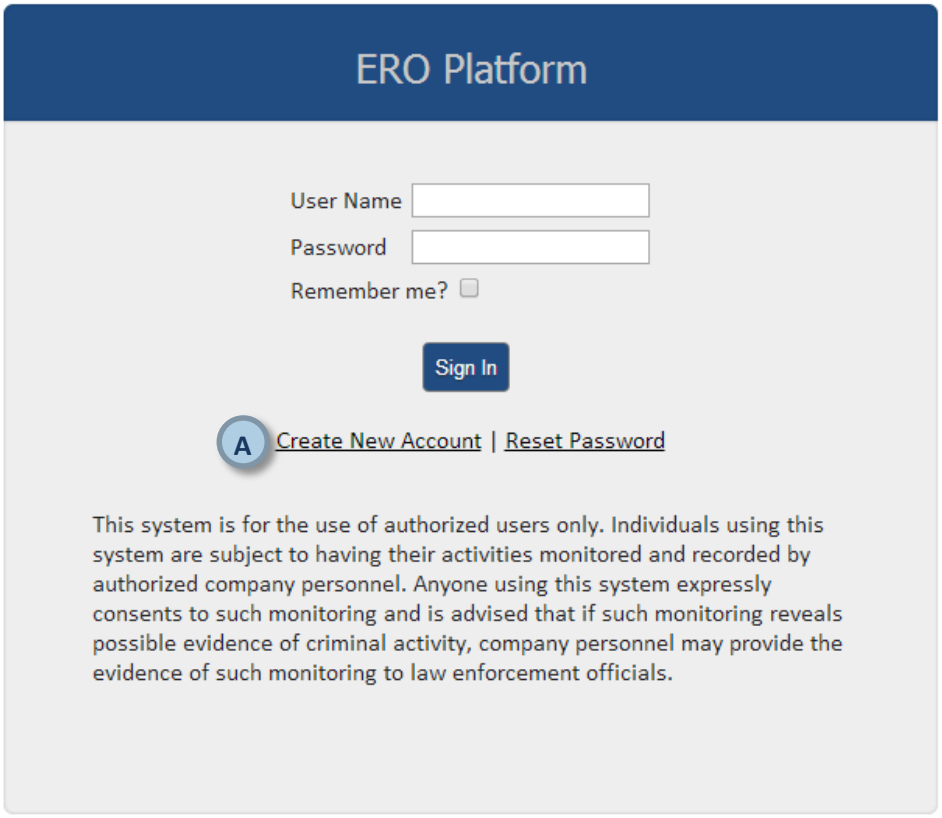


Figure 1: ERO Platform Login Screen

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

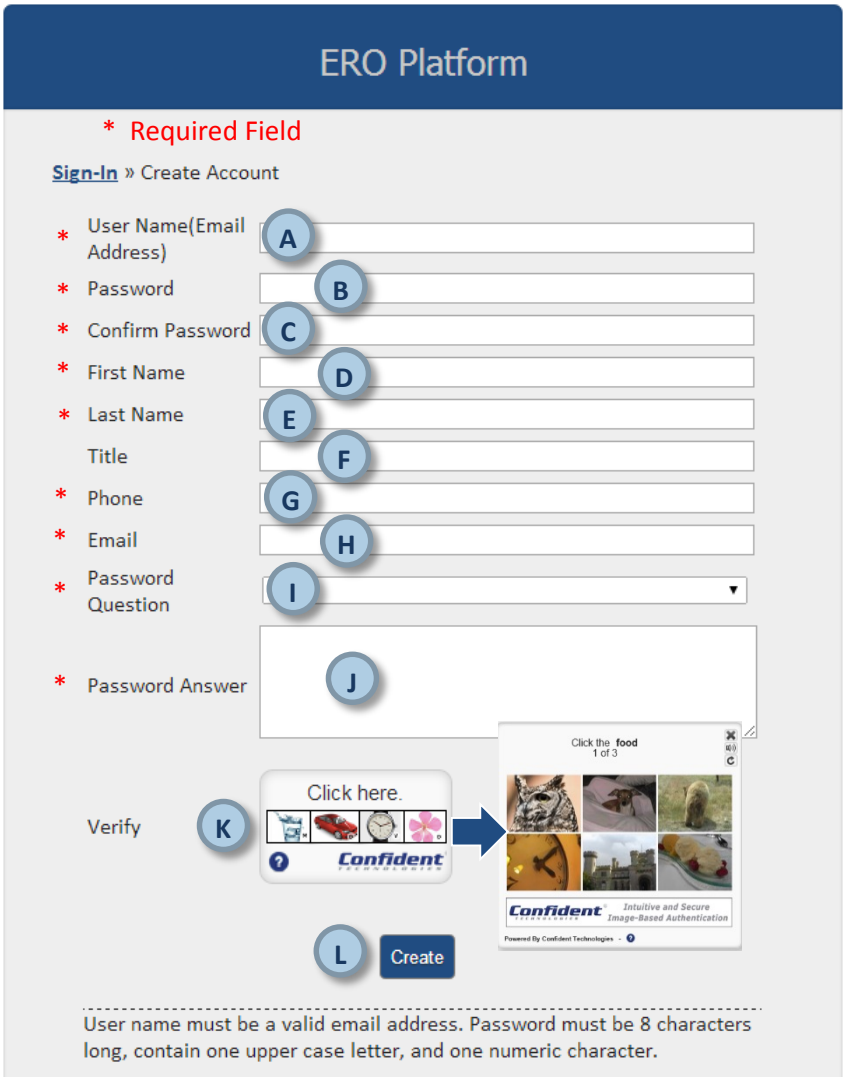


Figure 2: Create Account Screen

To create a new account,

A. Enter a **User Name** (MUST be a business email address - this can be the same email in step H).
B. Enter a **Password**. As the on-screen instructions indicate, this password:
    a. Must be at least eight (8) characters in length.
    b. Must contain at least one uppercase letter.
    c. Must contain at least one numeric character.
C. Re-enter the **Password**.
D. Enter the user's **First Name**.
E. Enter the user's **Last Name**.
F. Enter the user's **Title**.
G. Enter a valid business **Phone Number** where the user may be reached.
H. Enter an **Email Address**. This ***MUST*** be a valid email address, as it will be used to send ***ALL*** notifications of actions and status updates within the system. Both **User Name** and **Email Address** may be the same.

NOTE: Changing this field does not change a user's username.

I. For security purposes, select a **Password Question** from the list of questions.

J. Enter the **Password Answer** to the security question (I).

K. Select the **Verify** icon (K). Several images display. Select the correct image of each description as instructed until all three pictures have been verified.

L. Click the **Create** button (L).

Creating Account Step 2: Verify Account

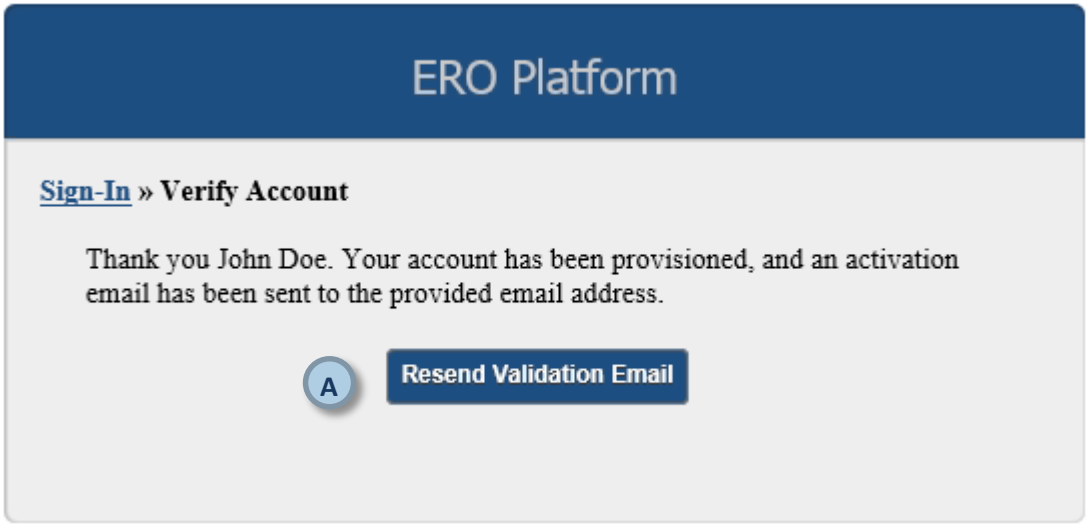


Figure 3: Verify Account Screen

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

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

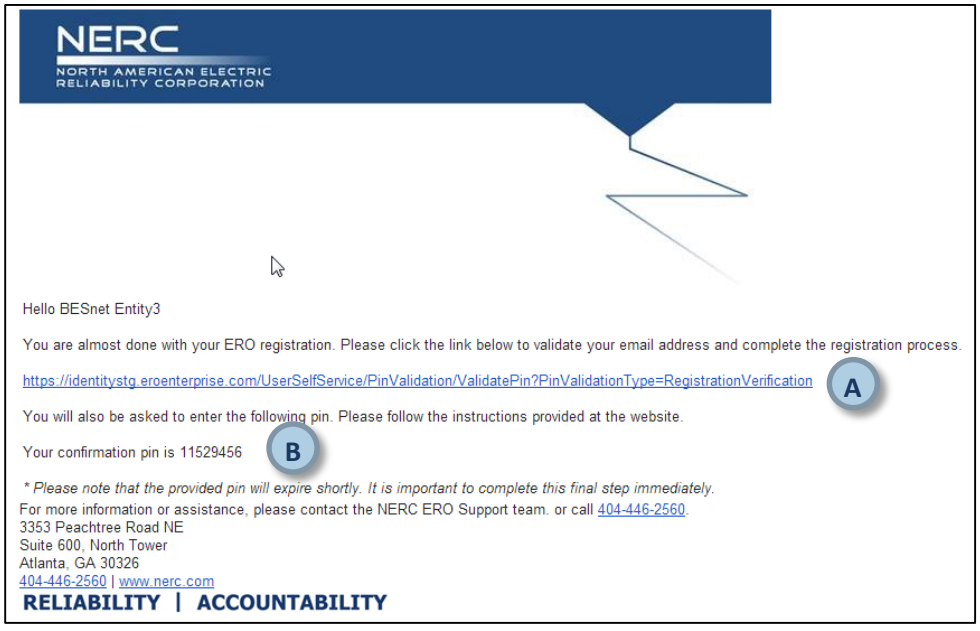


Figure 4: Sample Activation E-Mail

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

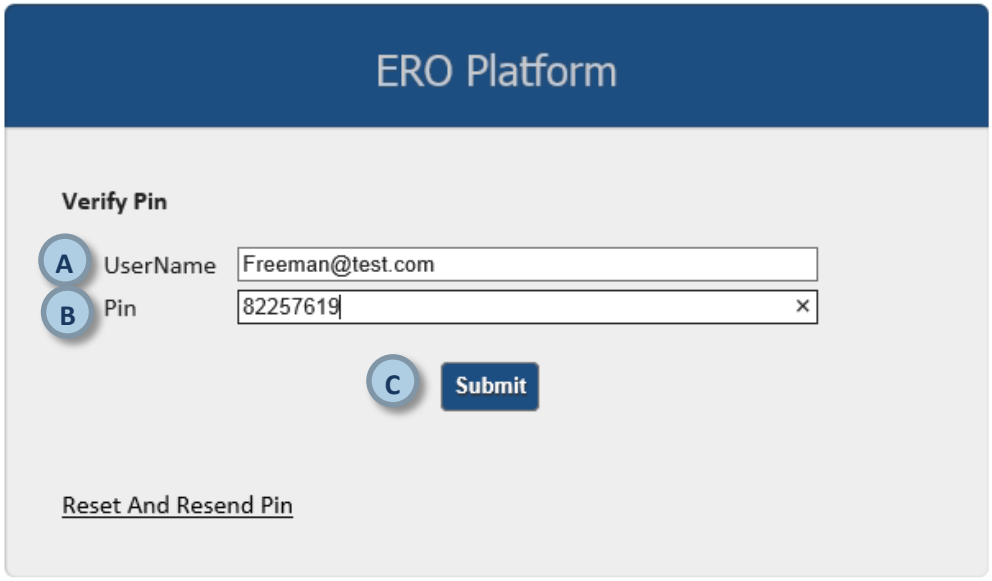


Figure 5: PIN Verification Screen

A. Enter your **User Name** (A).

B. Enter the **PIN** (B) contained in the verification email.

C. Click **Submit** (C).

PIN Expiration Procedure

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

NOTE: PINs expire 60 minutes after issuance.

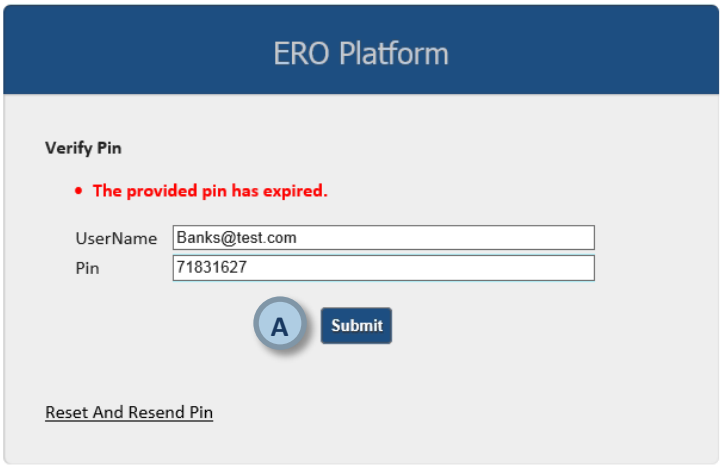


Figure 6: PIN Expiration Screen

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

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

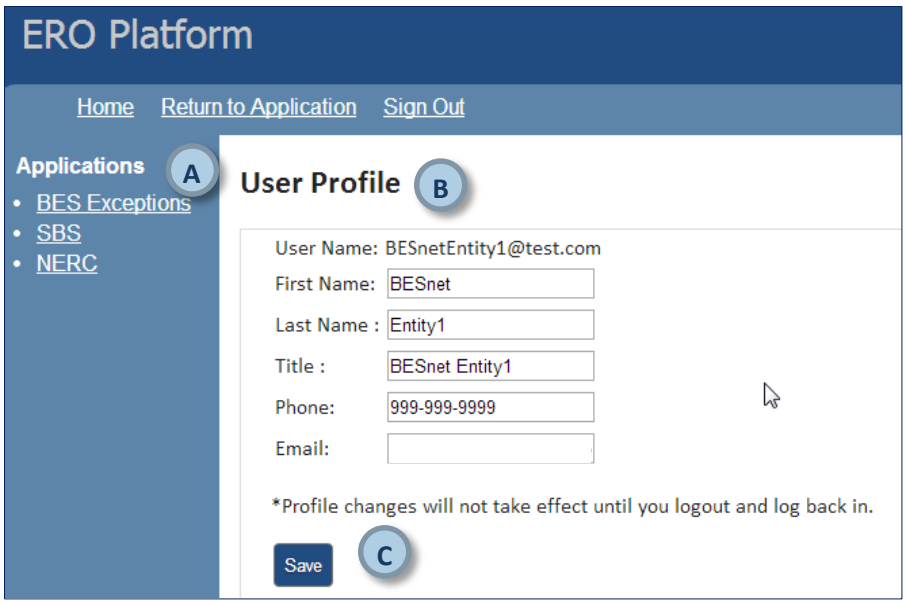


Figure 7: ERO Platform Screen

A. To enter the BESNet application, click on **BES Exceptions** (A).

B. At this screen, you also have the opportunity to modify your User Profile (B).If you have updated your profile, click **Save** (C) to save the changes.

   Note: You will have to logout of the application and log back in for the profile changes to take effect.

Logging Into the BESNet Application

For users who already have an account with BESNet, navigate to the following URL:

https://BESNET.EROENTERPRISE.COM

A. Enter the **User Name** (A).

B. Enter the **Password** (B) entered during the user registration process defined in Section **Creating a New Account.**

C. If desired, check the **Remember me?** (C) Checkbox, which gives permission for the system to remember the credentials entered.

D. Once completed with these fields, complete the login process by pressing the **Sign In** (D) button.

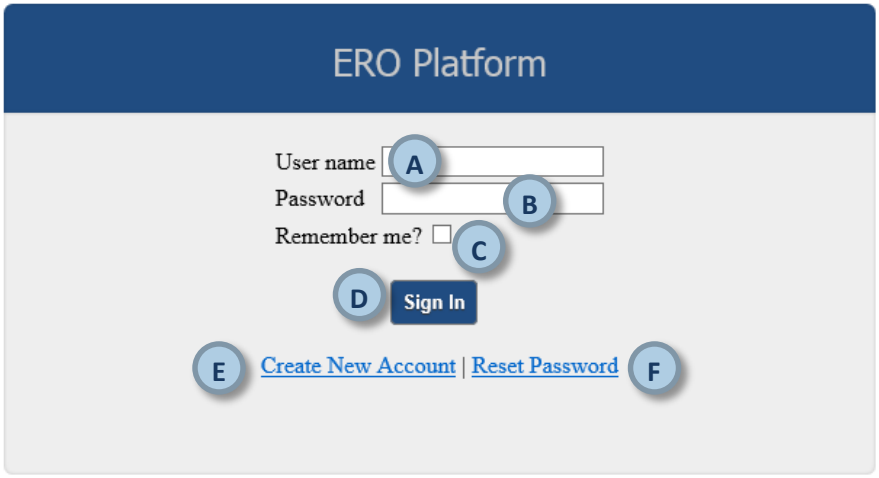


Figure 8: ERO Platform Log-In Screen

For users who do not have an account:

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

To reset your password.

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

Selecting the User's Entity to Use

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

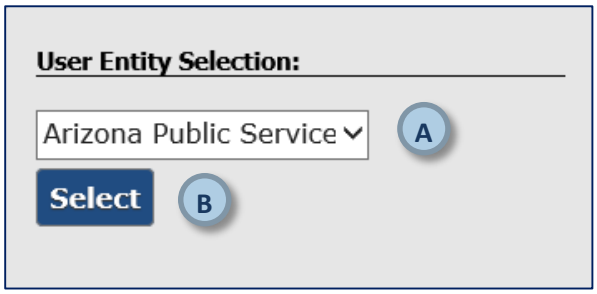


Figure 9: User Entity Selection Screen

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

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

B. Click the **Select** (B) button.

Setting up Your BESNet Application Account

Once your BESNet User ID has been established, you will need to finish setting up the functions of the new account.

Navigate to the BESNet application: https://BESNET.EROENTERPRISE.COM. You will be shown your user profile.

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

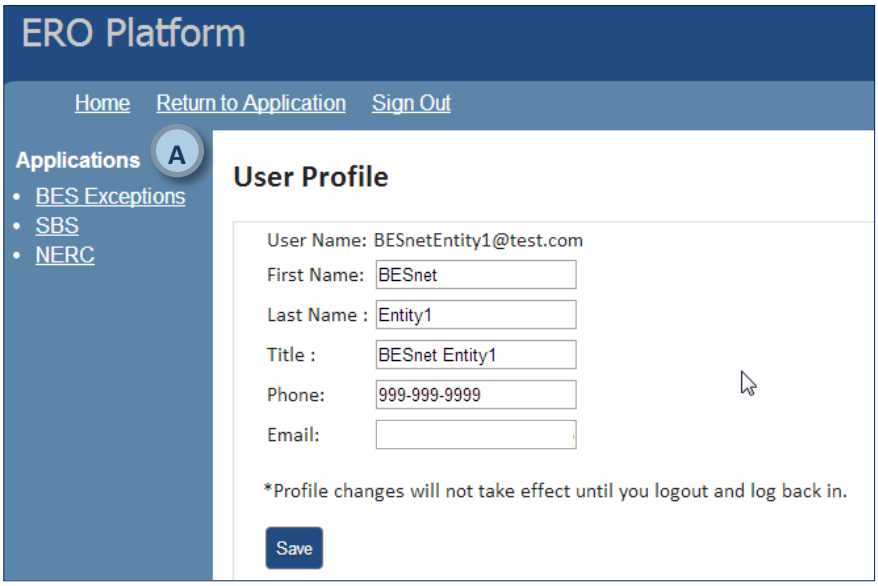


Figure 10: ERO Enterprise Platform Entry Page

Account Setup Step 1: Select Account Type

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

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

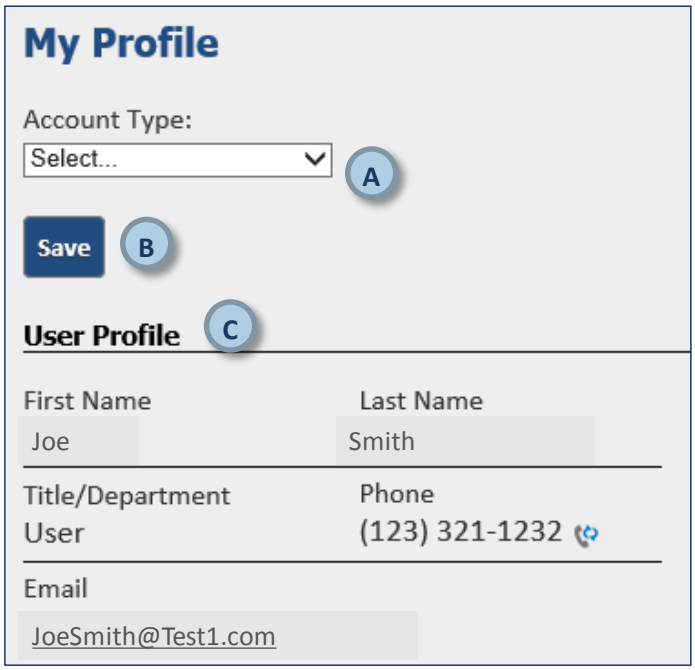


Figure 11: Account Type Selection Screen

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

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

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

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

Account Setup Step 2: Association of Account with Entities

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

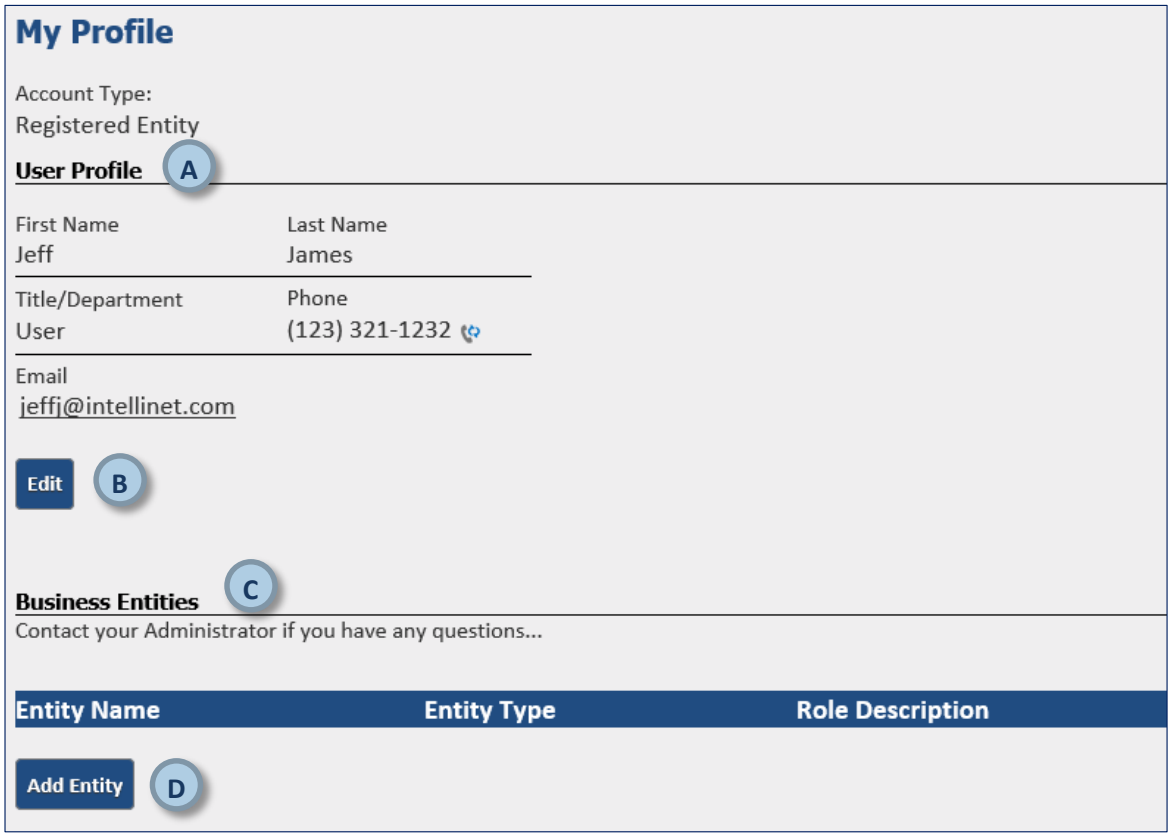


Figure 12: My Profile Screen

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

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

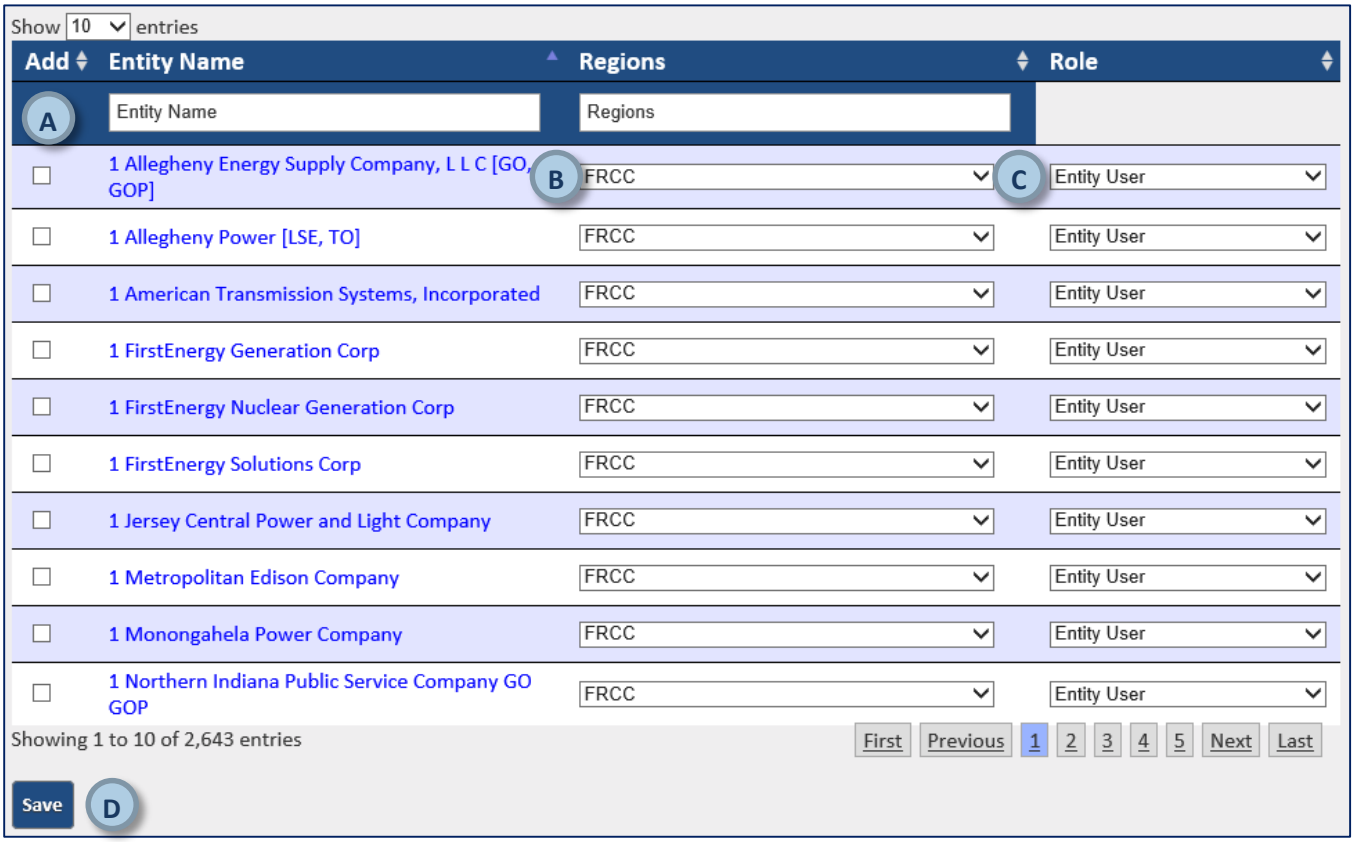


Figure 13: Entity Selection Screen

A. From this list, select the Entity to associate with the account by clicking the checkbox to the left of the Entity record, in the **Add** column (A).

   a. The Entity listing can be filtered by typing in the **Entity Name** filter textbox in the header (directly beneath the **Entity Name** label).

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

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

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

C. Select the **Role** (C) the account will perform for that Entity. Roles are:

   a. Entity User: A general user of the system.

   b. Entity Administrator: A user who has the ability to vet user accounts for that Registered Entity, as well as perform all functions of the Entity User role.

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

D. **Repeat steps A through C for each Entity to be associated with the account**. When complete, click the **Save** button (D). This will bring up the **Vetting Request Confirmation Screen**. This confirms your request

to be vetted by the Entity Administrator(s) associated for each selected Entity (See the **Vetting Users** section for further detail) and the following screen will be displayed.

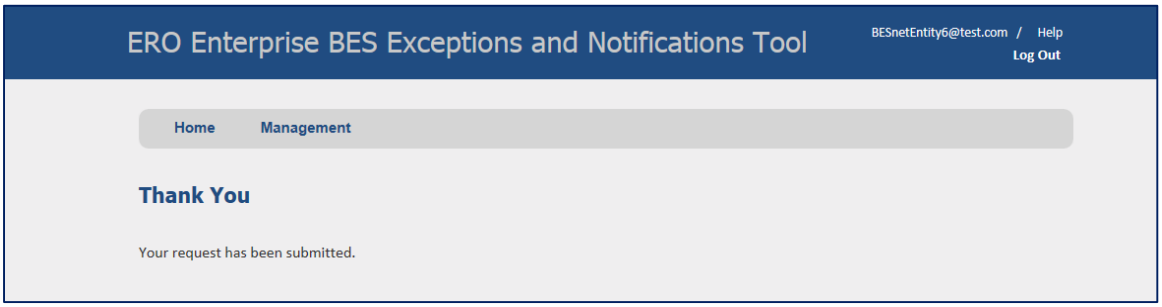


Figure 14: Vetting Request Confirmation Screen

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

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

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

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

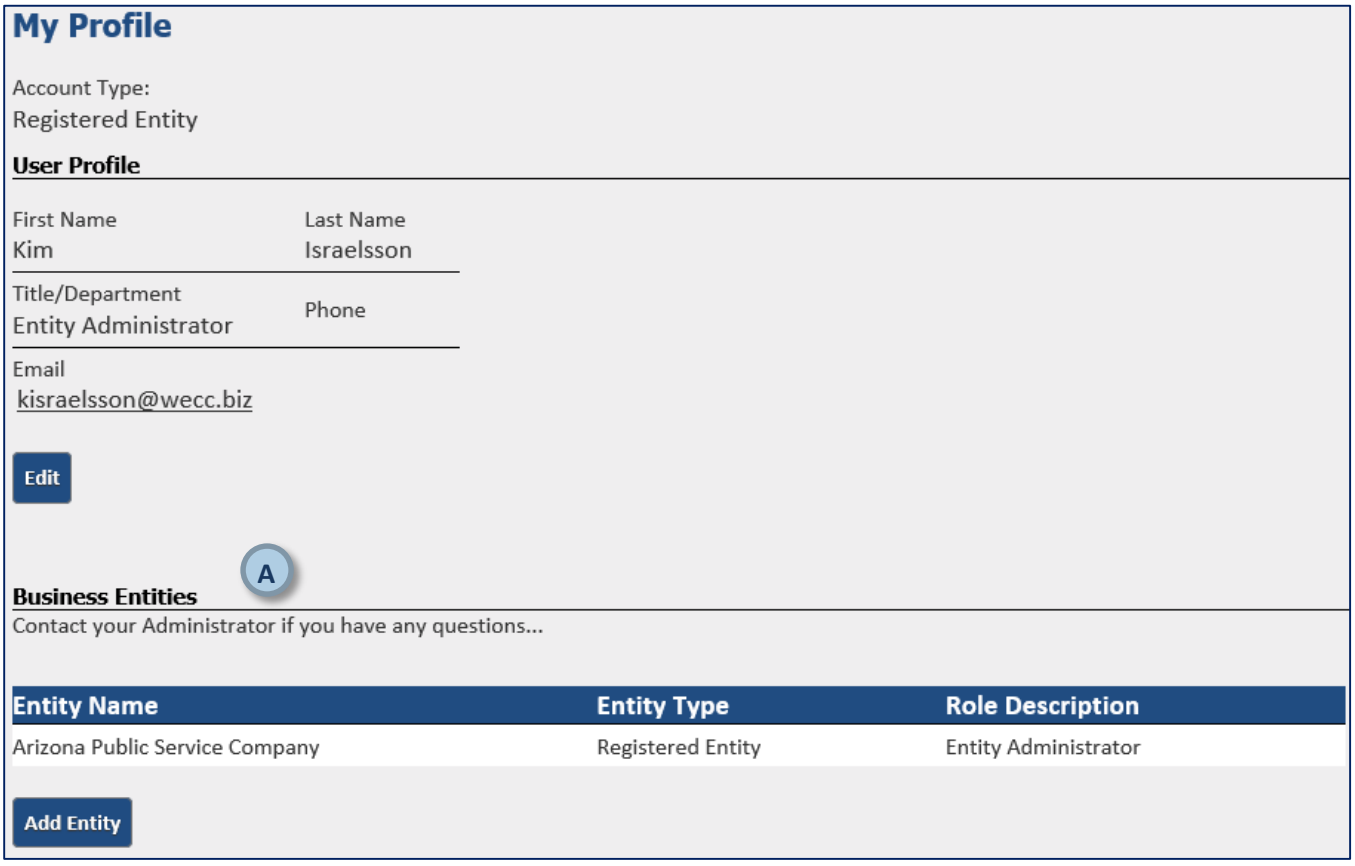


Figure 15: My Profile Screen with Entity Association

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

Editing Your User Profile

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

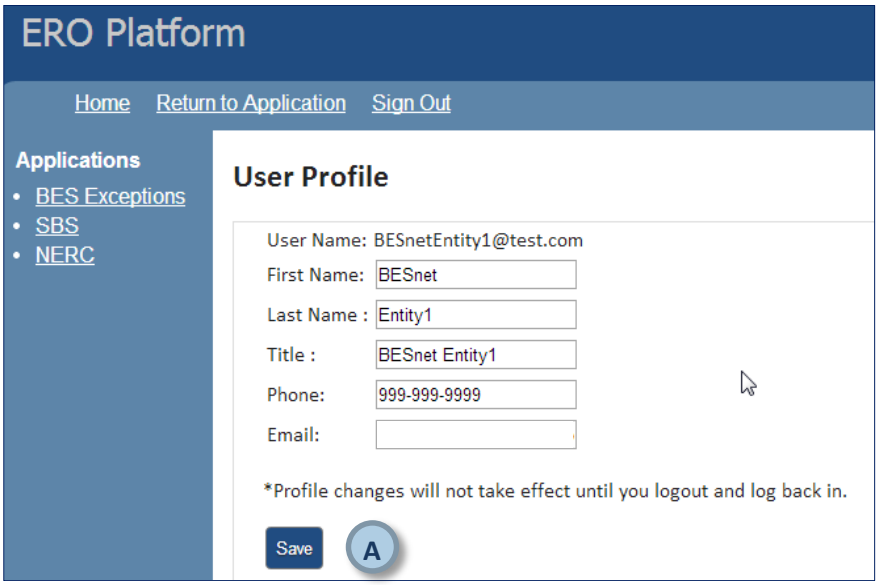


Figure 16: User Profile Screen

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

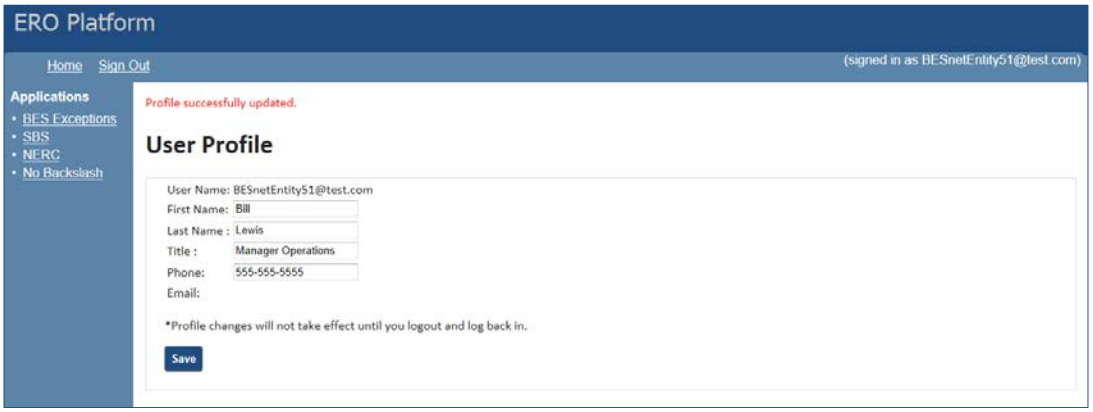


Figure 17: Profile Update Confirmation Screen

Log out and back into the BESNet application.

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

Password Management

Changing User Password

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

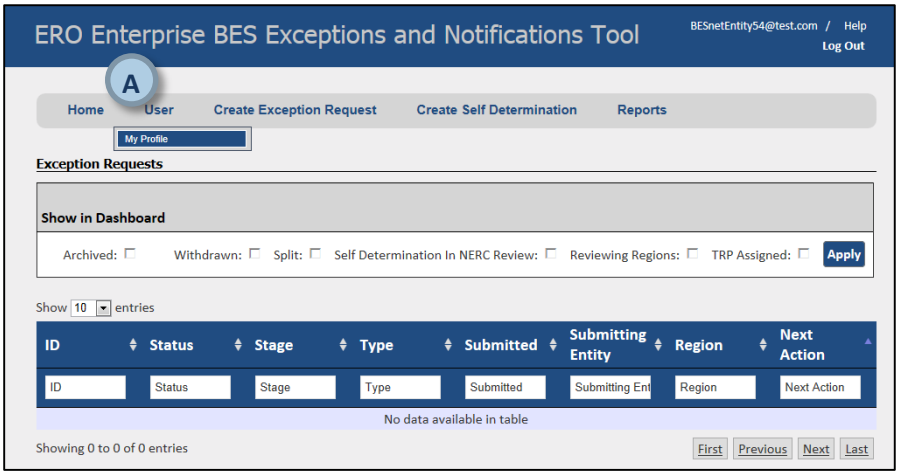


Figure 18: BESNet Home Page

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



Figure 19: My Profile Screen

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

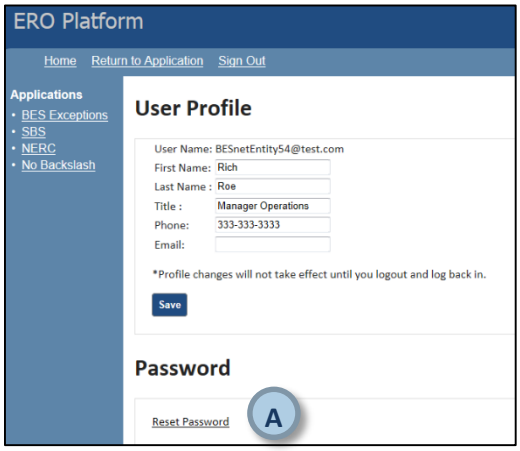


Figure 20: User Profile Screen

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

Forgot/Resetting the User Password

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

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

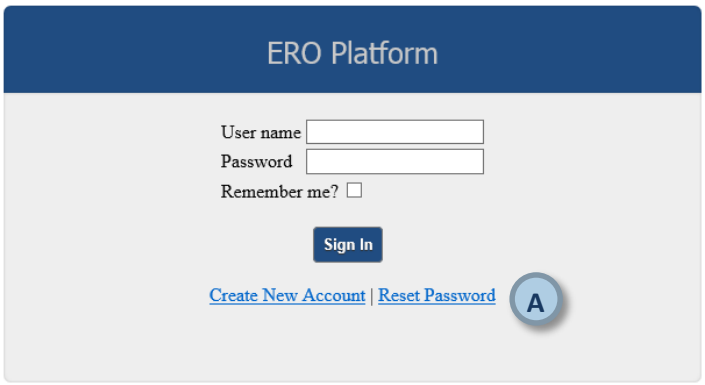


Figure 21: ERO Platform Log-In Screen

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

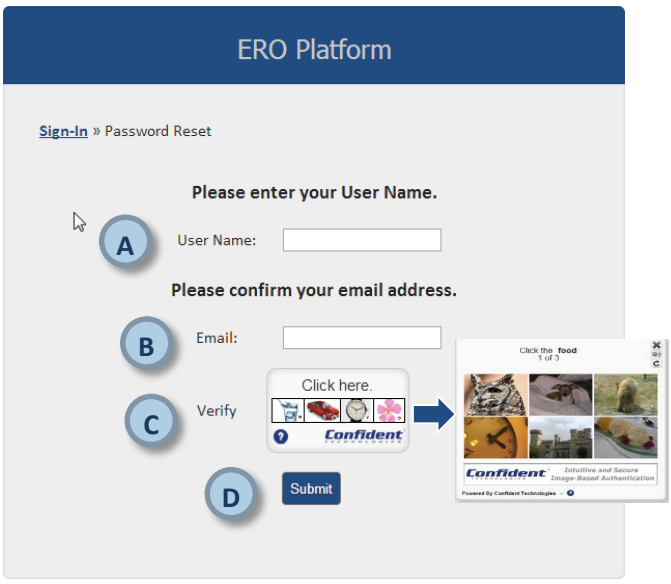


Figure 22: Password Reset Screen

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

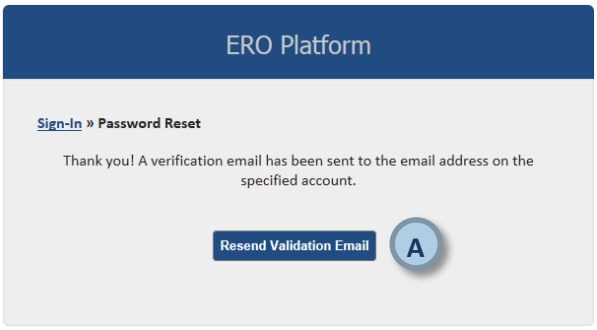


Figure 23: Password Reset Validation Screen

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

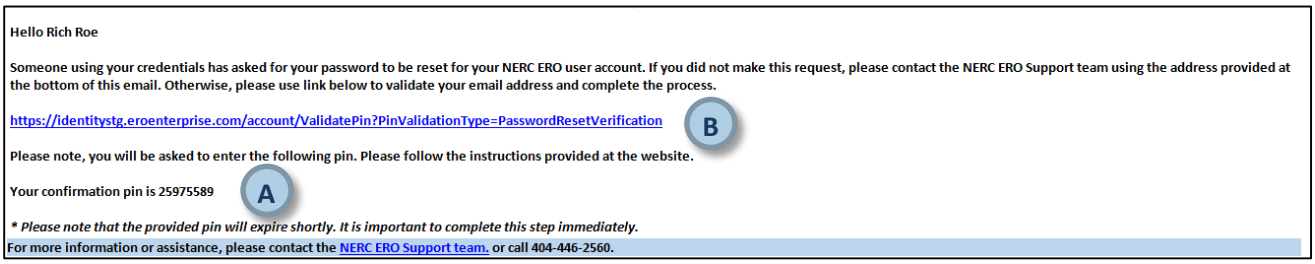


Figure 24: Password Reset Request E-mail

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

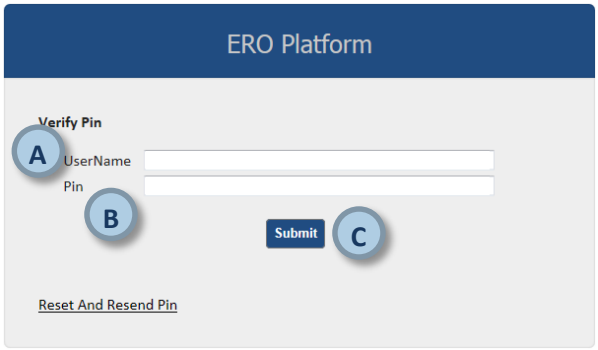


Figure 25: Verify Pin Screen

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

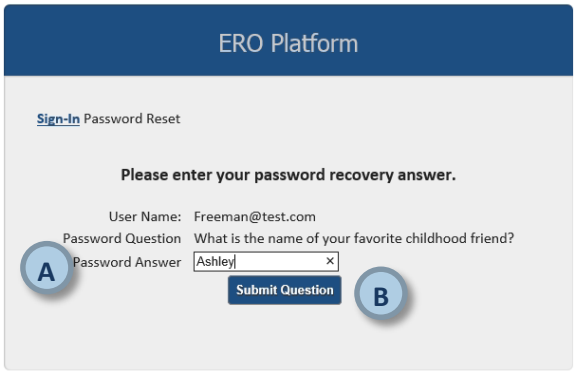


Figure 26: Password Recovery Screen

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



Figure 27: Enter New Password Screen

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

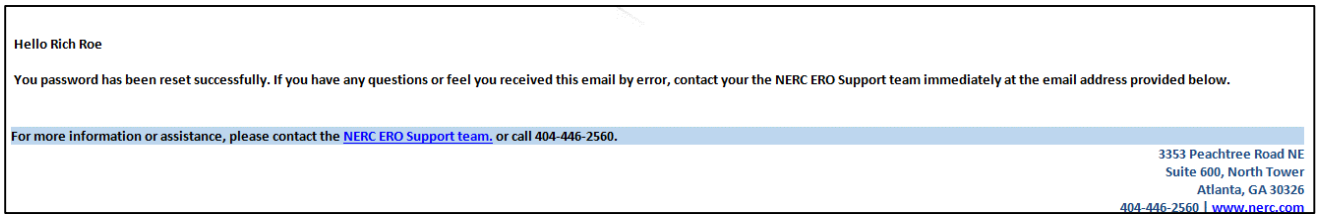


Figure 28: Password Change Confirmation E-mail

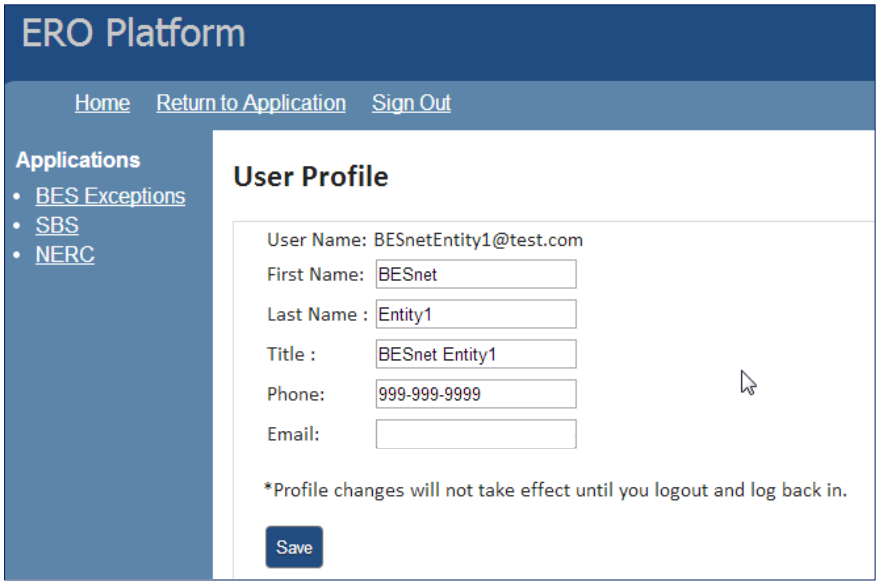


Figure 29: User Profile Screen

Managing Your User Account Properties

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

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



Figure 30: BES Application Screen Header

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



Figure 31: Dashboard Menu Detail

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

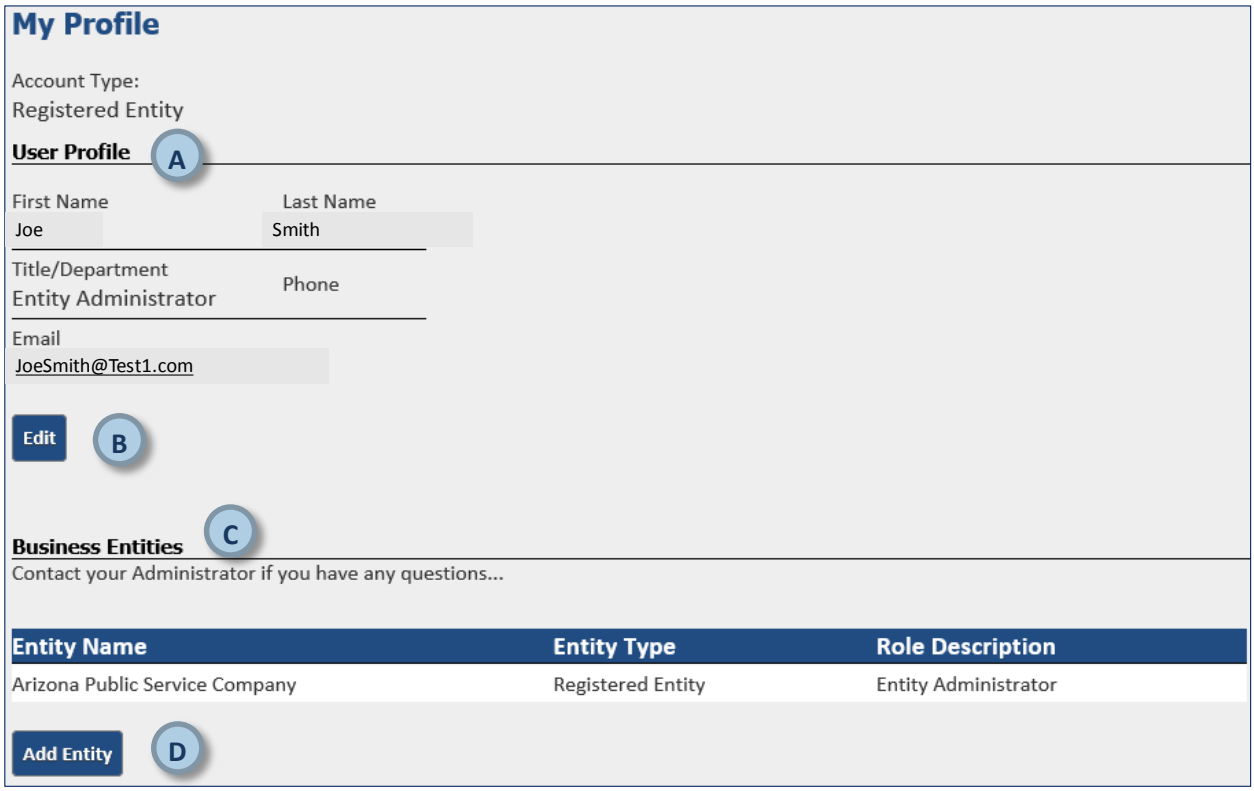


Figure 32: User Profile Management Screen

From here the user can:

A. View the **User Profile** (A) information.

B. Edit the **User Profile** information by clicking the **Edit** button (B).

C. View the listing of **Business Entities** (C) for which the user has access or has requested access.

D. Add an additional Business Entity request, by clicking the **Add Entity** (D) button.

Logging Out

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

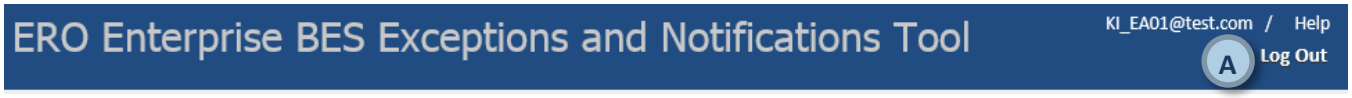


Figure 33: BESNet System Screen Header

Administrator User Account Management

Administrative User Management

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

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

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



Figure 34: BESNet Dashboard Header

Vetting New Users

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

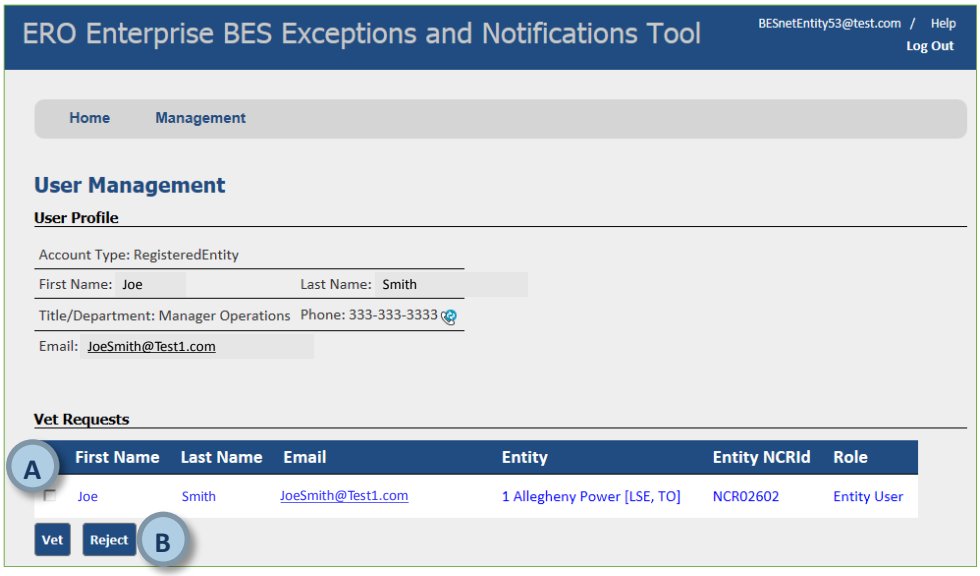


Figure 35: User Management Screen

A. Check the checkbox (A) next to each record to select it as one to approve or reject.

B. To approve the selected request(s), click the **Vet** button (A).

C. To reject the selected request(s), click the **Reject** button (B).

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

User Role Management

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

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

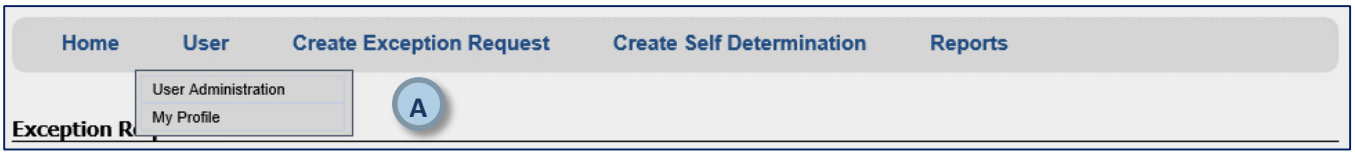


Figure 36: BESNet Dashboard Header

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

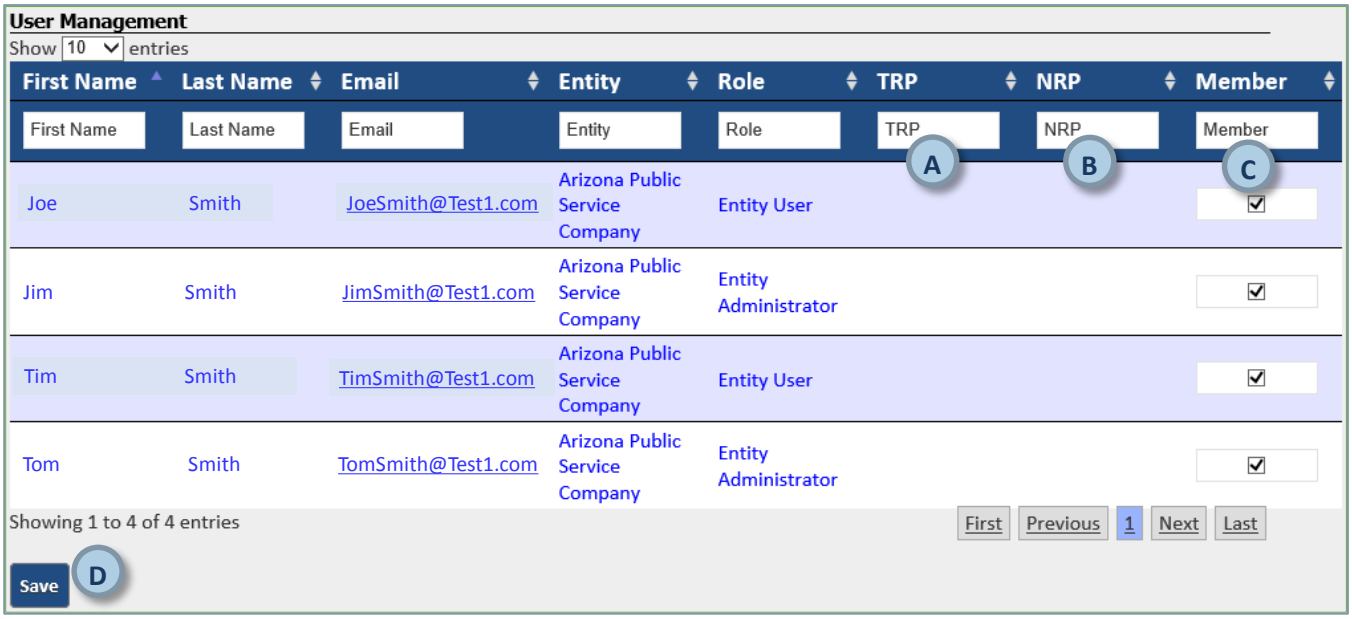


Figure 37: User Management Screen

A. The **Technical Review Panel** (TRP) membership can only be set by a **Regional Administrator**, and therefore cannot be set here.

B. The **NERC Review Panel** (NRP) membership can only be set by a **NERC Administrator**, and therefore cannot be set here.

C. To disassociate a user account from the Entity, uncheck the **Member** checkbox (C) for that account/Entity relationship. By default, all vetted members appear checked in the **Member** checkbox (C).

D. Once all the role changes have been made, click the **Save** button (D).

BESNet Dashboard Overview

The **BESNet Dashboard** is the home screen for the BESNet application. The Dashboard is displayed when a user first logs in and at any point when the **Home** link is pressed.

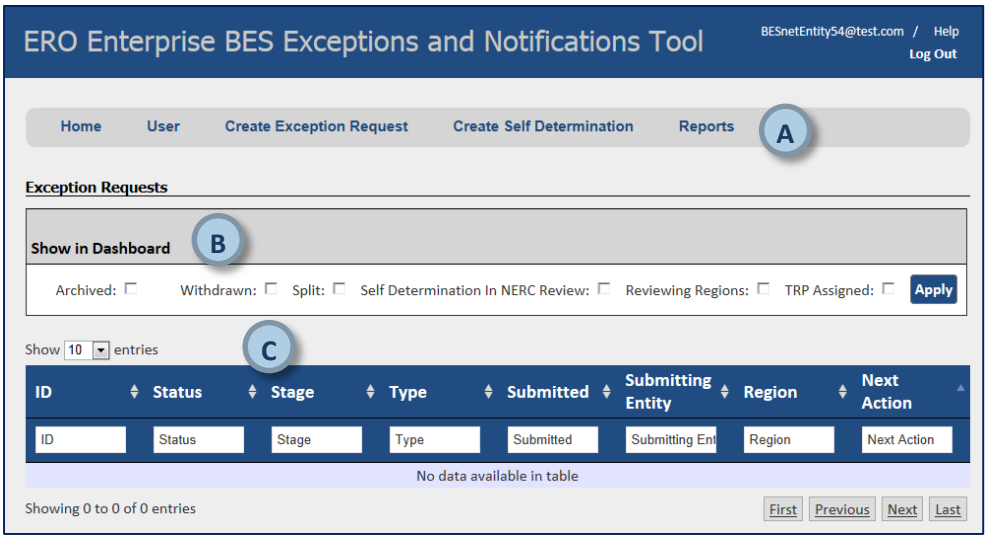


Figure 38: BESNet Dashboard

A. The **Dashboard navigation bar** (A) contains the following options:

   a. **Home:** Returns the user to the Dashboard

   b. **User:** Provides options for user management and account management.

   c. **Create Exception Request:** Starts the process for creating a new Exception Request.

   d. **Create Self-Determination:** Starts the process for creating a new Notification of Self-Determination.

   e. **Reports:** Contains options for reporting.

   NOTE: Some options may not appear, based on a user's role in the system.

B. The **Show in Dashboard** Filter (B). By default, Exception Requests that are archived or withdrawn, or that have been split and are therefore no longer active, do not appear in the Exception Requests listing. This filter allows the user to include any or all of these Exception Requests in the listing by checking the box next to the Exception Request state that should be included. These operate as follows:

   a. **Archived:** When checked, the dashboard will include Exception Requests that have been archived, cancelled, or terminated.

   b. **Withdrawn:** When checked, the dashboard will include Exception Requests that have been withdrawn; that is, those submitted to Initial Review, but then rescinded by the Submitting Entity.

   c. **Split:** When checked, the dashboard will include Exception Requests that have been split into one or more newer Exception Requests, and exist as a historical record.

      *NOTE: For more information about Split Exception Requests, see sections on **Splitting an Exception Request** or **Recertifying an Exception Request**.*

   d. **Self-Determination in NERC Review***: When checked, the dashboard will include any Notifications of Self-Determination that are awaiting NERC's review.*

C. The **Dashboard List** (C) contains a list of all **Exception Requests** and **Notifications of Self-Determination**. Here, the user can:

   a. Change the number of records that appear in the list, by changing the **Show in Entries** value.

   b. Change the display order of the entries in the list, by clicking on the header of each column.

   c. Filter the contents of the list, by entering text into the text boxes underneath each column header.

   d. Open a record, by clicking on the **Status** link.

   e. Navigate through the pages in the list, by clicking the navigation links to the bottom right of the listing.

Notifications of Self-Determination

Creating a Notification of Self-Determination

The BESNet application is the vehicle for officially notifying a Regional Entity of a self-determination of a change of status for an Element when applying the BES Definition.[1]

To start, click the **Create Self-Determination** pull-down (A) on the **Dashboard Menu**, and choose whether the Notification of Self-Determination is **For Inclusion** or **For Exclusion**. This will bring the user to the **Create Notification of Self-Determination Screen**.

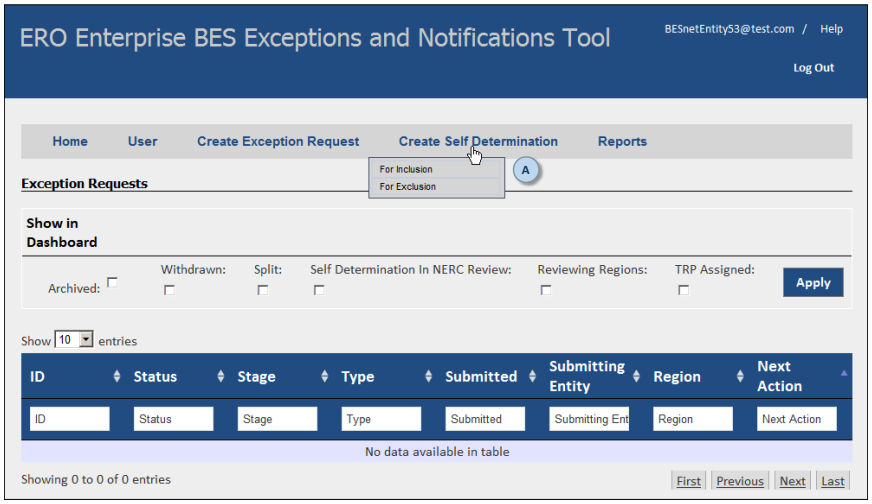


Figure 39: BESNet Dashboard

The **Create Notification of Self-Determination Screen** is broken into three sections for these instructions.

Create Notification of Self-Determination Screen Section 1: General Information

Section 1 contains **General Information (A)** about the Submitting Entity, pre-populated from the user information.

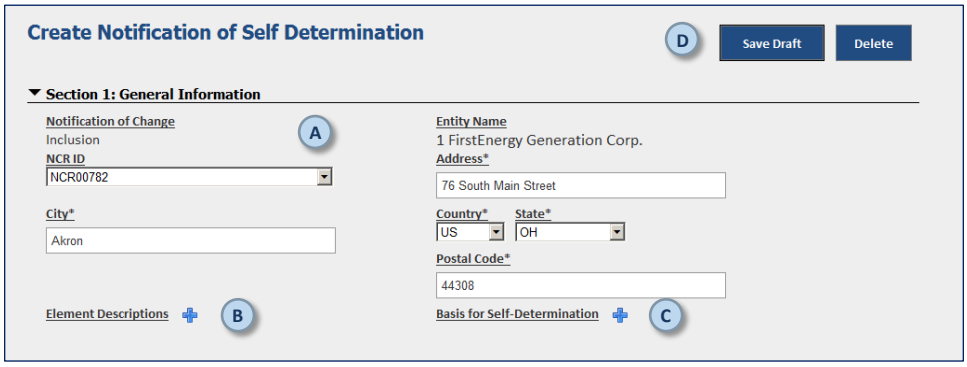


Figure 40: Create Notification of Self-Determination Screen Section 1

Basic information about the Submitting Entity (i.e., the Entity with which the user is operating) can be edited here, including the Address, City, Country, State, and Postal Code.

Section 1 also has two sub-sections about the Notification for:

A. The **Element Description** (B) and the **Basis for Self Determination** (C)

[1] Refer to the *BES Definition Reference Document* and the *BES Notification Review Guidelines* at: http://www.nerc.com/pa/RAPA/Pages/BES.aspx

B. **Save Draft** and **Delete** buttons (D) that can be used at any time.

NOTE: The BESNet application automatically saves a draft of the Notification if the browser is closed or the session is interrupted.

Selecting Element Description

NOTE: A Notification can contain more than one Element, but all Elements in the Notification should be of the same type and should be Included or Excluded for the same reasons.

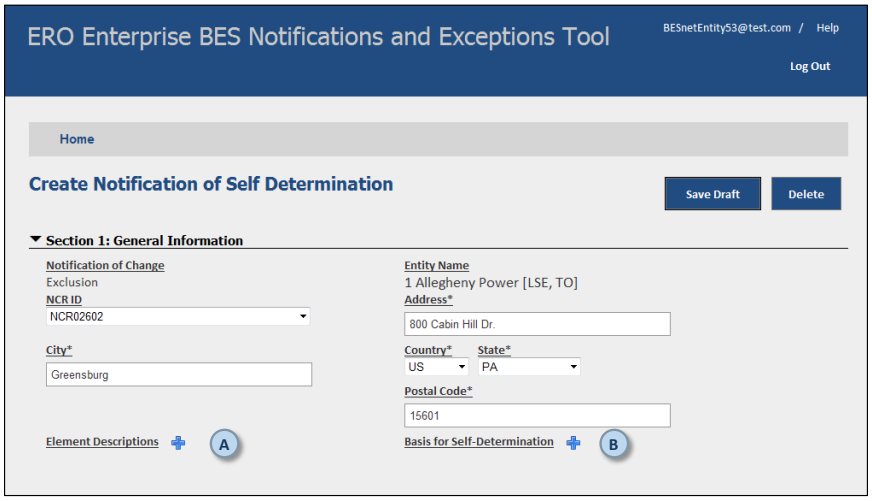


Figure 41: Element Description and Basis for Self-Determination

The user must select the **Element Description**. To do so, click on the blue **Plus Sign** at the **Element Descriptions** (A). This will bring the user to the **Add Element Description Screen**.

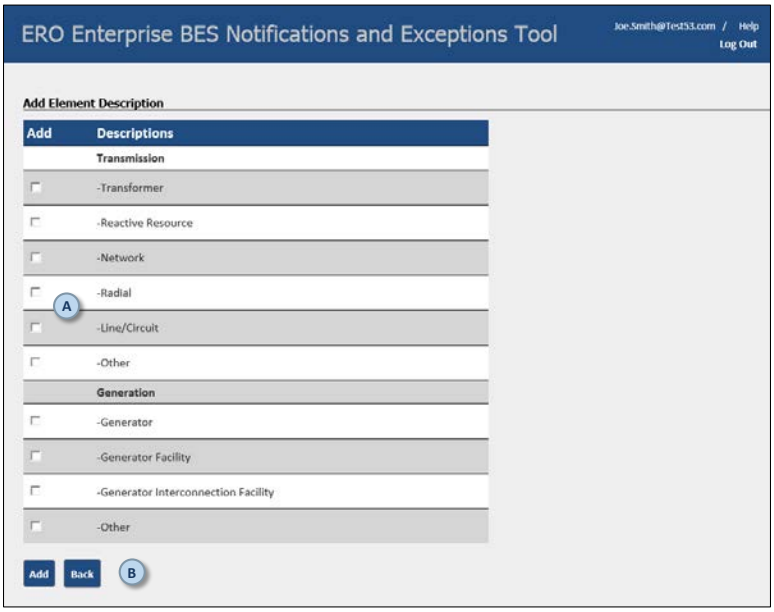


Figure 42: Add Element Description Screen

The user should select the appropriate **Element Description** for which the Notification of Self-Determination is being submitted (A), and click on **Add** (B) to complete the action. This will return the user to the **Create Notification of Self-Determination Screen**.

Selecting Basis for Self-Determination

NOTE: A Notification can contain more than one Element, but all Elements in the Notification should be of the same type and should be Included or Excluded for the same reasons.

The user must select the BES Definition reason for the Element's inclusion or exclusion. To do so, click on the blue **Plus Sign** at the **Basis for Self-Determination** (B). This will bring the user to the **Add BES Definition Screen**.

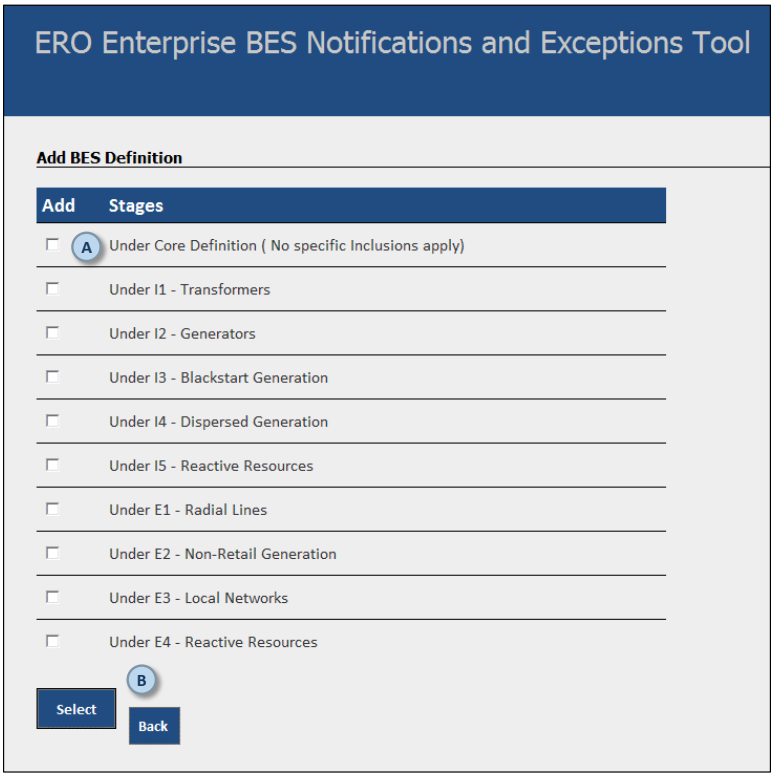


Figure 43: Add BES Definition Screen

The user should select the appropriate BES Definition reason that the Element is being included or excluded and for which the Notification of Self-Determination is being submitted (A), and click on **Add** (B) to complete the action. This will return the user to the **Create Notification of Self-Determination Screen**.

Removing an Element Description or Basis for Self-Determination

Once the Basis for Self-Determination is selected, the **Create Notification of Self-Determination Screen** will show **Red X's** (A) near the **Element Description** and **Basis for Self-Determination** areas on the screen.

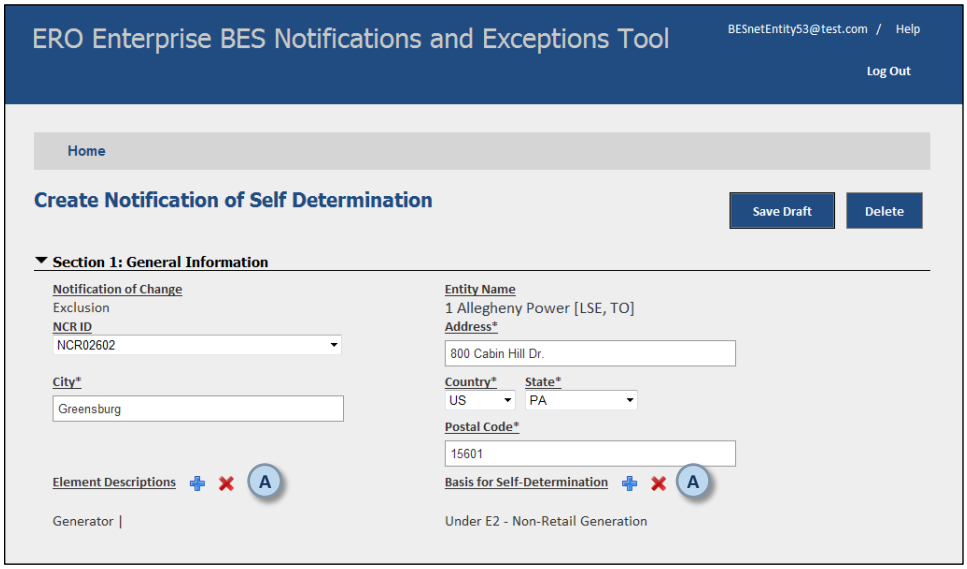


Figure 44: Create Notification of Self-Determination Screen

If either the Element Description or Basis for Self-Determination is incorrect or should be removed, click on the **Red X**. This will bring the user to the appropriate removal screen (Figure 45, **Remove Element Description Screen,** used as an example).

The user should check the box of the **Description** (A) to be removed and then click on the Remove button (B) to complete the action. This will return the user to the **Create Notification of Self-Determination Screen**.

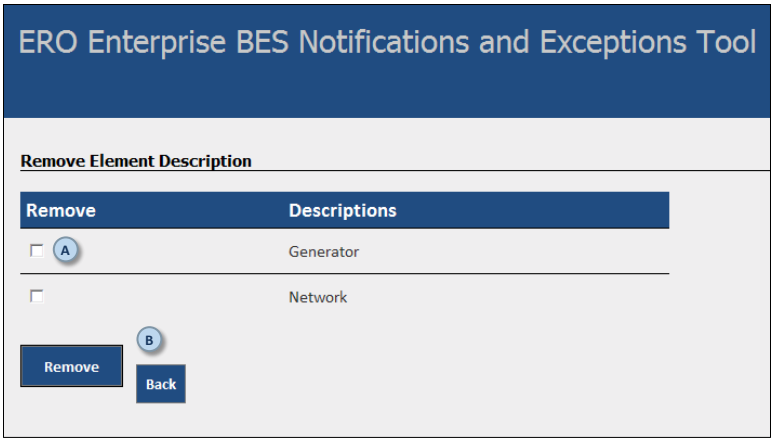


Figure 45: Remove Element Description Screen

Create Notification of Self-Determination Screen Section 2: Detailed Information

The **Detailed Information Section 2** contains information for the **Submitting Entity Contact Information** (A), and the Entity's authorized representative that is certifying the Notification of Self-Determination.

The user must enter:

A. The **Submitting Entity Contact Information** (A)

B. The **Authorized Representative's Name and Title** (B).

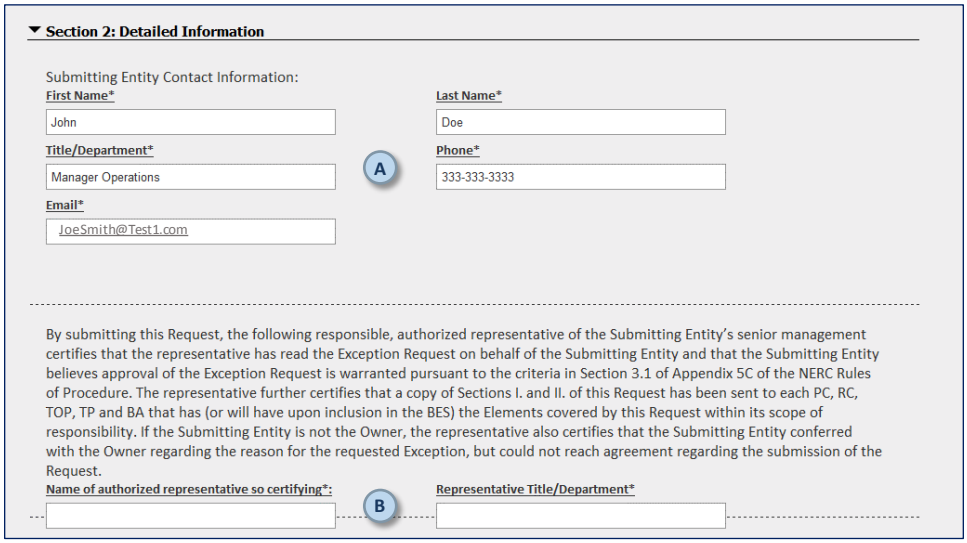


Figure 46: Create Notification of Self-Determination Screen Section 2

Adding an Element to a Notification of Self-Determination

Once the general information is entered in Sections 1 and 2 for the Notification on the **Create Notification of Self-Determination Screen**, the user should click on the **Add** button, which will take you to the **Add Element Screen.**

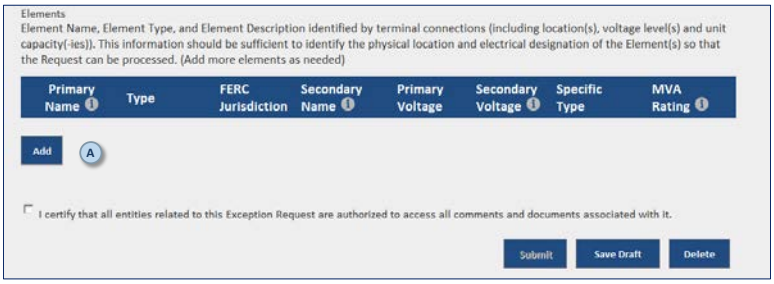


Figure 47: Create Notification of Self-Determination Screen – Add Element Screen

Several functions are performed through the Add Element Screen:

A. The **Element Type** (A) has a pull-down menu (B) allowing selection of the type of Element.

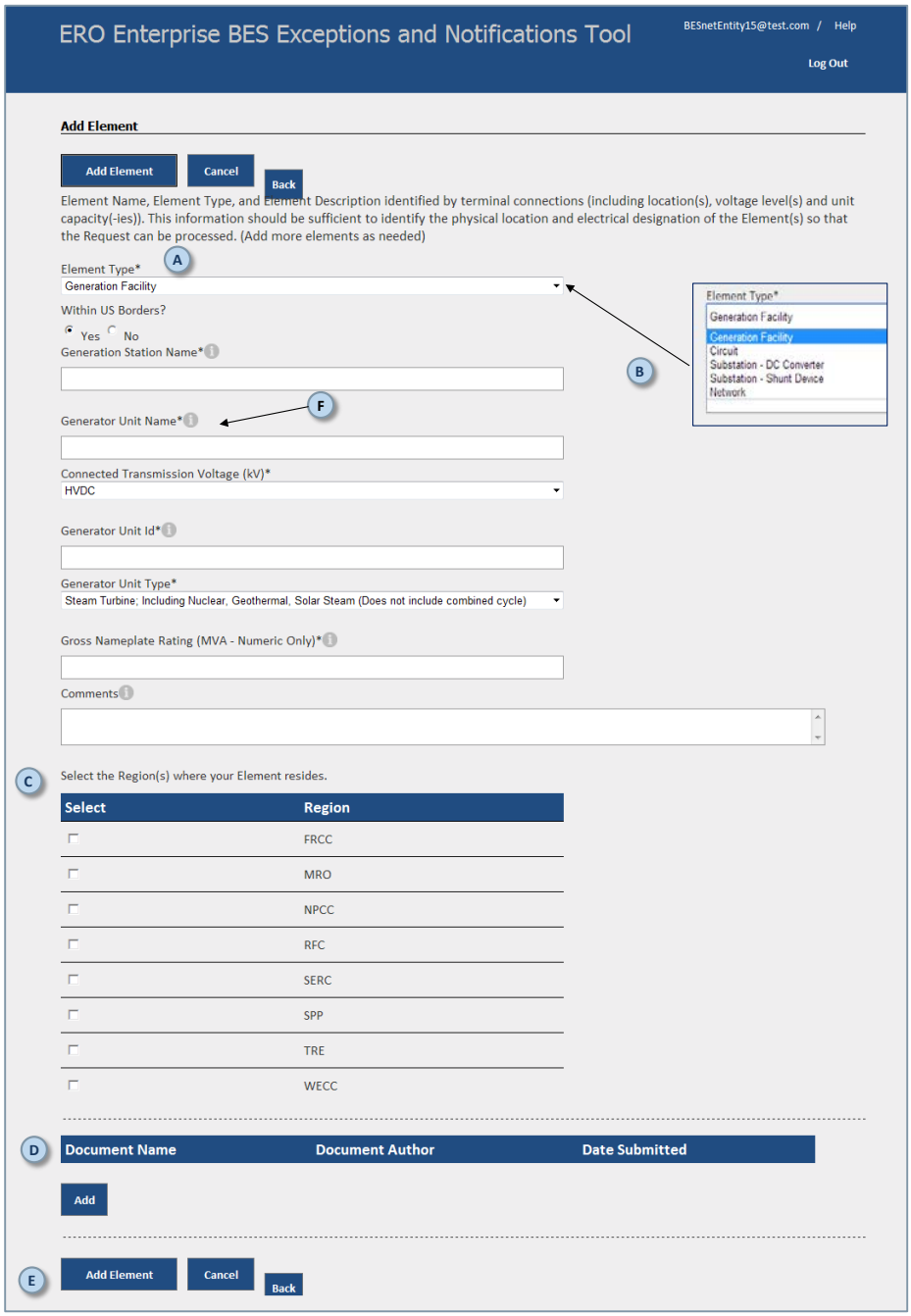


Figure 48: Add Element Screen

B. The user should select the **Element Type** from the pull-down menu (B), which will display data entry screens specific to that **Element Type**. Additional information on the types is in the **Element Type** section of this document.

C. The Region(s) where the Element resides is selected in the **Select the Region** area (C)—multiple Regions can be selected.

D. Attach necessary documentation[2] by clicking on the **Add** button (D). Additional guidance on adding documents is included in the Adding Documents section of this guide.

NOTE: At least one (1) supporting document is required for each Element in a Notification of Self-Determination.

E. Click on the **Add Element** button (E) when finished entering data for the Element to complete its addition to the Notification. That action will return the user to the **Create Notification of Self-Determination Screen**, where all Elements that are part of the Notification are displayed.

F. Informational points are denoted by an "i" (F) throughout the **Add Element Screens**. Hovering over them will reveal additional information about the item.

Element Types

When adding an Element to a Notification of Self-Determination, the fields to be completed vary by Element. Screenshots of each Element's properties are provided below for reference.

Table 1 shows the types of Elements listed in the **Element Type** pull-down menu (A) on the **Add Element Screen**.

Table 1: Element Types

	Within FERC Jurisdiction	Name(s)	Voltage (kV)	ID	Specific Type	MVA Rating	Comments
Generation Facility	Yes or No, Required	Generation Station Name, Required; Unit Name, Required	Connected AC Transmission Voltage, Required, from a list of values	Unit ID, Required	Required, from a list of Generator Unit Types	Gross Nameplate Rating, Required	Optional
Circuit	Yes or No, Required	From Point Name, Required; To Point Name, Required; Common Element Name, Required	From Point kV, Required, from a list of values; To Point kV, Required, from a list of values	Circuit ID, Optional	Required, from a list of Circuit Types	Normal Rating, Optional	Optional
Substation, DC Converter	Yes or No, Required	Converter Name, Required	Connected AC Transmission Voltage, Required, from a list of values	N/A	N/A	Normal Rating, Optional	Optional
Substation, Shunt Device	Yes or No, Required	Network Name, Required; Device Name, Required	Station kV, Required, from a list of values	N/A	Device Type	Normal Rating (MVA or MVAR), Optional	Optional
Network	Yes or No, Required	Network Name, Required	Connected AC Transmission Voltage, Required, from a list of values	N/A	N/A	N/A	Optional

[2] Refer to the *BES Notification Review Guidelines* for additional information on necessary documentation.

Add a Generation Facility

If the user clicks on the **Generation Facility** in the **Element Type** section of the **Add Element Screen**, the following **Generation Facility** Screen appears:

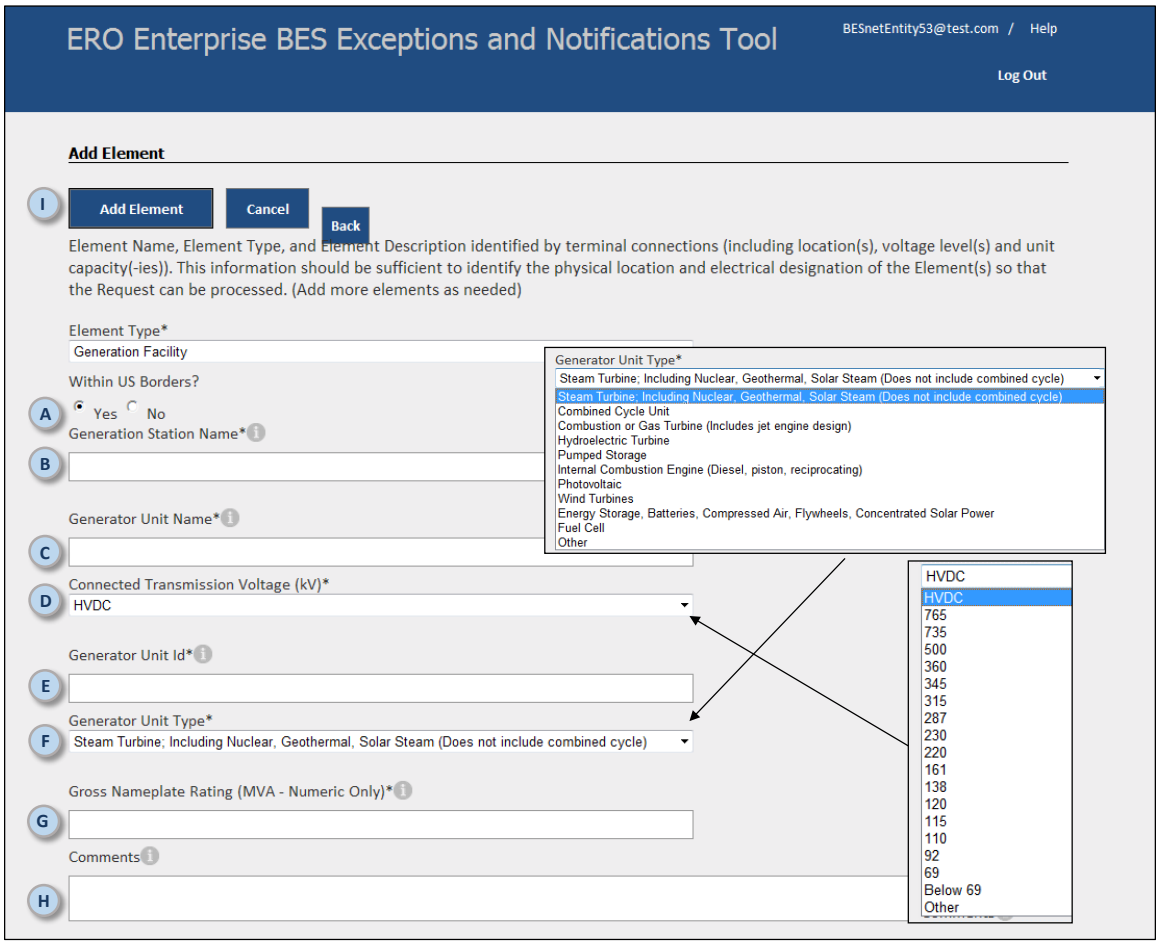


Figure 49: Add Generation Facility Screen

A. Select whether the **Generation Facility** is within the U.S. Borders (A).

B. Provide the **Generation Station Name** (B).

C. Provide the **Generator Unit Name** (C).

D. Select the **Connected Transmission Voltage** (D) from the pull-down list.

E. Provide the **Generator Unit ID** (E).

F. Select the **Generator Unit Type** from the pull-down list.

G. Provide the **Gross Nameplate Rating** in MVA (G). One decimal point is allowed.

H. Provide **Comments** (H) if desired.

I. Click on the **Add Element** button (I) to save the information. This will bring the user to the **Create Notification of Self-Determination Screen**.

Add a Circuit

If the user clicks on the **Generation Facility** in the **Element Type** section of the **Add Element Screen**, the following **Circuit Screen** appears:

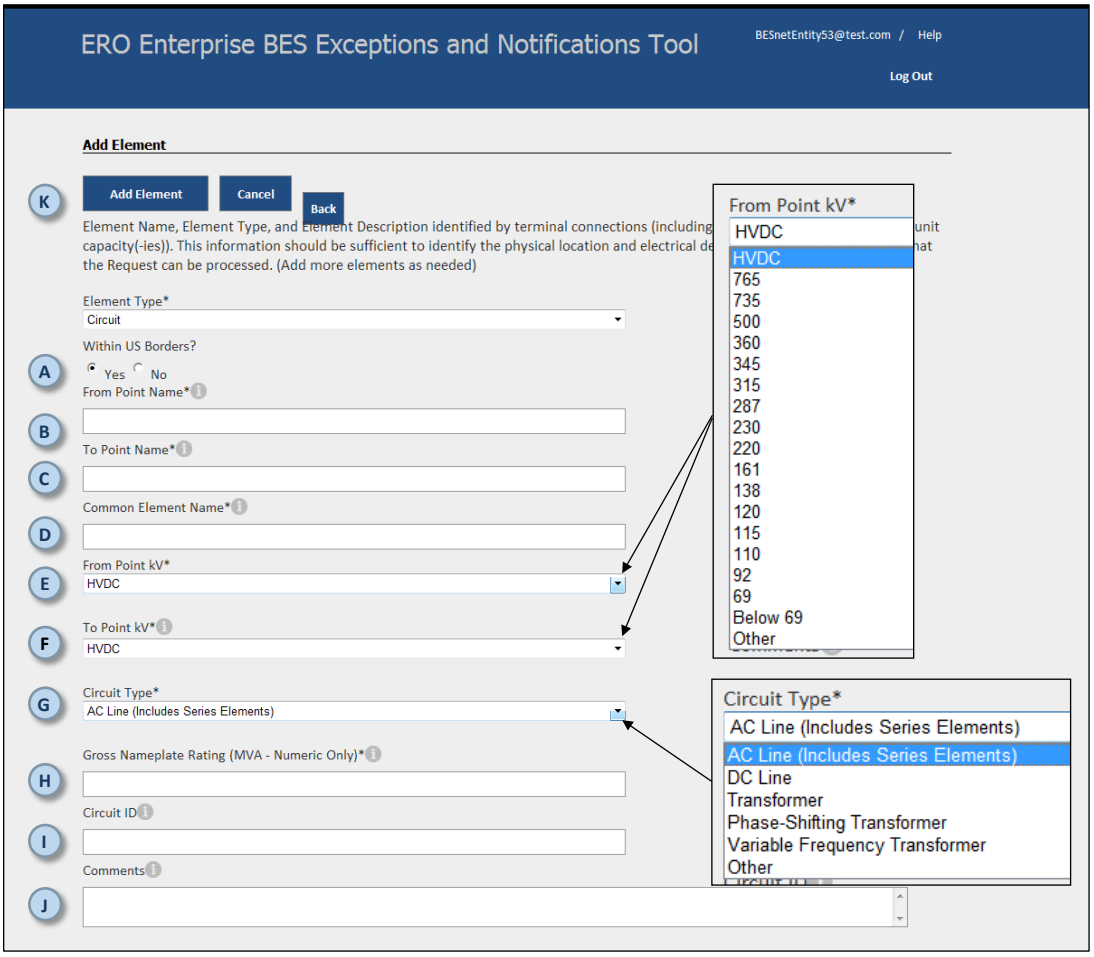


Figure 50: Add Circuit Screen

A. Select whether the **Circuit** is within the U.S. Borders (A).

B. Provide the **From Point Name** (B).

C. Provide the **To Point Name** (C).

D. Provide the **Common Element Name** (D) for the **Circuit**.

E. Select the **From Point kV** (E) from the pull-down list.

F. Select the **To Point kV** (F) from the pull-down list.

G. Select the **Circuit Type** (G) from the pull-down list.

H. Provide the **Gross Nameplate Rating** in MVA of the **Circuit** (H). One decimal point is allowed.

I. Provide the **Circuit ID** (I).

J. Provide **Comments** (J) if desired.

K. Click on the **Add Element** button (I) to save the information. This will bring the user to the **Create Notification of Self-Determination Screen**.

Add a DC Converter

If the user clicks on **Substation – DC Converter** in the **Element Type** section of the **Add Element Screen**, the following **Circuit Screen** appears:

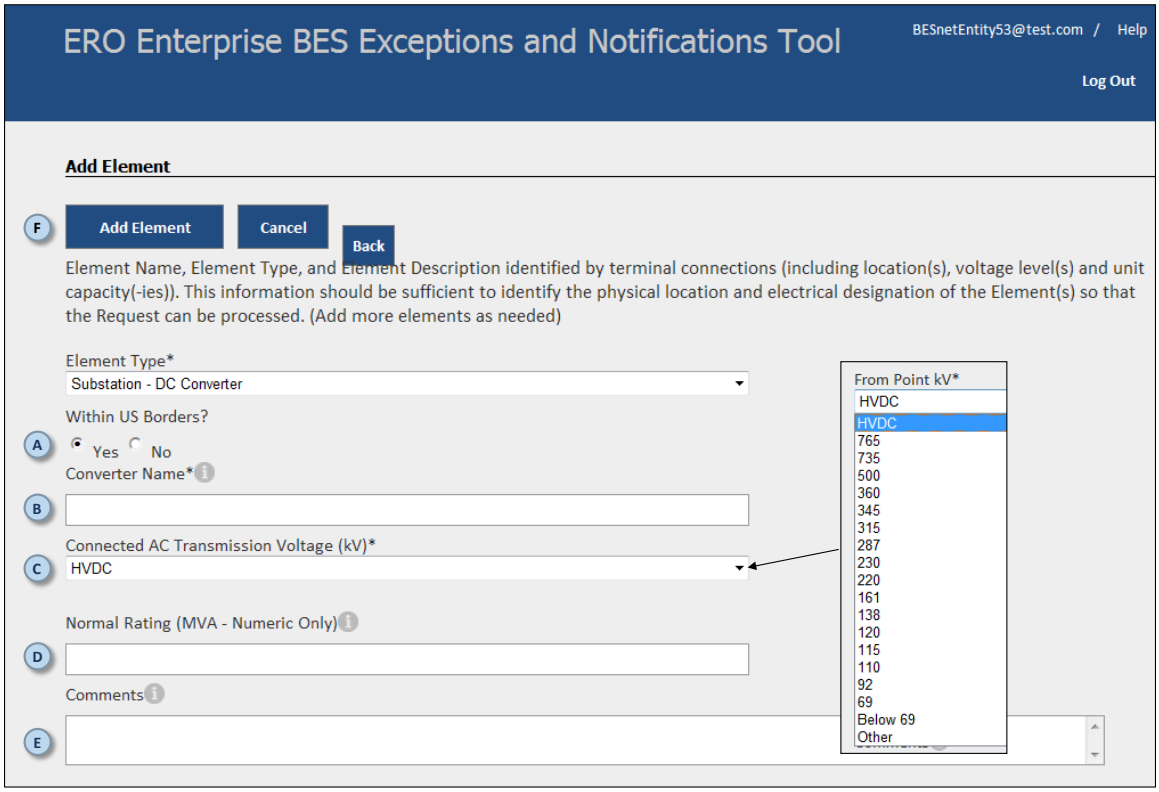


Figure 51: Add DC Converter Screen

A. Select whether the **DC Converter** is within the U.S. Borders (A).

B. Provide the **Converter Name** (B).

C. Select **HVDC** as the **Connected AC Transmission Voltage** (C) from the pull-down list.

D. Provide the **Normal Rating** in MVA for the **DC Converter** (D). One decimal point is allowed.

E. Provide **Comments** (E) if desired.

F. Click on the **Add Element** button (F) to save the information. This will bring the user to the **Create Notification of Self-Determination Screen**.

Add a Substation Shunt Device

If the user clicks on the **Substation – Shunt Device** in the **Element Type** section of the **Add Element Screen**, the following **Shunt Device Screen** appears:

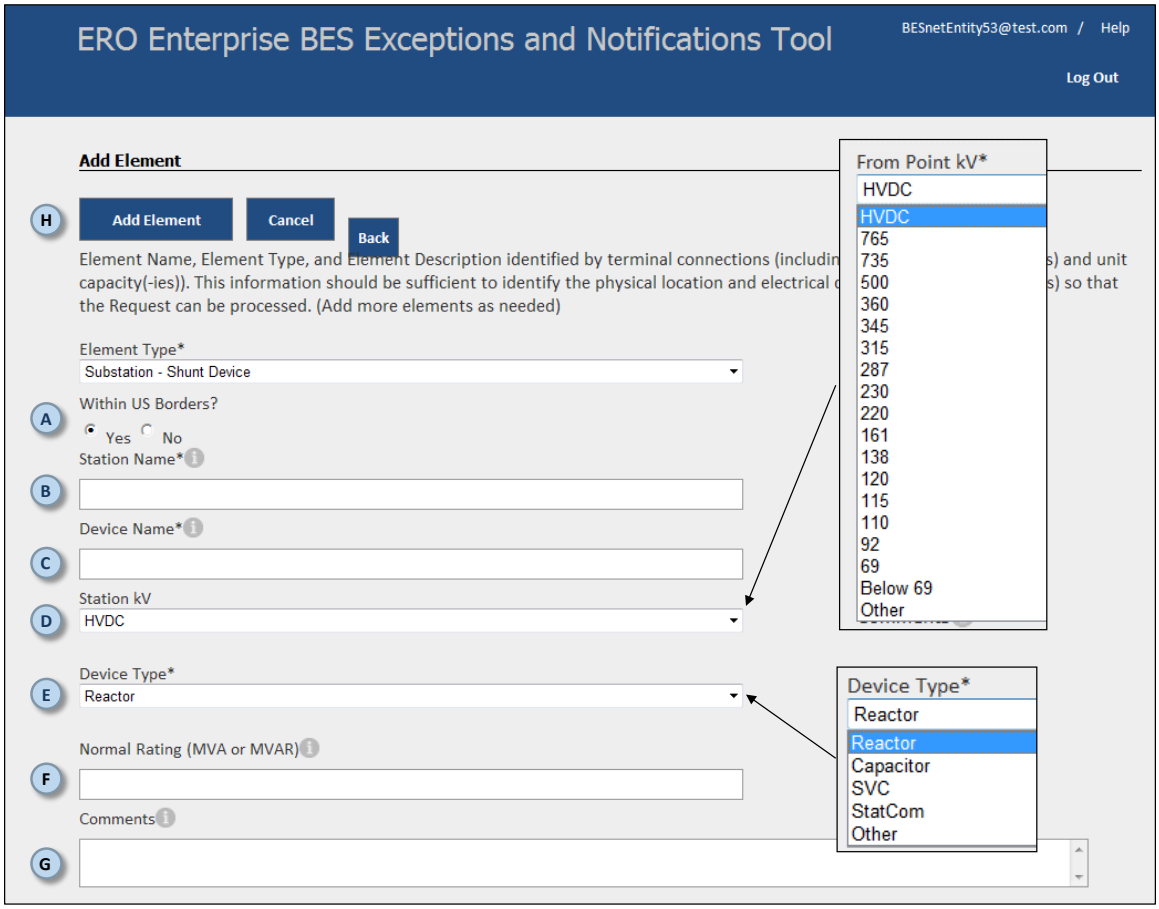


Figure 52: Add Shunt Device Screen

A. Select whether the **Shunt Device** is within the U.S. Borders (A).

B. Provide the **Station Name** (B) where the device is located.

C. Provide the **Device Name** (C).

D. Select the **Station kV** (D) from the pull-down list.

E. Select the **Device Type** (E) from the pull-down list.

F. Provide the **Normal Rating** in MVA for the **Device** (F). One decimal point is allowed.

G. Provide **Comments** (G) if desired.

H. Click on the **Add Element** button (H) to save the information. This will bring the user to the **Create Notification of Self-Determination Screen**.

Add a Network

If the user clicks on the **Network** in the **Element Type** section of the **Add Element Screen**, the following **Network Screen** appears:

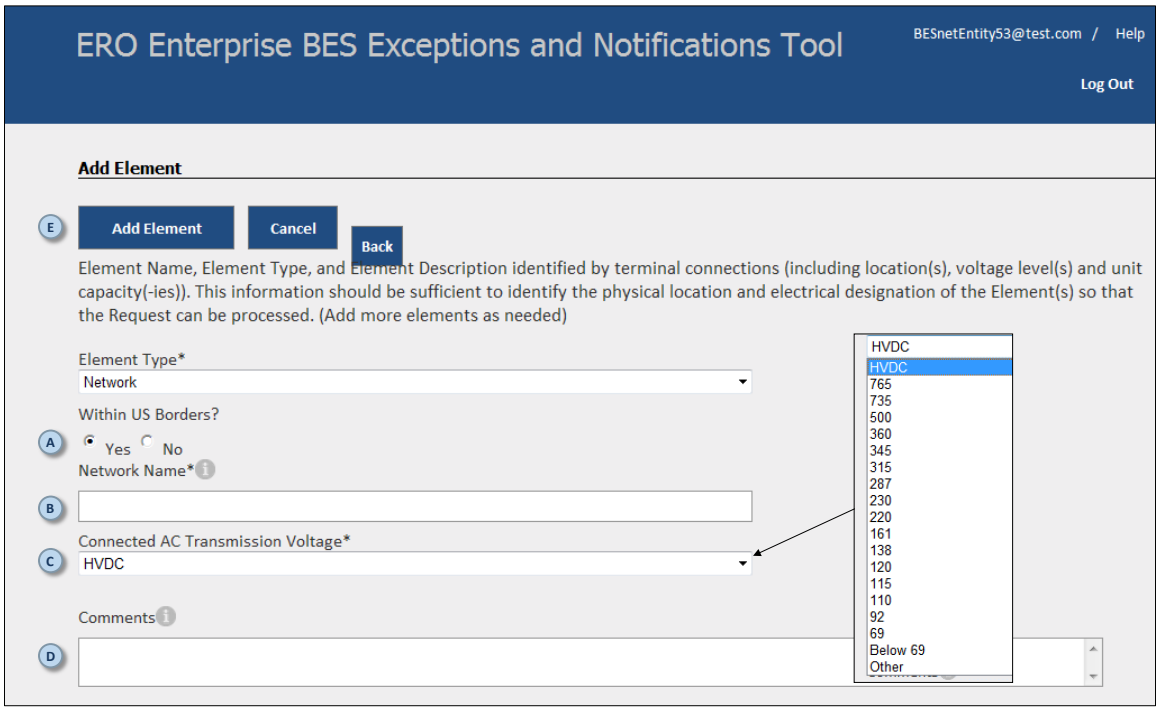


Figure 53: Add Network Screen

A. Select whether the **Network** is within the U.S. Borders (A).

B. Provide the **Network Name** (B).

C. Select the **Connected AC Transmission Voltage** (C) from the pull-down list.

D. Provide **Comments** (D) if desired.

E. Click on the **Add Element** button (E) to save the information. This will bring the user to the **Create Notification of Self Determination Screen**.

Selecting a Region for the Element

The user must select the Region(s) in which the Element of the Self-Determined Notification is located. Multiple Regions can be selected for Circuits.



Figure 54: Select Region(s) Section of Add Element Screen

Add Supporting Documentation for the Element

At least one supporting document[3] must be supplied for each Element in the Notification. To add a document, click the **Add** button in the Document section of the **Add Element Screen** (A). This will take you to the **Add Element Document Screen.**



Figure 55: Document Section of Add Element Screen

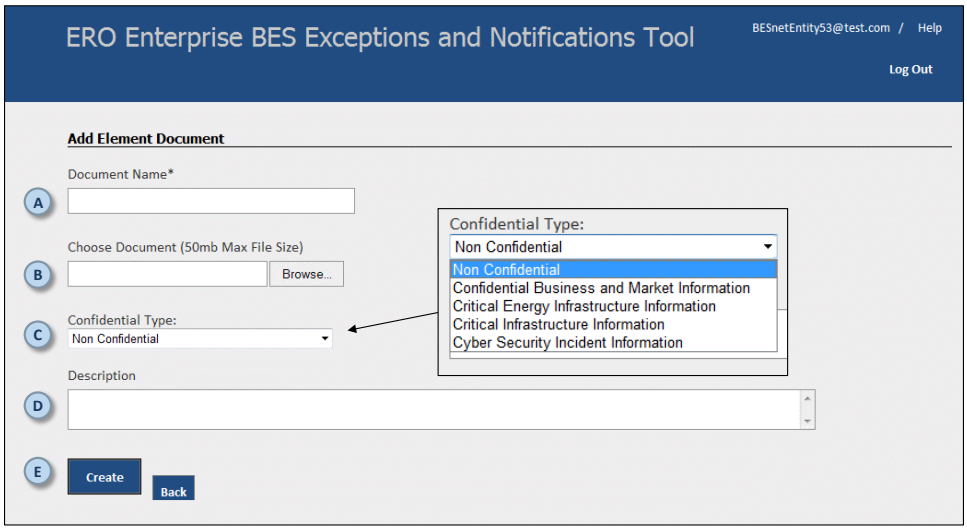


Figure 56: Add Element Document Screen

A. Provide a **Document Name** (A) for the document being attached.

B. Select a document using the **Choose Document** browsing area (B). NOTE: There is a 50 MB file size limit.

C. Select a **Confidential Type** (C) from the pull-down list.

D. Provide a **Description** (D) for the document.

E. When the **Add Element Document** form is completed, click on the **Create** button to attach the document to the Element. This will take the user back to the **Add Element Screen**



Figure 57: Add Element Screen Showing Attached Document

[3] Refer to the *BES Notification Review Guidelines* for additional information on necessary documentation.

When the supporting documentation has been attached to the Notification, the **Add Element Screen** will show that the **Document** (A) is attached to the Element. If additional files need to be attached as supporting documentation, the user should click on the **Add button** (B) and the **Add Document Screen** will appear again.

Certifying the Notification of Self-Determination

Before submitting the Notification of Self-Determination, the Notification must be certified by an authorized representative of the Entity. To do this, the representative's name and title must be entered on the **Create Notification of Self-Determination Screen** at (A).

The user must then select the **Certification** checkbox (B) before submitting the Notification.

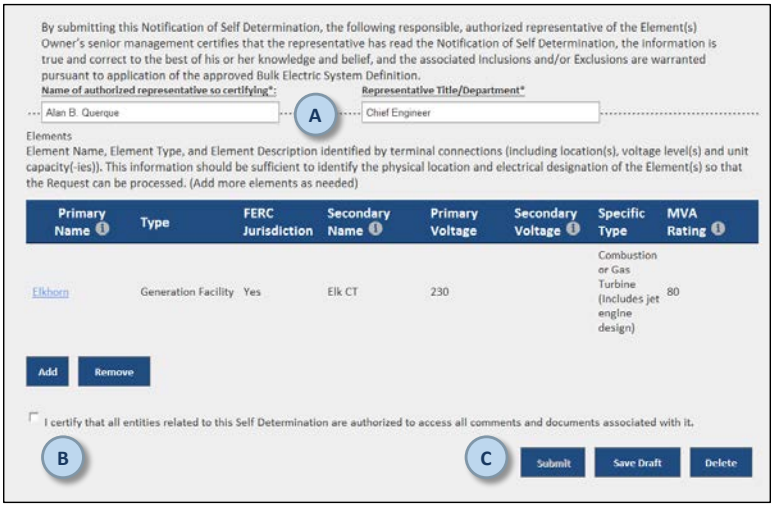


Figure 58: Create Notification of Self Determination Screen

Submitting the Notification of Self-Determination

To Submit the Notification of Self-Determination, the user should click on the **Submit button** (C) on the **Create Notification of Self-Determination Screen.** The user also has the option to **Save Draft** to allow the user to return to complete the draft Notification at a later time, as well as **Delete** to allow the user to completely delete the draft Notification.

The user will be returned to the **BESNet Dashboard** (Figure 59), showing that the submitted Notification is in Regional Review (A below). The **ID** for the Notification will also be complete with year, Region, NCR, and the SD number—SD indicating that the item is a Self-Determined Notification.

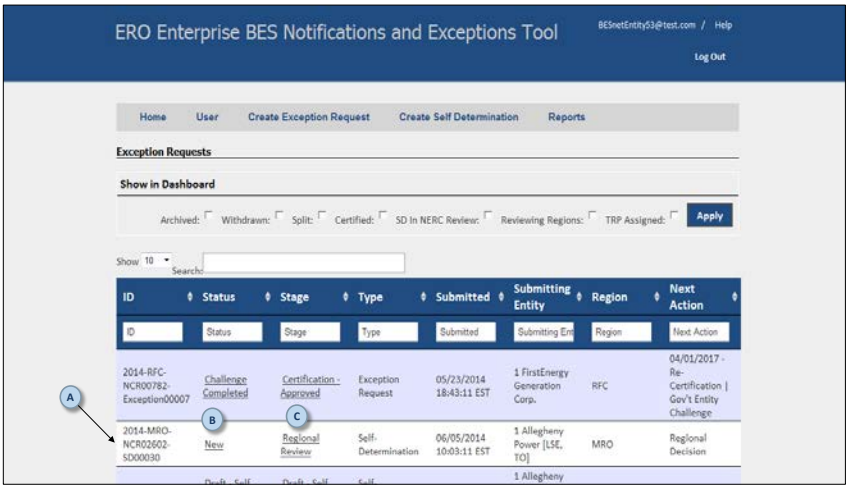


Figure 59: BESNet Dashboard with Self-Determined Notification in Regional Review

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BES Definition Implementation Guidance

August 25, 2014

RELIABILITY | ACCOUNTABILITY






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

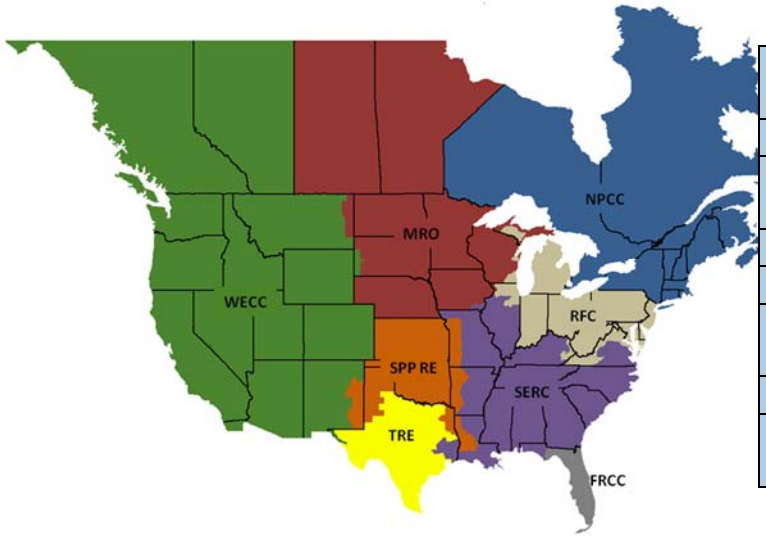
Table of Contents

Table of Contents ii
Preface iii
Introduction 4
Chapter 1 – Application of the BES Definition 1
Chapter 2 – Self-Determined Notifications and the BES Exceptions Request Process 3
Self-Determined Notifications 3
BES Exception Request Process 5
Appeal Process 5
BESnet Application Access 5
Chapter 3 – Registration Changes 7
Guidance on DP-Specific Registration Deactivation Requests 7
Chapter 4 – Reliability Standards Applicability 9
Dispersed Generation 9
Chapter 5 – FERC Local Distribution Determinations 10

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The following BES implementation guidance is offered to Regional Entities and Responsible Entities[1].

On December 20, 2012, the Federal Energy Regulatory Commission (FERC) issued Order No. 773[2] approving Phase 1 modifications to the currently effective NERC definition for Bulk Electric System (BES), which will become effective on July 1, 2014.[3] On December 13, 2013, NERC filed BES Phase 2 modifications for approval, with a requested effective date of July 1, 2014, to correspond with the Phase 1 effective date.[4] On March 20, FERC approved the Phase 2 modifications with a July 1, 2014 effective date.[5]

This document addresses implementation issues and communicates expectations for users, owners, and operators of the BPS,[6] registered entities, and Regional Entities during the transition period for the FERC-approved BES Definition. Specifically, this document covers the following:

- Application of the BES Definition
- Self-Determined Notifications and the BES Exceptions Request Process
- Registration Changes
- Reliability Standards Applicability
- Local Distribution Determinations

The revised BES Definition was developed through the NERC Standards Development Process for inclusion in the NERC Glossary.[7] The BES Definition removes language allowing for regional discretion and establishes a bright-line threshold that includes all Facilities operated at or above 100 kV. The revised BES Definition also identifies specific categories of facilities and configurations as Inclusions or Exclusions to the BES. Changes in classification of BES Elements due to the revised BES Definition (e.g., newly identified Inclusions or Exclusions) will be processed by NERC and the Regional Entities through the BES Notification and Exceptions Tool (BESnet application), to be made available by NERC by July 1, 2014.[8]

Additional information regarding application of the BES Definition can be found in the BES reference documents and training materials available at the NERC BES Definition web page:

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

[1] The term Responsible Entities refers to entities that are subject to registration as, or are registered as, users, owners or operators of the Bulk Power System (BPS).

[2] *Revisions to Electric Reliability Organization Definition of BES and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012); *order on reh'g*, Order No. 773-A, 143 FERC ¶ 61,053 (2013); *order denying reh'g*, 144 FERC ¶ 61,174 (2013).

[3] On June 6, 2013, FERC approved an extension of the Phase 1 BES effective date from July 1, 2013 to July 1, 2014.

[4] In Order No. 773, as clarified in Order 773-A, the Commission directed NERC to: (1) modify the Exclusions for radial systems (Exclusion E1) and local networks (Exclusion E3) so that they do not apply to tie-lines, *i.e.* generator interconnection facilities, for BES generators; and (2) modify the local network exclusion to remove the 100 kV minimum operating voltage to allow systems that include one or more looped configurations connected below 100 kV to be eligible for the local network exclusion. NERC addressed the Commission's directives in Phase 2 of the BES Definition. NERC requested expedited action for the Commission to approve the proposed Phase 2 BES Definition by no later than March 31, 2014. If approved by that time, the proposed Phase 2 BES Definition will go into effect on July 1, 2014, the effective date of the Phase 1 BES Definition. The proposed Phase 2 BES Definition will supersede, in its entirety, the Phase 1 version.

[5] *Order Approving Revised Definition*, 146 FERC ¶ 61,199 (2014).

[6] Users, owners and operators of the BPS are users, owners and operators of the BES.

[7] http://www.nerc.com/files/glossary_of_terms.pdf.

[8] The application will provide a common mechanism for each asset owner to provide notice to its Regional Entity of newly identified Exclusions and Inclusions after applying the BES Definition to its asset list.

Chapter 1 – Application of the BES Definition

Under the revised BES Definition, there are four methods for categorizing BES Elements:

1. Application of the BES Definition, allowing for Inclusions and Exclusions of Elements
2. Approval of removal or addition of Elements through the BES Exceptions Process
3. Determination by the Commission of whether an Element is "Local Distribution"
4. Determination by the Commission that an Element is included in the BES after an opportunity for notice and comment

The application of the BES Definition by an entity should generally be done in three steps:

STEP 1 (CORE DEFINITION): The core BES Definition is used to establish the bright line of 100 kV, the overall demarcation point between BES and Non-BES Elements.[9] The core BES Definition identifies the Real Power and Reactive Power resources connected at 100 kV or higher, as included in the BES.

STEP 2 (INCLUSIONS): This step involves applying the specific Inclusions to determine specific Elements that are included in the BES, such as certain Transmission Elements and Real Power and Reactive Power resources.

STEP 3 (EXCLUSIONS): This step evaluates specific situations for potential exclusion from the BES and should be applied in the sequence below:

> Exclusion E2 (Behind-the-Meter Generation) provides for the specific exclusion of certain Real Power resources that reside behind the retail meter (on the customer's side) and supersedes the more general Inclusion I2 (Generating Resources).
>
> Exclusion E4 (Reactive Power Devices) provides for the specific exclusion of Reactive Power devices installed for the sole benefit of a retail customer(s) and supersedes the more general Inclusion I5 (Static or Dynamic Reactive Power Devices).
>
> Exclusion E3 (Local Networks) provides for the exclusion of local networks that meet the specific criteria identified in the exclusion language. Exclusion E3 does not allow for the exclusion of Real Power and Reactive Power resources captured by Inclusions I2 through I5.
>
> Exclusion E1 (Radial Systems) provides for the exclusion of "Transmission Elements" from radial systems that meet the specific criteria identified in the exclusion language. Exclusion E1 does not allow for the exclusion of Real Power and Reactive Power resources captured by Inclusions I2 through I5.

As discussed below, an entity must submit any Self-Determined Notifications or requests for Exception to its Regional Entity and NERC through the BESNet application. Self-Determined Notifications are only required for: (i) Elements that were part of the BES under the original BES Definition and are not part of the BES under the new BES Definition; or (ii) Elements that were not part of the BES under the original BES Definition, but are now part of the BES under the new BES Definition.

[9] An "Element" is defined in the NERC Glossary as "[a]ny electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components."

FERC also approved a four-step BES transition plan for the revised BES Definition.[10] This BES transition plan provides a roadmap for entities to follow in moving from the current BES Definition to the revised BES Definition.

- Step 1: Identify a Comprehensive List of BES Facilities and Elements.
- Step 2: Perform a Gap Analysis.[11]
- Step 3: Develop Implementation Plans (for newly included Elements) to become compliant with Reliability Standards.
- Step 4: Complete Implementation Plans and Certify Completion.

A registered entity should follow the existing NERC Rules of Procedure set forth in Section 500 and Appendices 5A and 5B to submit requests for changes in Registration and Certification. To the extent an entity seeks de-activation or de-registration for a given functional designation due to application of the BES Definition, NERC will determine the appropriate time frame for making such a determination.[12]

[10] BES petition at pp 38-43 available at:
http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition_Rev_Def_BES_20120125.pdf.

[11] The Gap Analysis should identify:

(i) any Registration and/or Certification changes that are required due to the newly-identified Elements (e.g., reliability functions for which the entity is not currently registered on the Compliance Registry but should be registered based on the newly-included Elements), and

(ii) changes in compliance obligations for the entity, (i.e., the applicable Requirements of Reliability Standards with which the entity must now become compliant due to the inclusion or exclusion of the new Elements in the BES.)

[12] Order No. 773 at P 55.

Chapter 2 – Self-Determined Notifications and the BES Exceptions Request Process

Self-Determined Notifications

FERC has recognized that applying the new BES Definition may result in the identification of Elements that currently are treated as part of the BES but will no longer be considered part of the BES.[13] FERC further noted that registered entities are obligated to inform their Regional Entities and NERC of any Self-Determination that an Element is no longer part of the BES. For Notifications of Self-Determined Exclusions or Inclusions, the NERC BESNet application provides the functionality for entities to notify the Regional Entities of Self-Determined BES Inclusions and Exclusions.

With respect to a Self-Determined Notification of exclusion, the Regional Entities will validate, with NERC oversight, the submittal to determine complete and proper application of the BES Definition. The Regional Entities may request additional information, as needed, under existing authority, in order to establish a complete and proper Notification. In order to provide consistent application of the BES Definition and associated processes, NERC in its oversight role will review Self-Determined Notifications through sampling or other approaches, and will provide necessary guidance or direction to achieve consistent results. Compliance monitoring and enforcement obligations for Elements that are excluded through a correct application of the BES Definition will be considered to have ended as of the date that a complete Notification was submitted, barring any unique facts and circumstances. Incomplete Notifications of exclusion or incorrect applications of the BES Definition will continue to subject those Elements to compliance monitoring and enforcement until all required information is submitted and the BES Definition is correctly applied.

An entity makes a good faith[14] Notification of a Self-Determined Exclusion of a particular Element by properly applying the BES Definition and relevant Inclusions or Exclusions, then notifying its appropriate Regional Entity. **Good faith Self-Determinations are those that are made consistent with the BES Definition and reference materials provided by NERC.** With NERC oversight, the Regional Entity will validate the Notification to ensure that the BES Definition was properly applied and that no mistakes occurred.[15] Once validation is concluded, the registered entity will be advised of the determination. If additional information is required, the registered entity may be requested to supply it prior to the Regional Entity reaching a conclusion. An Element will not be excluded from the BES until the removal is validated. [16]

[13] *See* Order No. 773 at P 317; *see also* Order No. 773-A at P 110.

[14] Order No. 773-A at P 110 ("… [I]n the absence of bad faith, if a registered entity applies the [BES] Definition and determines that an element no longer qualifies as part of the [BES], upon notifying the appropriate Regional Entity that the element is no longer part of the [BES] the element should not be treated as part of the [BES] unless NERC makes a contrary determination in the exception process**.** If the Regional Entity disagrees with the classification of the element and believes the element is necessary for reliable operation, the Regional Entity should initiate an exception request to include the element in the [BES]. If NERC agrees with the Regional Entity and determines that the element should be included in the [BES], the registered entity should not be subject to retroactive liability for the time period the element was not included in the [BES].").

[15] The validation process is consistent with current practice with respect to Notifications to NERC Rules of Procedure Section 501.1.3.5, as well as Order Nos. 773 and 773-A. In Order No. 773, FERC stated that the Notification was a necessary feature, because NERC and the Regional Entities would need this information for their compliance programs, for audit purposes and to understand the contours of the BES within a particular region. Order No. 773 at P 317 (FERC further noted that, because entities had discretion to declassify certain facilities as part of the BES, NERC, the Regional Entities and FERC needed "notification of such instances to assure that the entities are appropriately implementing the revised definition."). *Id.*

[16] In Order No. 773-A, FERC responded to a circumstance in which a Regional Entity disagrees with the registered entity's determination that an element is not part of the BES and the registered entity acts in good faith, by outlining the appropriate process to use. Order No. 773-A at PP 108-109. FERC agreed that, in the absence of bad faith, and the Regional Entity believes the element is necessary for reliable operation, it should initiate an exception request to include the element in the BES. Order No. 773-A at P 110.

Taken together, Order Nos. 773 and 773-A, as well as the NERC Rules of Procedure, point to the need for NERC and the Regional Entity to review a Notification to determine if it comports with the Definition and validate the Notification to confirm appropriate application of the Definition. The registered entity can facilitate this effort by reviewing these situations with the Regional Entity prior to formally submitting the Notification. This will provide the greatest confidence of appropriate application of the BES Definition and facilitate consistent application of the Definition.

Until the validation process described for Self-Determined Notifications of exclusion is completed, the registered entity has the potential to be subject to applicable Reliability Standards. Any instances of non-compliance for potentially excluded Elements will be held in abeyance until such time as the Notification is validated by the Regional Entity, with NERC oversight as described above. If the Self-Determined Notification of exclusion is accepted as valid, instances of potential non-compliance involving excluded Elements that occurred after the submission of the complete and proper Notification up to the date of its validation will be closed, barring any unique facts and circumstances. A Self-Determined Notification of exclusion that is incomplete or based on improper application of the BES Definition will result in Elements associated with that Notification remaining subject to compliance monitoring and enforcement until such time all required information is submitted and the BES Definition is correctly applied.

If a Regional Entity believes that a Notification of a Self-Determined Exclusion is based on an incorrect application of the Definition and is unable to come to a common understanding of the Definition with the submitting entity, the Notification will be rejected and the Element at issue will remain part of the BES by application of the Definition.[17]

If a Regional Entity and NERC determine that an Element that is excluded as a result of properly applying the BES Definition should be included in the BES for other reasons, the Regional Entity would initiate an Inclusion exception request through the BESNet application and inform the registered entity. Once the process has been completed, the Element then would be included in the BES and the registered entity notified accordingly. The registered entity will not be subject to retroactive liability for the time period the Element was not included in the BES.

As discussed previously, the July 1 implementation date for the new BES Definition is rapidly approaching. As part of the transition across the ERO, NERC recognizes that entities may desire to submit Self-Determined Notifications of exclusion as soon as possible after the effective date. In order to accommodate all entities and manage the flow of processing such materials, NERC is providing an extended initial submittal period as described below.

NERC and the Regional Entities are committed to processing and efficiently managing these submissions in a timely manner for all entities. Accordingly, NERC requests that entities pace their submittals within period beginning July 1 and ending September 1 to ensure a smooth transition. Entities that submit a Notification during the period of July 1, 2014, through September 1, 2014, will be deemed to have submitted such Notification on July 1 for purposes of determining compliance obligations.

In other words, during this initial submittal period of activity, a Notification of Self-Determined exclusion will be treated the same as one received on July 1 when it comes to effective dates for compliance with NERC Reliability Standards. An extended initial submittal period will enable a levelized pace that can be more effectively managed for entities, NERC, and the Regional Entities.

[17] Order No. 773-A at PP 317 ("…[T]he revised definition allows entities the discretion to "declassify" certain facilities as part of the [BES], and NERC, Regional Entities and the Commission need notification of such instances to assure that the entities are appropriately implementing the revised definition.").

BES Exception Request Process

Appendix 5C of the NERC Rules of Procedure sets forth the process to be followed with respect to exception requests for Inclusion and Exclusion of Elements from the BES.[18]

If an Element that is already deemed part of the BES and subject to relevant Reliability Standards is included by application of the revised BES Definition, but an entity believes it has good reason for it not to be included, an entity may submit an Exclusion exception request for the Element through the BESnet application. The Element will remain subject to the relevant Reliability Standards during the pendency of the exception process. All existing BES Elements consistent with the BES Definition continue to remain subject to Reliability Standards—with no gap in coverage or compliance obligations—when the new BES Definition goes into effect on July 1, 2014.

As noted in Order No. 773-A (at P 26), entities with newly included Elements may file exception requests (after a gap analysis is performed). Regional Entities and NERC will make determinations for the exception requests submitted during the 24-month implementation period applicable to newly included Elements. Accordingly, newly included BES Elements will only become subject to relevant Reliability Standards 24 months after the effective date of the revised BES Definition (i.e., July 1, 2016).

If, after validation by the Regional Entity and NERC of a Self-Determined Notification of Exclusion, an Element is excluded from the BES by application of the revised BES Definition, a third-party entity with a reliability oversight obligation may submit an Inclusion exception request to include the Element in the BES as part of the exception process. The Element will not be subject to Reliability Standards during the pendency of the Inclusion exception process.

As noted in the BES transition plan (Steps 3 and 4 above) an entity with newly included Elements may need to develop a Registration implementation plan (which may include the need for Certification or a revision to an existing Certification), a compliance implementation plan, or both. If the Regional Entity and registered entity are unable to agree on the implementation plan, the Regional Entity will notify NERC, and NERC will specify a reasonable implementation schedule.

Finally, to the extent an Element is needed to comply with a Reliability Standard that is based on facility characteristics (e.g., FAC-003 200 kV threshold for individual transmission lines), the Element would not be excluded under the exception process. However, such entities could be considered for a sub-list of Reliability Standards, as appropriate.

Appeal Process

Section 500 and Appendices 5A and 5B of the NERC Rules of Procedure provides for appeals of entity registration and certification decisions.

BESnet Application Access

Requests for Exceptions to the BES will only be accepted through the BESnet Application. Entities that anticipate submitting a BES exception request should contact their applicable Regional Entity contact below, review the relevant training and resource materials, and establish a user account for the BESnet Application.

[18] http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

Region	Method of Contact
FRCC	Send email to bes@frcc.com
MRO	Send email to besnet@Midwestreliability.org
NPCC	Send email to bes@npcc.org
RF	Online at https://www.rfirst.org/Pages/ContactUs.aspx
SERC	Send email to serccomply@serc1.org
SPP	Send email to sppreregistration@spp.org
TRE	Send email to bes@texasre.org
WECC	Send email to support@wecc.biz

Reference materials for Regional Entities either are being or have been developed—and will be provided to Responsible Entities for informational purposes—regarding: (1) BES Guideline for Reviewing Self-Determined Notifications; (2) BES Exception Request Evaluation Guideline; (3) BESNet Application User Guide; and (4) Frequently Asked Questions (FAQs). In addition, a BES Definition Reference Document developed through the NERC standards drafting process has been made available to Responsible Entities to demonstrate proper application of the BES Definition.

Chapter 3 – Registration Changes

NERC's objective in implementing the revised BES Definition is to ensure that the proper entities are registered and responsible for Reliability Standards that are necessary to ensure the reliability of the BPS. In Order No. 773 (at P 55), FERC stated, "[w]e do not expect there to be significant numbers of entities either needing to register or deregister due to the change in definition." NERC shares FERC's expectation that only a small number of entities will require changes to their NERC registration as a result of the revised BES Definition.

An entity seeking to modify its current registration, including de-registration or deactivation, must inform its applicable Regional Entity of this change in status. In turn, the Regional Entity will notify NERC of such changes. All changes to registration are processed by the NERC Registration and Certification department, in accordance with the NERC Rules of Procedure.

Guidance on DP-Specific Registration Deactivation Requests

For entities registered for the Distribution Provider (DP) function, and that currently own or operate BES protection schemes, including Underfrequency Load Shedding (UFLS), Undervoltage Load Shedding (UVLS), or Special Protection Systems (SPS) and Remedial Action Schemes (RAS), these devices support the reliability of the Bulk Electric System (BES), often serving as the "last-resort" tool for avoiding a total power system blackout. Consequently, NERC and the Regional Entities will not approve the deactivation of the DP function for Registered Entities on the NERC Compliance Registry that have these types of protection devices, solely on the basis that the entity does not own or operate a BES Element by application of the BES Definition. NERC and the Regional Entities will evaluate the relevant facts and circumstances in reaching a decision.

Registered Entities currently performing the DP function may determine to file a Self-Determined Notification of Exclusion of Elements based on the current BES Definition. There is no automatic change in the registration status of an entity for any functional registration categories if a particular Element is excluded from the BES Definition either through the Self-Determined Notification of Exclusion or the BES Exception process. Determinations of registration status are addressed through the registration program. NERC believes that the deactivation of the DP function registration of Registered Entities that have responsibilities relating to BES protection schemes including UFLS, UVLS, and SPS/RAS equipment would present a reliability risk due to the lack of compliance oversight. These types of equipment are essential to the reliable operation of the BES, even in cases where the equipment is installed below the BES 100 kV bright line. In addition, NERC will closely evaluate requests which involve entities that have transmission Remedial Action Schemes or other types of schemes that have the same or similar BES system protection objectives.

Registered Entities should note that if an Element owned by an entity is excluded from the BES Definition, either through an Exclusion Exception Request or a validated Self-Determined Notification of Exclusion, this exclusion alone does not necessarily provide for deactivation of any functional registration from the NERC Compliance Registry. The Registration Criteria states that a "Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System." The list includes references to required UFLS programs, UVLS programs, SPS/RAS and transmission Protection Systems. The importance of these programs to system reliability is not diminished by the revised BES Definition.

Under the current registration rules, entities have an opportunity to establish that they are not material to the reliability. Such determinations depend on the specific facts and circumstances. In the future, NERC is moving forward with a new proposal for Distribution Provider registration criteria related to the Risk-Based Registration (RBR) initiative. The proposed criteria will accommodate those DPs who are registered only as a result of the owning of UFLS systems and will include a reduced set of reliability standards for which UFLS-Only DPs will be

responsible. RBR also will build on current authority to allow an entity to make a case that it should not remain registered if it is not material to the reliability of the BES. To ensure consistency, a new materiality test is being developed that would be reviewed by a new NERC-led panel comprised of NERC and Regional Entity participants, that the entity is not material to the reliability of the BES and should not remain registered as a DP. The draft design program also includes a process for determining a sub-set of applicable Reliability Standards.

NERC notes that, to the extent that direct application of the BES Definition results in a determination that an Entity's Elements are not BES, an Inclusion Exception process can be initiated by a Responsible Entity to bring such Elements back into the BES. While this would not affect the DP registration status, it may affect other functional registration categories.

Chapter 4 – Reliability Standards Applicability

On a case-by-case basis, NERC may determine if an entity is eligible for a sub-list of applicable Reliability Standard requirements rather than automatically subjecting the entity to the full scope of standards applicable to a particular function. This occurs through the NERC Organization Registration process, in concert with the respective Regional Entity.[19] To initiate a request for a sub-list of applicable Reliability Standards, an entity must inform its Regional Entity contact. As part of its Risk-Based Registration Initiative that was launched in 2014, NERC will lead a review panel with participation by Regional Entities to evaluate, among other things, subsets of applicable Reliability Standard requirements for certain functional entities.

NERC has previously worked with industry to modify applicability designations for Reliability Standards that affect large groups of entities. For example, to address a reliability gap for generator interconnection facilities, FERC recently approved the NERC GO-TO Project.[20] Specifically, in Order No. 785, FERC approved modifications to the applicability sections for Reliability Standards FAC-001-1, FAC-003-3, PRC-004-2.1a, and PRC-005-1.1b.[21] FERC also noted that a small number of "complex" facilities may be subject to additional Reliability Standards than those approved in the GO-TO Project.[22] NERC will continue to address these "complex" facilities on a case-by-case basis.

Dispersed Generation

Project 2014-01 Standard Drafting Team is focusing on identifying Reliability Standard requirements applicable to dispersed power-producing resources. The list developed from the Standards Authorization Request (SAR) may provide a subset of applicable Reliability Standards. Once the Standard Drafting Team concludes its work, NERC will determine next steps, as part of the Risk-Based Registration Initiative.

[19] NERC has identified a corporate goal for 2014 to examine the registration and certification framework.

[20] *Generator Requirements at the Transmission Interface*, Order No. 785, 144 FERC ¶ 61,221 (2013).

[21] FERC approved NERC's request for an effective date of one year following the first quarter after regulatory approvals for FAC-001-1, and for FAC-003-3 Requirement R3. For the remaining requirements of FAC-003-3, FERC approved an effective date of two years following the first calendar quarter after regulatory approvals. FERC also approved that PRC-004-2.1a and PRC-005-1.1b become effective upon receiving required regulatory approvals. (*See* Order No. 785 at P 9).

[22] Order No. 785 at P 53 ("Consistent with prior decisions in *New Harquahala Generating Co., LLC*, and *Cedar Creek Wind Energy, LLC*, for the anticipated small number of generator owners and operators owning facilities deemed to be "complex" and therefore potentially subject to additional Reliability Standards, NERC should evaluate, in consultation with the Regional Entity, which Reliability Standards should apply to the particular entity based on the specific facts and circumstances.").

Chapter 5 – FERC Local Distribution Determinations

In Order No. 773 (at P 66) FERC approved NERC's BES exception request process to determine the technical issue of whether facilities are part of the BES; however, FERC determined that it (FERC) will decide the jurisdictional question of whether facilities are "used in local distribution." Thus, FERC reserved authority to designate sub-100 kV facilities, or other facilities, as part of the BES.

FERC also established a process by which an entity can seek a determination by FERC as to whether facilities are "used in local distribution" as set forth in the Federal Power Act. FERC will make such case-by-case jurisdictional determinations by starting with the Seven-Factor Test set forth in Order No. 888.

When and whether to submit such a jurisdictional question to FERC are business and legal decisions for a registered entity, upon which NERC is not opining in this guidance document.

Canadian Provincial Summaries of Standard-Making and Enforcement Functions with U.S. Comparators

Last Updated: October 9, 2014

The Federal, Provincial, and Territorial Monitoring and Enforcement Sub-group (MESG) developed the following Canadian provincial summaries and will review them annually and update them as needed. If you have comments on the summaries, please submit them to NERC Director of Canadian Affairs Laura Hussey.

The provincial summary for Manitoba will be posted as soon as it is finalized.

Alberta - US Comparator:
Standard-Making and Enforcement Functions

Fast Facts about Alberta's Electricity System

Total annual consumption: 77,451 GWh
(2013)
Customers: approx. 1,632,000
Installed capacity: 14,500 MW (2013)
Record summer peak: 10,063 MW
Record winter peak: 11,139 MW (2013)
Total length of transmission system: 26,000 km
Interconnections: British Columbia, Saskatchewan (DC), Montana

Current Reliability Standards

Below is a link to current reliability standards in Alberta:
http://www.aeso.ca/rulesprocedures/17006.html

Key Organizations in Alberta's Electricity Sector

Alberta Energy

Alberta Energy is responsible for setting the policy and legislative framework for Alberta's electricity system. Alberta Energy develops solutions and advises on all aspects of energy policy for Alberta, including electricity, natural gas and oil.

Alberta Utilities Commission

The Alberta Utilities Commission ("AUC or Commission") is an independent, quasi-judicial agency of the Province of Alberta. The AUC regulates the utilities sector, and is responsible to ensure that the delivery of Alberta's utility service takes place in a manner that is fair, responsible and in the public interest. The AUC has authority to approve as effective in Alberta, reliability standards filed before it by the AESO, or to reject reliability standards based upon the recommendation of the AESO. The AUC must follow the AESO's recommendation related to Alberta reliability standards unless an interested person satisfies the AUC that the recommendation is either "technically deficient" or "not in the public interest". The AUC is the adjudicative body for compliance enforcement in respect of both ISO rules and Alberta reliability standards.

Alberta Electric System Operator

The Independent System Operator (ISO) in the Province of Alberta is the Alberta Electric System Operator ("AESO") – a statutory corporation pursuant to the *Electric Utilities Act, 2003* ("the Act"). Its statutory mandate requires it to direct the reliable operation of the Alberta interconnected electric system (AIES), plan the transmission system, and operate the wholesale electricity market. The AESO also evaluates Alberta's current and short-term electricity needs, and the adequacy and reliability of the integrated power system to meet those needs. As set out in the Alberta Transmission Regulation, the reliability standards applicable in Alberta are the standards adopted by the AESO following public consultation with those

market participants that it considers likely to be directly affected by the Alberta reliability standards, and AUC approval. The AESO is also mandated by the Act and the Transmission Regulation to 'establish practices and procedures' and 'monitor' the compliance of market participants with ISO rules, with AUC rules, and with Alberta reliability standards.

Market Surveillance Administrator

The Market Surveillance Administrator ("MSA") is a statutory corporation established under the *Electric Utilities Act, 2003* of the Province of Alberta and continued under the *Alberta Utilities Commission Act, 2007*. The mandate of the MSA is to carry out surveillance in respect of the Alberta electricity markets and the Alberta retail gas market to ensure they operate in a fair, efficient, and openly competitive manner. The scope of the MSA's legislative mandate includes the enforcement of ISO rules and reliability standards effective in Alberta. Under rules established by the AUC, the MSA may issue specified penalties for contravention of ISO rules or reliability standards or may request a hearing or other proceeding before the AUC to seek an administrative penalty or other relief. The MSA's mandate of enforcement for both ISO rules and Alberta reliability standards extends to Alberta market participants and the AESO.

Table Definitions

Provincial Organization: the Alberta organization accountable and responsible for performing the function according to provincial legislation for matters concerning Alberta entities.

US Organization: the US organization engaged to perform the function according to an executed Memorandum of Understanding for matters concerning Alberta entities.

US Comparator: the US organization that is responsible for performing the functions according to US law.

Functions		Provincial Organization	Relevant US Organization	US Comparator
Standards Making	Standards Approval	AUC (1)	Not Applicable	FERC
	Standards Development	AESO (1)	NERC (1)	NERC, WECC
	Entity Registration	AESO (2)	Not Applicable	NERC and WECC in their respective roles
Compliance Monitoring	Compliance Monitoring and Violation Detection	AESO/MSA (3)(5)(6)	WECC (3)	NERC and WECC in their respective roles, FERC
Enforcement Processes	Execution of Investigations	AESO/MSA (7)	Not Applicable	NERC and WECC in their respective roles, FERC
	Violation Determination and Sanction Imposition	MSA (8)(9)(10)	Not Applicable	NERC, WECC, FERC
Violation Prevention and Outreach	Violation Prevention, Outreach, including education	AESO/MSA (4)	NERC and WECC	NERC, WECC, FERC
Appeals	First Right of Appeal	AUC (11)	Not Applicable	NERC
	Second Right of Appeal	Review and Variance application to the AUC (12)	Not Applicable	FERC
	Third Right of Appeal	Court of Appeal of Alberta (13)	Not Applicable	US Court of Appeals
Oversight	Approval of Alberta's Rules of Procedure	Not applicable	Not Applicable	FERC
	Approval of Alberta's Compliance Monitoring Plan	AESO (5)/MSA (6)	Not Applicable	NERC and WECC
	Performance Oversight of CMP	AESO (5)/MSA (6)	Not Applicable	NERC BOT CC
	Violation Prevention and Outreach	AESO/MSA	NERC and WECC	NERC and WECC in their respective roles, FERC

Notes:

1. **Standards Approval:** Pursuant to section 20 of the Alberta Transmission Regulation, NERC is recognized as the Electricity Reliability Organization (ERO) in Alberta. NERC reliability standards are assessed by AESO subject matter experts together with the Alberta Reliability Committee (ARC). The ARC advises the AESO on the adoption of NERC standards as Alberta standards. The AESO must consult with market participants who are likely to be directly affected and must file proposed standards with the AUC with its recommendation to approve or reject a standard. In accordance with the Transmission Regulation, the AUC must follow the recommendation of the AESO unless an interested party satisfies the AUC that the recommendation of the AESO is either technically deficient or not in the public interest.

2. **Entity Registration:** Market participants have a duty to comply with Alberta reliability standards that are applicable to them under the Act. The AESO maintains a registry that is used to administer the compliance monitoring program, including scoping and scheduling of monitoring activities. Not being registered does not remove the market participant from complying with the Alberta Reliability Standards. The AESO bases registration on the Alberta Reliability Standards Functional Model and Criteria for Registration which maps Alberta market participant roles to the AESO functional model roles.

3. **Compliance Accountability:** The Alberta Transmission Regulation mandates that the AESO monitor the compliance by market participants with Alberta reliability standards. Further to the MSA's mandate under the Alberta Utilities Commission Act, the MSA oversees compliance of the AESO in respect of Alberta reliability standards applicable to the AESO. The MSA has entered into a services agreement with WECC such that WECC conducts compliance monitoring of the AESO under the auspices of the MSA.

4. **Prevention and Outreach:** The AESO conducts periodic stakeholder meetings for the purpose of updating entities on standards development activities and changes to the compliance monitoring program. In addition, the MSA provides guidance on compliance trends and expectations via its compliance reporting activities.

5. **Monitoring:** Pursuant to the Alberta Transmission Regulation and ISO rules, the AESO has established the Alberta Reliability Standards Compliance Monitoring Program (CMP) and associated processes and procedures for monitoring Alberta market participants. The AESO oversees performance of the CMP.

6. **Monitoring:** The MSA is the compliance monitor with respect to the AESO. In this regard, the MSA has entered into a service agreement with WECC to conduct compliance monitoring of the AESO under the auspices of the MSA including self-certification and compliance audits. Under the service agreement, WECC assists the MSA in the development of an Implementation Plan annually.

The Implementation Plan is applicable solely to the AESO and is subject to MSA approval and oversight.

7. **Investigations:** The AESO and WECC (as applicable) are required to refer suspected contraventions of Alberta reliability standards to the MSA for disposition. The MSA may also investigate and make its own independent conclusions for violation determinations and sanctions for all Alberta entities, including the AESO.

8. **Violation Determination and Sanction Imposition:** MSA makes violation and sanction determinations for all Alberta entities and the AESO. In accordance with AUC rules, the MSA may issue a notice of specified penalty for contravention of an Alberta reliability standard. Alternatively, the MSA may seek an administrative penalty before the AUC or other relief. The maximum administrative penalty amount is $1,000,000 per day on which the contravention occurs or continues.

9. **Violation Determination and Sanction Imposition:** NERC and WECC have no authority to impose sanctions on Alberta entities or the AESO.

10. **Public Disclosure:** In the event that the MSA issues a notice of specified penalty for contravention of a reliability standard, the name of the responsible entity is made public on the MSA website in accordance with AUC rules. A copy of the notice of specified penalty issued to the entity is typically the form of disclosure. In the event of an administrative proceeding before the AUC, the outcome of the proceeding is made public in an AUC decision.

11. **Appeals to MSA Determinations:** If a registered entity or the AESO fails to pay or disputes a specified penalty issued by the MSA, the MSA is required to notify the AUC and request a hearing. The AUC may confirm or rescind the notice of specified penalty or may impose an administrative penalty.

12. **Review of AUC Decisions:** A registered entity or the AESO may seek application to review and vary a decision of the Commission.

13. **Legal Review of AUC Decisions:** A registered entity or the AESO may seek leave to appeal a decision of the AUC with the Court of Appeal of Alberta.

British Columbia – United States Comparator: Standard-Making and Enforcement Functions

Fast Facts about British Columbia's Electricity System

Total annual consumption: approx. 63 Terawatt-hours TWh
Customers: over 2 million
Installed capacity: approx. 13,000 MW
Record summer peak: provincial peak not available
Record winter peak: 10,113 MW Nov. 2006[1]
Total length of transmission system: approx. 20,600 km[2]
Interconnections: British Columbia is part of the Western Interconnection which includes BC, Alberta, all or part of 14 western States and the northern portion of Baja California, Mexico. BC has direct interconnections to Alberta and Washington.

Reliability Standards Currently in Effect

Below is a link to a list of Mandatory Reliability Standards adopted in BC, accessed from both the BCUC and WECC websites:
http://www.wecc.biz/Standards/BCApproved%20Standards/Forms/AllItems.aspx

Key Organizations in British Columbia's Electricity Sector

Ministry of Energy and Mines

The Ministry of Energy and Mines is responsible for British Columbia's electricity sector. The Ministry develops and oversees British Columbia's (BC) policies with regard to electrical power generation and transmission, including replacing and upgrading infrastructure. See the *2007 BC Energy Plan: A Vision for Clean Energy Leadership.* The Ministry also develops and implements policies to ensure reliable electricity supply through mandatory reliability standards and participation with the Western Electricity Coordinating Council. The Ministry administers statutes relating to the energy sector and has policy responsibilities under the *Utilities Commission Act*. The Ministry also oversees the British Columbia Hydro and Power Authority (BC Hydro) through the *British Columbia Hydro and Power Authority Act.*

British Columbia Utilities Commission (BCUC)

The British Columbia Utilities Commission (Commission) is an independent, quasi-judicial, regulatory agency that operates under and administers the *Utilities Commission Act*. The Commission's primary responsibility is the regulation of energy utilities under its jurisdiction to ensure that the rates charged for energy are fair, just and reasonable, and that utilities provide safe, adequate and secure service to their customers. The Commission's mandate in the MRS Program is described in legislation and the *Mandatory Reliability Standards Regulation* (MRS Regulation), *BC Reg. 32/2009, MO39*. Specifically, the Commission adopts or rejects reliability standards in BC and is responsible for the administration of the MRS Program

[1] BC Hydro data only, BC Hydro 2007 annual report
[2] Compiled from BC Hydro and FortisBC annual reports and Rio Tinto Alcan information

in BC. In addition, the Commission also has the authority to impose administrative penalties for contraventions of MRS in accordance with the *Utilities Commission Act* and the *Administrative Penalties Regulation, BC Reg. 316/2012, OIC 731/2012.*

Western Electricity Coordinating Council

The Commission engaged the Western Electricity Coordinating Council (WECC) as the Commission's Administrator for the MRS Program in BC. Through the Administration Agreement the Commission grants WECC authority to act as the Commission's Administrator in the assessment of registration criteria and administration of approved reliability standards in BC. WECC's authority is limited to actions and obligations specified in the Commission's Rules of Procedure for reliability standards in BC, as well as the Registration Manual and Compliance Monitoring Program, or as otherwise ordered by the Commission.

British Columbia Hydro and Power Authority

The British Columbia Hydro and Power Authority (BC Hydro) is a provincially owned crown corporation and the largest electric utility in BC. BC Hydro delivers electricity to its customers through a network of over 75,000 kilometres of transmission and distribution lines and its system connects with other transmission systems in Alberta and Washington State. BC Hydro's responsibilities in the MRS Program are outlined in the Utilities Commission Act and MRS Regulation. Specifically, BC Hydro evaluates MRS for suitability for BC according to certain criteria stated in accordance with the Act and the MRS Regulation. In consultation with stakeholders, BC Hydro assesses reliability standards approved by FERC and reports to the Commission on their suitability for adoption in BC.

Table Definitions:

Provincial Organization: the British Columbia (BC) organization accountable and responsible for performing the function according to provincial legislation for matters concerning entities in BC.

US Organization: the US organization assisting the Commission in administrative matters related to the function described, in accordance with the approved Administrative Agreement (Order G-123-09, Oct. 15, 2009)

US Comparator: the US organization responsible for performing the functions in the United States.

Functions[3]		Provincial Organization	Relevant US Organization Assisting BCUC in Day-to-Day Administration	US Comparator
Standards Making[4]	Standards Approval	BCUC (1)	Not Applicable	FERC
	Standards Development	Not applicable	NERC and WECC	NERC and WECC
	Entity Registration	BCUC (2)	WECC (2)	NERC and WECC in their respective roles
Compliance Monitoring	Compliance Monitoring and Violation Detection	BCUC (3)	WECC (3)	NERC or WECC in their respective roles, FERC
Enforcement Processes	Execution of Investigations (4)	BCUC (5)	WECC (5)	WECC or NERC in their respective roles, FERC
	Violation Determination and Imposes Administrative Penalties	BCUC (6)	WECC recommends NOAVs to BCUC	WECC , NERC, or FERC
Violation Prevention and Outreach	Violation Prevention, Outreach, including Education (7)	BCUC to a limited extent	WECC	WECC, or NERC in their respective roles, FERC
Appeals	First Right of Appeal	BCUC	Not applicable	NERC Board of Trustees Compliance Committee (BOT CC)
	Second Right of Appeal	Supreme Court or Court of Appeal (8)	Not applicable	FERC
	Third Right of Appeal	Not applicable	Not applicable	US Court of Appeals
Oversight	Approval of BC's Rules of Procedure	BCUC	Not applicable	FERC
	Approval of BC's Compliance Monitoring Program and Implementation Plan	BCUC	Not applicable	FERC for approval of the CMEP and NERC for approval of a Regional Entity's Implementation Plan
	Performance Oversight of CMP	BCUC	Not applicable	WECC, or NERC BOT CC in their respective roles

[3] This table is intended to illustrate *who has authority over these various processes* vs. *who has authority for their execution.*
[4] Reliability standards Include FERC approved NERC reliability standards and FERC approved regional reliability standards.

Notes:

1. **Standards Approval:** Pursuant to section 125.2(2) of the *Utilities Commission Act* (Act) the British Columbia Utilities Commission (BCUC in table above) has exclusive jurisdiction to determine whether a "reliability standard" as defined in the Act, is in the public interest and should be adopted in BC. To provide the necessary information required for determinations and in accordance with the Act, British Columbia Hydro and Power Authority (BC Hydro) submits a Mandatory Reliability Standard (MRS) Assessment Report to the Commission assessing the new and revised reliability standards adopted in the US by the Federal Energy Regulatory Commission (FERC) within the annual assessment period (December 1 to November 30). The Assessment Report is developed in consultation with Registered Entities in the BC MRS Program. Further, in consultation with stakeholders regarding the estimated time required for the entities to implement and come into compliance with the reliability standards, BC Hydro suggests BC effective dates for each of the reliability standards assessed. After a public comment process, the Commission adopts reliability standards in the Assessment Report to maintain or achieve consistency with other regions, unless the Commission determines otherwise after a hearing.

2. **Entity Registration:** Entities subject to adopted Mandatory Reliability Standards are required to register with the Commission. The Western Electricity Coordinating Council (WECC) in its role as the Commission's Administrator for the BC Mandatory Reliability Standards Program (BC MRS Program) reviews registration materials provided by all applicable Entities and makes recommendations to the Commission.

3. **Compliance Monitoring:** The Rules of Procedure for reliability standards in British Columbia include the Compliance Monitoring Program and describe the procedures for monitoring and enforcement of adopted reliability standards. The processes include among other things Audits, Self-Certifications, Spot-Checks, Self-Reports, and Periodic Information (Data) Submittals. An annual Implementation Plan, recommended by WECC and approved by the Commission, identifies the Actively Monitored Standards List and schedules for the procedures listed above for the up-coming year. WECC assists the Commission with the compliance monitoring activities for BC entities in accordance to the annual Implementation Plan approved by the Commission.

4. **Execution of Investigations:** The Commission may execute investigations and may direct WECC to execute investigations..

5. **Investigations:** As the Commission's Administrator, WECC may conduct investigations at the direction of the Commission.

6. **Violation Determination and Sanction Imposition:** The Commission makes violation determinations for all BC entities and pursuant to Bill 30 – 2012, the Energy and Mines Statues Amendment Act – 2012, has the authority to impose administrative penalties and set financial limits for confirmed violation of a reliability standard. Penalty maximums are outlined in the Administrative Penalties Regulation. The process for imposing penalties for confirmed violation of reliability standards is under development at this time.

7. **Violation Prevention and Outreach:** The Commission communicates openly with entities and endeavours to foster a culture of compliance with the BC MRS Program. The Commission has offered educational workshops to entities from time to time and relies on WECC for entity outreach on technical matters. In addition to alerts and other publications issued by NERC and/or WECC to help inform entities and prevent violations, the Commission may issue similar notices for this purpose. WECC considers prevention of recurrence when reviewing mitigation plans before recommending them for acceptance by the Commission.

8. **Appeals to Commission Determinations:** There are two (2) avenues of recourse for enforcement decisions made by the Commission: first through the Commission's Application/Request for Reconsideration and, subsequently, through an appeal to the BC Supreme Court or BC Court of Appeal.

9. **Public Disclosure:** Possible and Alleged Violations are confidential unless the Commission determines they are Confirmed Violations and the Commission considers that disclosure would not relate to a cyber-security incident or otherwise jeopardize the security of the Bulk Power System.

New Brunswick - US Comparator: Standard-Making and Enforcement Functions

Fast Facts about New Brunswick's Electricity System

Total annual consumption: 12.885 Terawatt-hours TWh (2012-2013)
Customers: approx. 394,000
Installed capacity: 4,069 MW
Record peak (winter): 3,333 MW (2004)
Total length of transmission system: 6,849 km (4,226 miles)
Interconnections: Quebec, Nova Scotia, Maine, PEI

Reliability Standards Currently in Effect

Below is a link to the reliability standards currently in effect in New Brunswick:
http://www.nbeub.ca/index.php/en/electricity/reliability-compliance/new-brunswick-approved-reliability-standards

Key Organizations in New Brunswick's Electricity Sector

Department of Energy and Mines

The New Brunswick Department of Energy and Mines is responsible for setting the policy and legislative framework for New Brunswick's electricity system. The Department administers the Electricity Act and Reliability Standards Regulation which establishes the authority and requirements for the adoption and enforcement of electric reliability standards in New Brunswick.

New Brunswick Energy and Utilities Board

The New Brunswick Energy and Utilities Board (NBEUB) is an independent, quasi-judicial board that regulates New Brunswick's electricity sector. The NBEUB has the responsibility under the Electricity Act to adopt and enforce reliability standards in New Brunswick. The NBEUB implements the Reliability Standards Regulation which addresses the adoption of standards, determination of the bulk power system, compliance registrations and compliance monitoring and enforcement processes.

New Brunswick Power Corporation

The New Brunswick Power Corporation (NBPC) is a Crown corporation and the province's vertically integrated electric utility. In addition to its responsibility to comply with reliability standards applicable to its functions, NBPC is also responsible under the Electricity Act to make filings to the EUB to update reliability standards, maintain a list of bulk power system elements and to make recommendations on compliance registrations.

Table Definitions:

Provincial Organization: the New Brunswick organization accountable and responsible for performing the function according to provincial legislation.

US Organization: the US organization responsible for performing the function according to an executed agreement for the provision of services.

US Comparator: the US organization responsible for performing the functions in the US according to US law.

Functions[1]		Provincial Organization	Relevant US Organization	US Comparator
Standards Making[2]	Standards Approval	NBEUB (1)	Not Applicable	FERC
	Standards Development	Not Applicable	NERC	NERC NPCC
	Entity Registration	NBEUB (2,3)	NPCC Recommendations to NBEUB (4)	NERC NPCC
Compliance Monitoring	Compliance Monitoring and Violation Detection	NBEUB	NPCC (5)	FERC NERC NPCC
Enforcement Processes	Execution of Investigations	NBEUB	NPCC (6)	FERC NERC NPCC
	Violation Determination and Sanction Imposition	NBEUB	NPCC recommendations to NBEUB (7)	FERC NERC
Violation Prevention and Outreach	Violation Prevention, Outreach, including education	N/A	NERC/ NPCC	FERC NERC NPCC
Appeals	First Right of Appeal	NBEUB Review or Hearing	Not Applicable	NPCC Hearing Body
	Second Right of Appeal	NBEUB Appeal (8)	Not Applicable	NERC Board of Trustees Compliance Committee (BOT CC)
	Third Right of Appeal	A person aggrieved by an order of the NBEUB can make an application for judicial review to The Court of Appeal of New Brunswick.	Not Applicable	FERC
Oversight	Approval of New Brunswick's "rules of procedure"	Lieutenant Governor in Council (9)	Not Applicable	FERC
	Approval of New Brunswick's Compliance Monitoring and Enforcement Implementation Plan	NBEUB	NPCC Recommendations to EUB (10)	NERC NPCC
	Performance Oversight of CMEP	NBEUB	Not Applicable	NERC BOT CC

[1] This table is intended to illustrate *who has authority over these various processes* vs. *who has authority for their execution.*
[2] Reliability standards include FERC approved NERC reliability standards and FERC approved regional reliability standards.

Notes:

1. **Standards Approval:**
   Authority- Pursuant to Section 119 of the *Electricity Act* and the *Reliability Standards Regulation*, the NBEUB may approve NERC reliability standards that have been approved by FERC and filed by NBPC, with or without NB amendments.

   NERC Standards Filing- NBPC files standards with the NBEUB for approval within 60 days of the FERC approval effective date.

   Standard Review- NBPC reviews NERC standards and files with an accompanying NB Appendix to describe the specific application of the standard in NB.

   Public Process- the NBEUB notifies NERC, NPCC and NB Registered Entities when NBPC files an application for approval and the filed materials are publically available on the NBEUB website for a 60 day comment period.

   Approval/Remand – NBEUB approves the application as filed unless there are substantive revisions to the FERC approved version, or if there are substantive comments received during the review period , in which case the NBEUB may hold a hearing and may determine to approve, not approve or remand the proposed reliability standard back to NBPC.

2. **Bulk Power System:** The NB BPS is determined according to the FERC approved definition of the bulk electric system, as it appears in the "NERC Glossary of Terms Used in Reliability Standards". NBPC is required to file updates to the BPS and may submit requests for BPS exceptions to the NBEUB for approval.

3. **Entity Registration:** The NBEUB maintains a NB Compliance Registry identifying those owners, users and operators of the BPS who must comply with approved reliability standards. The NB registry is based on the NERC functional model and registry criteria. NBPC is required to make recommendations to the NBEUB to maintain the compliance registry.

4. **NPCC Recommendations for Entity Registrations:** NPCC provides recommendations to the NBEUB for entity registrations under the provisions of a service agreement the NBEUB has executed with NPCC.

5. **Compliance Monitoring:** The NBEUB implements a compliance monitoring system for reliability standards that is based on the requirements of the NERC compliance program. The NB program is documented as the New Brunswick Compliance Monitoring and Enforcement Program (NB CMEP) – Schedule A to the Reliability Standards Regulation. As a recognized compliance body under the

regulations, NPCC assists the NBEUB with compliance monitoring activities according to a service agreement the NBEUB has executed with NPCC.

6. **Investigations:** The NBEUB is responsible for compliance investigations in New Brunswick. NPCC assists the NBEUB with compliance investigations in NB according to a service agreement the NBEUB has executed with NPCC. The NBEUB may also request NERC to assist with compliance investigations.

7. **Violation Determination and Sanction Imposition:** The NBEUB is responsible for the determination of violations, enforcement action and imposition of fines and penalties. Under a service agreement the NBEUB has executed with NPCC, NPCC makes recommendations on enforcement matters to the NBEUB including recommendations on dismissals, find fix track actions, mitigation plans, settlement agreements and penalties and sanctions. The NBEUB may request that NPCC include a NERC review and comments on NPCC enforcement recommendations to the NBEUB.

8. **Appeals to NBEUB:** A person may appeal to the NBEUB a decision from a review or compliance hearing relating to contested violations, mitigation plans and penalties and sanctions.

9. **NB "rules of procedure":** NB does not adopt a separate rules of procedure document, compliance program requirements (including the NB CMEP), are incorporated into provincial regulations that require LGIC approval to modify.

10. **NB Annual Implementation Plan:** The NB AIP is based on the NERC and NPCC implementation plans and may include NB specific requirements. Under a service agreement the NBEUB has executed with NPCC, NPCC makes recommendations to the NBEUB for a NB AIP.

Nova Scotia-US Comparator:
Standard-Making and Enforcement Functions

Fast Facts about Nova Scotia's Electricity System

Total annual consumption: 10.5 Terawatt-hours TWh (2013)
Customers: approx. 0.5 million
Total Installed capacity: 2,756 MW (as of January 2014)
Record summer peak: 1373 MW (2013-08-28)
Record winter peak: 2122 MW (2014-01-02)
Total length of transmission system: 5,900 km (3,700 miles)
Interconnections: New Brunswick

Key Organizations in Nova Scotia's Electricity Sector

Department of Economic and Rural Development and Tourism

The Minister for this Department is responsible for the Nova Scotia Utility and Review Board (UARB) Act which is the legislation that establishes the governance, structure and mandate of the UARB.

Department of Energy

The Nova Scotia Department of Energy ("Department") is responsible for setting the policy and legislative framework for Nova Scotia's electricity system. The Department develops solutions and advises on all aspects of energy policy for Nova Scotia, including electricity, natural gas and oil.

Nova Scotia Utility and Review Board

The Nova Scotia Utility and Review Board ("NSUARB" or "Board") is an independent, quasi- judicial body which has both regulatory and adjudicative jurisdiction flowing from the Utility and Review Board Act. It reports to the Legislature through the Minister of Economic and Rural Development and Tourism. Pursuant to the Public Utilities Act, the Board exercises general supervision over all electric utilities operating as public utilities within the Province. This jurisdiction includes setting rates, tolls and charges; regulations for provision of service; approval of capital expenditures in excess of $250,000 and any other matter the Board feels is necessary to properly exercise its mandate. The Board has the authority to stay or revoke the operation of a reliability standard in Nova Scotia and refer it back to NERC or the NPCC for further consideration.

Nova Scotia Power

Nova Scotia Power Incorporated (NSPI) is a vertically integrated, privately owned utility serving 95% of customers in Nova Scotia. NSPI owns the majority of transmission and distribution assets in the province as well as a significant portion of the generation. NSPI is a Regulated- Utility under the Public Utilities and subject to supervision by the NSUARB. NSPI is responsible for planning for and maintaining a reliable electricity service to all loads in the province. NSPI is responsible for reviewing and implementing NERC standards under the supervision of the NSUARB.

Nova Scotia Power System Operator

The system operator is financially part of Nova Scotia Power, but operationally and functionally separated from other parts of NSPI and must adhere to a UARB approved Standard of Conduct to ensure its independence from NSPI's other business units.. The system operator bears responsibility for, and

manages the wholesale electricity market and oversees the reliable daily operation of the provincial electricity grid.

Table Definitions

Provincial Organization: Nova Scotia's organization accountable and responsible for performing the function according to provincial legislation.

US Organization: the US organization responsible for performing the function according to an executed agreement for the provision of services.

US Comparator: the US organization responsible for performing the functions in the US according to US law.

Functions[1]		**Provincial Organization**	**Relevant US Organization**	**US Comparator**
Standards Making[2]	Standards Development	Not Applicable	NERC	NERC
	Standards Approval	NSUARB, NSPI (1)	Not Applicable	FERC
	Entity Registration	NSPI-SO (2,3)	NPCC Recommendations to NSPI-SO (4)	NERC
Compliance Monitoring	Compliance Monitoring and Violation Detection	NSUARB	NERC and NPCC (5)	NERC / NPCC and FERC
Enforcement Processes	Execution of Investigations	NSUARB	NERC and NPCC (6)	NERC/ NPCC and FERC
	Violation Determination and Sanction Imposition	NSUARB	Recommendations to NSUARB only (7)	NERC, FERC
Violation Prevention and Outreach	Violation Prevention, Outreach, including education	N/A (10)	NERC/ NPCC	NERC / NPCC and FERC
Appeals	First Right of Appeal	NSUARB Review or Hearing	Not Applicable	NPCC Hearing Body
	Second Right of Appeal	NSUARB Appeal (8)	Not Applicable	NERC BOT CC
	Third Right of Appeal	An order of the NSUARB can be appealed to The Nova Scotia Court of Appeal.	Not Applicable	FERC
Oversight	Approval of Nova Scotia's Compliance Monitoring and Enforcement Implementation Plan	NSUARB	NERC (9)	NERC/NPCC
	Performance Oversight of CMEP	NSUARB	Not Applicable	NERC BOT CC

[1] This table is intended to illustrate *who has authority over these various processes* vs. *who has authority for their execution.*
[2] Reliability standards include FERC approved NERC reliability standards and FERC approved regional reliability standards.

Notes:

1. **Standards Approval:** NERC submits standards to NSUARB and NSPI for approval, each organization may approve, modify, remand or dismiss the standard as not applicable, though final approval authority rests with the NSUARB. The NSUARB has a quarterly review process allowing the submission, by NERC, of standards already approved by FERC.

2. **Bulk Electric System:** The FERC approved definition of the bulk electric system, as modified on May 6th, 2014, has not yet been adopted in Nova Scotia.

3. **Entity Registration:** NPCC as the regional Entity maintains the list of all market participants of the BES who must comply with approved reliability standards. The registry is based on the NERC functional model and registry criteria.

4. **NPCC Recommendations for Entity Registrations:** NPCC provides recommendations and may also identify organizations that may be candidates for registration and assign them to the Compliance Registry.

5. **Compliance Monitoring:** As per MOU with NERC, compliance is mandatory in Nova Scotia. The NSUARB will monitor compliance and accept compliance information and recommendations from NERC.

6. **Investigations:** The NSUARB is responsible for compliance investigations in Nova Scotia. NERC may assist the NSUARB with compliance investigations by providing: Compliance reports and spot checks, Readiness evaluations, disturbance reports, etc.

7. **Violation Determination and Sanction Imposition:** NERC, NPCC and NSUARB may all suggest compliance violation; proceedings shall be conducted under the Board's direction and control. NERC may recommend a particular penalty for any violation, but the NSUARB will be responsible for determining if a violation occurred and what penalties should be imposed.

8. **Appeals to NSUARB:** Any person may appeal to the NSUARB a decision from a review or compliance hearing. Further appeals may proceed to a court of law.

9. **Compliance Monitoring and Enforcement Plan:** Approval for the compliance and monitoring plan is by MOU between NERC and NSUARB on 22nd of Dec, 2006 and later through MOU between NERC, NPCC and NSPI on 20th April 2010. NSPI is subject to NERC's CMEP as implemented by NPCC.

10. **Violation Prevention:** Compliance is mandatory in Nova Scotia.

Ontario-US Comparator:
Standard-Making and Enforcement Functions

Fast Facts about Ontario's Electricity System

Total annual consumption: 140.7 Terawatt-hours TWh (2013)
Customers: approx. 4.9 million
Installed capacity: 34,946 MW (as of December 2013)
Record summer peak: 27,005 MW (August 1, 2006)
Record winter peak: 24,979 MW (December 20, 2004)
Total length of transmission system: 30,000 km (18,600 miles)
Interconnections: Quebec, Manitoba, New York, Michigan, Minnesota

Reliability Standards Currently in Effect in Ontario

http://www.ieso.ca/Pages/Participate/Reliability-Requirements/Reliability-Standards-Compliance.aspx

From the above linked IESO web page, download excel file named, "Milestones in Reliability Standard Development and Lifecycle".

Key Organizations in Ontario's Electricity Sector

Ministry of Energy

The Ontario Ministry of Energy ("Ministry") is responsible for setting the policy and legislative framework for Ontario's electricity system. The Ministry develops solutions and advises on all aspects of energy policy for Ontario, including electricity, natural gas and oil. It also has legislative responsibility for the Ontario Energy Board ("OEB") and Independent Electricity System Operator ("IESO").

Ontario Energy Board

The Ontario Energy Board ("OEB") is an independent, quasi-judicial tribunal that regulates the province's electricity and natural gas sectors in the public interest. Its mandate is prescribed in legislation – primarily the *Ontario Energy Board Act, 1998* and the *Electricity Act, 1998* (the "Act") – and associated regulations. Part of the OEB's mandate is to protect the interests of consumers with respect to prices and the reliability and quality of electricity service. The OEB is the Governmental Authority for Ontario as defined by NERC. The OEB also has the legislative authority to stay or revoke the operation of a reliability standard in Ontario and refer it back to NERC or the NPCC for further consideration.

Independent Electricity System Operator and the Market Assessment and Compliance Division

The Independent Electricity System Operator ("IESO") is a not-for-profit corporate entity established under the Act that manages the wholesale electricity market and oversees the reliable operation of the provincial electricity grid. The IESO evaluates Ontario's current and short-term electricity needs as well as the adequacy and reliability of the integrated power system. The IESO is also responsible for

establishing and enforcing reliability standards and participating in developing standards made by standards authorities[1]. The IESO is subject to the OEB's oversight authority.
The Act also authorizes the IESO to make and enforce rules ("Market Rules") that govern the operation of Ontario's electricity system. The IESO's compliance and enforcement activities have been delegated to an independent business unit called the Market Assessment and Compliance Division ("MACD") through a letter of delegation from the IESO's President and CEO to MACD's Director. As such, MACD makes all determinations and exercises all authorities accorded the IESO in the Market Rules concerning monitoring, investigation and the enforcement of rules and standards concerning the wholesale electricity system and market. MACD establishes and executes processes, procedures and programs for monitoring, investigating and imposing sanctions (including financial penalties) against Ontario market participants and the IESO.

Table Definitions

This table is intended to illustrate who has authority over these various processes vs. who has the authority for their execution.

Provincial Organization: the Ontario organization accountable and responsible for performing the function according to provincial legislation, or through delegation, for matters concerning Ontario entities.

Relevant US Organization: the US organization responsible for performing the function according to an executed Memorandum of Understanding for matters concerning Ontario entities.

US Comparator: the US organization responsible for performing the functions according to US law.

[1] "Standards authority," as defined by the Act, means the North American Electric Reliability Corporation (NERC) and "any other agency or body designated by regulation that approves standards or criteria applicable both in and outside Ontario relating to the reliability of transmission systems." Ontario Regulation 214/08 has designated the Northeast Power Coordinating Council (NPCC) a standards authority in Ontario.

Functions		Provincial Organization	Relevant US Organization	US Comparator
Standards Making[2]	Standards Development	Not Applicable (14)	NERC	NERC, NPCC
	Standards Approval	OEB (1)	Not Applicable	FERC
	Entity Registration	IESO (2)	Not Applicable	NERC, NPCC
Compliance Monitoring	Compliance Monitoring and Violation Detection	MACD (6)	NPCC (7)	NERC, NPCC, FERC
Enforcement Processes	Execution of Investigations	MACD (8)	NERC and NPCC (8)	NERC, NPCC, FERC
	Violation Determination and Sanction Imposition	MACD (9, 11)	NERC and NPCC (10)	NERC, NPCC, FERC
Appeals	First Hearing	Dispute Resolution Panel (13)	NPCC (12)	NPCC Hearing Body
	Right of Appeal	OEB (13)	NERC (12)	NERC Board of Trustees Compliance Committee
	Further Right of Appeal	An order of the OEB can be appealed to Divisional Court on a matter of law or jurisdiction (OEB Act s. 33)	Not applicable (12)	FERC

[2] Reliability standards include FERC-approved NERC reliability standards and FERC-approved regional reliability standards.

Oversight	Approval of Ontario's Rules of Procedure	IESO Board and right of appeal to OEB	Not applicable	FERC
	Approval of Ontario's Compliance Monitoring and Enforcement Implementation Plan (CMEP)	MACD	Not applicable	NERC and NPCC
	Performance Oversight of CMEP	MACD (4)	NERC and NPCC (4)	NERC Board of Trustees Compliance Committee
	Violation Prevention and Outreach (including education)	MACD (5)	NERC and NPCC (5)	NERC, NPCC, FERC

Notes:

1. **Standards Approval:** Generally, unless a NERC reliability standard is otherwise stayed or remanded (by the OEB) back to NERC, the standard will become effective in Ontario when it is declared in force in the United States, unless the standard has been made in response to a regulatory directive that has not been approved by the NERC ballot body.

2. **Entity Registration:** Ontario market participants are subject to compliance with reliability-related market rules which include reliability standards. The IESO has applied a risk-based approach to the applicability criteria it uses to determine which Ontario market participant facilities are subject to reliability standards. These criteria are similar to NERC's Compliance registry criteria and make Purchase Selling Entity standard requirements not applicable in Ontario.

3. **Compliance Accountability:** The IESO is the sole Ontario entity accountable to NERC or NPCC for compliance with NERC reliability standards. This accountability includes violations by Ontario entities of any of these requirements. By extension of licence conditions, the OEB could also find licenced entities non-compliant and invoke penalties including revocation of licence and financial penalties for contravening enforceable provisions. The Board is not accountable to NERC or NPCC.

4. **Peer Review:** MACD, NERC and NPCC can initiate a peer review of each other's compliance program with a mutually-agreed-upon scope of review.

5. **Prevention and Outreach:** Each of NERC, NPCC and MACD can issue alerts and other publications to help Ontario market participants and the IESO prevent violations. In the past, MACD has done so through Interpretation Bulletins and Enforcement Statements. The Reliability Compliance Section (RCS) of the IESO conducts outreach to Ontario entities regarding the requirements of Ontario's Reliability Compliance Program and standards development engagement.

6. **MACD Monitoring:** MACD establishes procedures for monitoring Ontario market participants through the Ontario Reliability Compliance Program (ORCP) and MACD's audit and spot check program. The ORCP is equivalent to the NERC-NPCC CMEP implementation plan for self-certifications and reporting requirements. The RCS conducts these activities on behalf of MACD. MACD conducts additional monitoring of all Ontario market participants through direct access to SCADA systems and other operational information available to the IESO and through referrals from IESO personnel. MACD conducts additional monitoring of the IESO through direct access to SCADA systems and other operational information.

7. **NERC and NPCC Monitoring:** NPCC conducts audits, spot checks and self-certification of the IESO in accordance with the NERC-NPCC Monitoring Program.

8. **Investigations:** In collaboration and coordination with MACD investigations, NPCC and NERC have the right to draw their own conclusions with respect to compliance investigations of Ontario entities. MACD also investigates and makes its own independent conclusions for violation determinations and sanctions for all Ontario entities, including the IESO.

9. **MACD Violation Determination and Sanction Imposition:** MACD makes violation and sanction determinations for all Ontario entities and the IESO. Sanctions include, among other things, orders to: 1) do "such things as may be necessary" to comply with the Market Rules; 2) cease the act, activity or practice constituting the violation; 3) impose record-keeping or reporting requirements on a market participant; 4) issue a non-compliance letter and 5) impose financial penalties. The maximum financial penalty amount is $1,000,000 per occurrence for each breach at issue.

10. **NERC and NPCC Violation Determination and Sanction Imposition:** After determining that a violation has occurred in Ontario, NERC and NPCC may only impose sanctions on the IESO. These sanctions could be in respect of either a violation by an Ontario market participant or by the IESO itself. The possible sanctions imposed may include additional reporting, development of a mitigation plan, additional auditing, and in the case of material threats to reliability, remedial action directives.

11. **Public Disclosure:** When MACD makes a determination of a reliability standard violation or reliability-related market rule violation, the name of the responsible entity is made public on the IESO website. The level of detail disclosed for any violation varies according to what MACD deems necessary. NERC or NPCC do not disclose violations by Canadian entities. MACD sanctions are posted at: http://www.ieso.ca/Pages/Participate/Market-Oversight/Sanctions.aspx

12. **Appeals of NERC and NPCC Determinations:** The IESO is the sole Ontario entity accountable to NERC or NPCC for compliance by market participants and the IESO with NERC standards. If the IESO faces a violation determination or sanction by NERC or NPCC, it has a right to a compliance hearing with NPCC and a subsequent appeal to NERC. The IESO can also appeal any final NERC or NPCC order to the OEB.

13. **Appeals of MACD Determinations:** An enforcement decision made by MACD can be contested through the IESO's Dispute Resolution Panel (DRP) process, which is composed of negotiation, mediation and arbitration stages. The award of a DRP arbitrator can then be appealed to the OEB if it includes a financial penalty above $10,000 or otherwise denies authorization for, or terminates, suspends or restricts, the relevant market participant's right to participate in the Ontario market.

14. The IESO has the authority under s. 32(1) (c) of the *Electricity Act, 1998 to* establish standards and criteria relating to the reliability of electricity service or the IESO-controlled grid, if necessary.

Québec - US Comparator:
Standard-Making and Enforcement Functions

Fast Facts about Québec's Electricity System

Total annual consumption: 168 Terawatt-hours TWh (2012)
Customers: approx. 4,1 million
Installed capacity: 35 829 MW (as of May 2013)
Record summer peak: 22 092 MW (July 2010)
Record winter peak: 39 031MW (January 22, 2014)
Total length of transmission system: 33 640 km (20 900 miles)
Interconnections: Ontario, New Brunswick, Newfoundland & Labrador, New York, New England (Vermont, Massachusetts)

Reliability Standards Currently in Effect

A list of Québec's reliability standards and their status is available at this link:
http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html

Key Organizations in Québec's Electricity Sector

Ministère des Ressources naturelles

The ministère de l'Énergie et des Ressources naturelles (the "Ministry") is responsible for, among other things, setting the policy and legislative framework for Québec's electricity system. The Ministry develops solutions and advises on all aspects of energy policy for Québec, including electricity, natural gas and oil.

Régie de l'énergie

The Régie de l'énergie (the "Régie") is an independent, economic regulation agency that regulates the province's electricity and natural gas sectors in the public interest. Pursuant to its governing legislation, the *Act respecting the Régie de l'énergie* (the "Act"), it has the authority to establish, monitor and enforce a mandatory regime of reliability standards for electricity transmission in Québec. The mandatory reliability regime is not yet in place, and the framework for the regime is still in development. Once the mandatory regime is in place, the Régie will be responsible for ensuring that electric power transmission in Québec is carried out according to the reliability standards it adopts. The Régie may request the Reliability Coordinator (the "RC") for Québec to modify a standard filed or submit a new one, on the conditions it sets. The Régie adopts reliability standards and sets the dates of their coming into force.

The Régie will make all determinations and exercises all authorities concerning monitoring, investigation and enforcement of reliability standards, including the imposition of sanctions and financial penalties, but will obtain recommendations from NPCC and sometimes NERC, both of whom it has recognized, through an agreement, as experts in the development and monitoring of electric power transmission reliability standards. A second agreement, signed in September 2014, details the mandate granted by the Régie to NPCC and NERC with respect to monitoring and assessing the compliance of registered entities in Québec with the reliability standards adopted by the Régie.

Direction Contrôle des mouvements d'énergie (System Control unit) of Hydro-Québec TransÉnergie ("HQCMÉ")

HQCMÉ was designated by the Régie, pursuant to the Act, as the RC for Québec. Under that function, it oversees the reliable operation of the provincial electricity grid. It files with the Régie reliability standards, either NERC or NPCC standards, as well as any variant or other standard it deems necessary. It also files a register identifying the entities that are subject to the reliability standards adopted by the Régie.

Functions[1]		Provincial Organization	Relevant US Organization	US Comparator
Standards Making[2]	Standards Development	HQCMÉ (RC) (rarely)	NERC	NERC
	Standards Adoption	The Régie (1)	Not Applicable	FERC
Entity Registration		The Régie / RC(2)	Not Applicable	NERC
Compliance Monitoring	Compliance Monitoring and Violation Detection	The Régie (3, 4)	NPCC (5)	NERC, NPCC, FERC
	Execution of Investigations	The Régie (6)	NPCC or NERC (6)	NERC, NPCC, FERC
Enforcement Processes	Violation Determination and Sanction Imposition	The Régie (7, 8, 9)	Not Applicable	NERC, FERC
Appeals	Revision of a decision	The Régie (10)	Not applicable	NPCC Hearing Body
	Further Right of Appeal	Québec Superior Court (11)	Not applicable	NERC Board of Trustees Compliance Committee (BOT CC)
	Further Right of Appeal	Court of Appeal of Québec (12)	Not applicable	FERC
Oversight	Approval of Québec's Rules of Procedure	The Régie (13)	Not applicable	FERC
	Approval of Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) and of the Implementation Plan	The Régie (14)	Not applicable	NERC, NPCC
	Performance Oversight of QCMEP	The Régie (15)	NERC and NPCC (15)	NERC BOT CC
	Violation Prevention and Outreach (including education)	The Régie (16)	NERC and NPCC (16)	NERC, NPCC, FERC

[1] This table is intended to illustrate who has authority over these various processes vs. who has authority for their execution.

[2] Reliability standards include FERC approved NERC reliability standards and FERC approved regional reliability standards and locally developed reliability standards proposed by the RC.

Table Definitions:

Provincial Organization: the Québec organization accountable and responsible for performing the function according to provincial legislation or through designation for matters concerning Québec registered entities.

Relevant US Organization: the US organization that is responsible for performing the function according to an agreement for matters concerning Québec registered entities.

US Comparator: the US organization that is responsible for performing the functions according to US law.

Notes:

1. **Standards Adoption:**
   Authority – Pursuant to section 85.7 of the Act, the Régie adopts the reliability standards and sets the dates of their coming into force.
   NERC Standards Filing – For information purposes, NERC files Board approved standards in Québec. Generally, when a NERC reliability standard is approved by FERC, the standard will be filed by the RC (HQCMÉ) with the Régie for adoption. The RC can as well file any variant of these standards or other standards it considers necessary.
   Standards Review – The Régie holds public hearing on the standards before their adoption. NERC/NPCC can make observations/recommendations to the Régie pursuant to their signed agreement.
   Public Process – The RC posts the standards on their website for public comments from the registered entities before filing them to the Régie for their adoption.
   Adoption/Remand – The Régie may request that the RC modifies a filed reliability standard or submit a new one, on the conditions it sets. Thus a reliability standard that has been filed with the Régie by the RC will not be remanded to NERC.

2. **Entity Registration:** Section 85.3 of the Act lists the entity characteristics to which the reliability standards applies. Pursuant to the Act (Section 85.13) the RC must file with the Régie, for approval, a register identifying the entities that are subject to the reliability standards adopted by the Régie.

3. **Compliance Accountability:** All Québec registered entities are accountable to the Régie for compliance with the reliability standards it adopts.

4. **Monitoring:** The Régie establishes processes for monitoring Québec registered entities through the *Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP)*. The QCMEP is analogous to the NERC CMEP.

5. **Monitoring:** NPCC monitors compliance to the reliability standards by conducting audits, self-certification, spot checks and other means in accordance with the QCMEP.

6. **Investigations:** The Régie may request or authorize NPCC or NERC to lead a compliance investigation.

7. **Violation Determination and Sanction Imposition:** The Régie makes violation and sanction determinations for all Québec registered entities after reviewing NPCC's findings and recommendations. Sanctions will be fixed according to the *Sanction Guide for the Enforcement of the Reliability Standards in effect in Québec*. The Régie may impose financial penalties or sanctions. The maximum financial penalty amount is $500 000 per occurrence per day.

8. **Enforcement Measure:** The Régie may impose a mitigation plan, a remedial action for non-compliance seriously compromising the reliability of electric power transmission, or conditions for carrying on certain activities.

9. **Public Disclosure:** In the event that a reliability standard violation is determined by the Régie, the name of the responsible entity is made public on the Régie's website. The level of detail disclosed for any violation varies according to what is deemed necessary by the Régie.

10. **Revision of a Decision:** Section 37 of the Act provides the conditions for a revision or revocation of a determination by the Régie.

11. **Further Right of Appeal:** Section 40 of the Act provides that "no appeal lies from a decision of the Régie." The only available recourse is a judicial review to the Superior Court of Québec. However, section 41 of the Act provides for a relatively tight privy clause.

12. **Further Right of Appeal:** A Superior Court decision on judicial review can be appealed to the Quebec Court of Appeal and ultimately, by permission, to the Supreme Court of Canada.

13. **Québec's Rules of Procedure:** Québec's Rules of procedure are integrated into the second agreement and the QCMEP.

14. **QCMEP and Implementation Plan:** Each year, the Régie approves the Implementation Plan to be used by NPCC to monitor and assess Registered Entities' compliance with the reliability standards. The Implementation Plan includes, among other things, the Annual Audit Plan and the Self-Certification program with their schedules.

15. **Performance Oversight:** NPCC provides the Régie and NERC with the *QCMEP Annual Implementation Report* regarding, among other things, the effectiveness of the QCMEP. Upon request from the Régie, NERC will conduct an audit of NPCC.

16. **Prevention and Outreach:** In addition to alerts and other publications issued by NERC and/or NPCC to help Québec registered entities prevent violations, the Régie may also issue similar notices for this purpose in an effort to clarify Québec's mandatory reliability standards regime, the requirements of the QCMEP and reliability standards development.

Saskatchewan - US Comparator: Standard-Making and Enforcement Functions

Table Definitions:

Provincial Organization: the Saskatchewan organization accountable and responsible for performing the function according to provincial legislation or through delegation for matters concerning Saskatchewan entities.

US Organization: the US organization that is responsible for performing the function according to an executed Memorandum of Understanding for matters concerning Saskatchewan entities.

US Comparator: the US organization that is responsible for performing the functions according to US law.

Functions		Provincial Organization	Relevant US Organization	US Comparator
Standards Making[1]	Standards Approval	SPC (1)	Not applicable	FERC
	Standards Development	Not applicable	NERC	NERC, MRO
	Entity Registration	Not applicable	NERC (2)	NERC
Compliance Monitoring	Compliance Monitoring and Violation Detection	SPC (3)	NERC and MRO (3)	NERC, MRO, FERC
Enforcement Processes	Execution of Investigations	SPC (3)	NERC and MRO (3)	NERC, MRO
	Violation Determination and Sanction Imposition	SPC (3)	NERC and MRO (3)	FERC
Violation Prevention and Outreach	Violation Prevention, Outreach, including education	Not Applicable	NERC and MRO (4)	NERC, MRO
Appeals	First Right of Appeal	SPC (5)	Not applicable	MRO Hearing Body
	Second Right of Appeal	SPC (5)	Not applicable	NERC Board of Trustees Compliance Committee (BOT CC)
	Third Right of Appeal	SPC (5)	Not applicable	FERC
Oversight	Approval of Saskatchewan's Rules of Procedure	Not Applicable	Not applicable	FERC
	Approval of Saskatchewan's Compliance Monitoring and Enforcement Implementation Plan	Not Applicable	Not applicable	NERC, MRO
	Performance Oversight of CMEP	Not Applicable	NERC and MRO (6)	NERC BOT CC
	Violation Prevention and Outreach	Not Applicable	NERC and MRO (4)	NERC, MRO, FERC

[1] Reliability standards Include FERC approved NERC reliability standards and FERC approved regional reliability standards.

Notes:

1. **Standards Approval:** SaskPower has the legislative authority via *The Power Corporation Act* (Saskatchewan) to set standards and enforce compliance for the bulk electric system in the Province of Saskatchewan. Typically NERC Board of Trustees approved standards shall be viewed as being automatically adopted in Saskatchewan, unless the standard is otherwise ordered, stayed or remanded back to NERC within 120 days of receiving notice.

2. **Entity Registration:** SaskPower is currently registered in the NERC Compliance Registry.

3. **Compliance Monitoring/Enforcement Processes:** The oversight unit within SaskPower will be the monitoring, compliance and enforcement authority for the province, as per SaskPower's legislative authority. The Midwest Reliability Organization currently performs on-site compliance audits for SaskPower.

4. **Prevention and Outreach:** SaskPower receives alerts and other publications issued by NERC and/or MRO that address violation prevention.

5. **Appeals:** If SaskPower disputes an MRO finding of non-compliance regarding a reliability standard, the SaskPower Oversight Unit may choose to hear arguments.

6. **Peer Review:** NERC and MRO can initiate a peer review of each other's compliance program with a mutually agreed scope of review.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, please email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Application of certain GO/GOP Reliability Standards and Requirements to Dispersed Generation		
Date Submitted:	10/1/2013		
SAR Requester Information			
Name:	Jennifer Sterling-Exelon, Gary Kruempel-MidAmerican, Allen Schriver-NextEra Energy, Inc., Brian Evans-Mongeon-Utility Services Inc.		
Organization:	Exelon, MidAmerican, NextEra Energy, Utility Services Inc.		
Telephone:	(630) 437-2764 – primary contact	E-mail:	jennifer.sterling@exeloncorp.com primary contact
SAR Type (Check as many as applicable)			
☐ New Standard ☒ Revision to existing Standard		☐ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
The industry is requesting that the application section of certain GO/GOP Reliability Standards or the requirements of certain GO/GOP Reliability Standards be revised in order to ensure that the Reliability Standards are not imposing requirements on dispersed generation that are unnecessary and/or counterproductive to the reliable operation of the Bulk Electric System (BES). For purposes of this SAR, dispersed generation are those resources that aggregate to a total capacity greater than 75 MVA (gross

SAR Information
nameplate rating), and that are connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage of 100 kV or above. This request is related to the proposed new definition of the Bulk Electric System (BES) from Project 2010-17, that results in the identification of elements of new dispersed generation facilities that if included under certain Reliability Standards may result in a detriment to reliability or be technically unsound and not useful to the support of the reliable operation of the BES .
Purpose or Goal (How does this request propose to address the problem described above?):
The goal of the request is to revise the applicability of GO/GOP Reliability Standards or the Requirement(s) of GO/GOP Reliability Standards to recognize the unique technical and reliability aspects of dispersed generation, given the proposed new definition of the BES.
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objective of the revisions to the applicability section and/or Requirements of certain GO/GOP Reliability Standards is to ensure that these revisions are approved by the Board of Trustees and applicable regulatory agencies prior to the effective date for newly identified elements under the proposed BES definition (i.e., June 2016).
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The scope of this SAR involves revisions to the applicability section of the following GO/GOP Reliability Standard applicability sections and/or Reliability Standard Requirements: (a) PRC-005-2 (-3); (b) FAC-008-3; (c) PRC-023-3/PRC-025-1; (d) PRC-004-2a (-3) ; and (e) VAR-002-2 so it is clear what, if any, requirements should apply to dispersed generation. Also, IRO,MOD, PRC or TOP Standards that require outage and protection and control coordination, planning, next day study or real time data or reporting of changes in real and reactive capability should be examined and revised, as needed, to ensure it is clear that these activities and reporting are conducted at the point of aggregation to 75 MVA, and not at an individual turbine, inverter or unit level for dispersed generation. This scope would also include development of a technical guidance paper for standard drafting teams developing new or revised Standards, so that they do not incorrectly apply requirements to dispersed generation unless such an application is technically sound and promotes the reliable operation of the BES. To the extent, there are existing Reliability Standard Drafting Teams that have the expertise and can make the requested changes prior to the compliance date of newly identified assets under the BES definition (i.e., June 2016), those projects may be assigned the required changes as opposed to creating new projects.

SAR Information
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

The following description and technical justification(including an assessment of reliability impacts) is provided for the standard drafting teams to execute the SAR for each applicable Standard.

PRC-005-2

Testing and maintenance of protection and control equipment for dispersed generation should start at the point of aggregation to 75 MVA. Manufacturers of dispersed generation turbines and solar panels recommend against specific testing and maintenance regimes for protection and control equipment at the dispersed generation turbine and panel level. In fact it is counterproductive to implement protection and control at the individual turbine, solar panel, or unit level. Instead this is best done at an aggregated level. Therefore, PRC-005 should indicate that the standard applies at the point of aggregation to at 75 MVA or greater for dispersed generation. This change would clarify that the facility section 4.2.5.3 is the section that would apply to dispersed generating facilities and that the remaining sections would not apply.

FAC-008-3

For dispersed generation, it is unclear if in FAC-008-3 the term “main step up transformer” refers to the padmount transformer at the base of the windmill tower or to the main aggregating transformer that steps up voltage to transmission system voltage. From a technical standpoint, it should be the point of aggregation at 75 MVA or above that is subject to this standard for dispersed generation, such as wind. It is at the point of aggregation at 75 MVA or above that facilities ratings should start, since it is this injection point at which a planner or operator of the system is relying on the amount of megawatts the dispersed generation is providing with consideration of the most limiting element. To require facility ratings at for each dispersed turbine, panel or generating unit is not useful to a planner or operator of the system, and, therefore, FAC-008-3 should be revised to be clear that facility ratings start at the point of aggregation at 75 MVA or above for dispersed generation.

SAR Information

Also consider that the BES definition specifically excludes collector system equipment at less than 75 MVA from being included in the BES. Thus, those portions of the collector systems that handle less than 75 MVA are not BES "Facilities," and, therefore, need not be evaluated per R1 or R2. Given this, there seems to be no technical value to conduct facility ratings for individual dispersed generation turbines, generating units and panels.

PRC-023-3/PRC-025-1

In keeping with the registration criteria for Generator Owners as well as the proposed BES Definition, the 75MVA point of aggregation should be the starting point for application of relay loadability requirements.

PRC-004-2

There is no technical basis to claim that misoperation analysis, corrective action plan implementation and reporting for dispersed generation at the turbine, generating unit or panel level is needed for the reliable operation of the BES. Similar to the statements above, the appropriate point to require misoperation analysis, corrective action plan implementation and reporting is at the point of aggregation at 75 MVA and above.

VAR-002-2

Voltage control for some types of dispersed generating facilities is accomplished by a controller that is able to adjust either generating unit controls or discrete reactive components to provide transmission system voltage adjustment. The VAR-002 standard should be modified to allow this type of control for dispersed generation facilities under the requirements of the standard.

General review of IROs, MODs, PRCs, TOPs

IRO, MOD, PRC or TOP Standards that require outage and protection and control coordination, planning, next day study or real time data or reporting of changes in real and reactive capability should be examined and revised, as needed, to ensure it is clear that these activities are conducted at the point of aggregation at 75 MVA, and not an individual turbine, generating unit or panel level for dispersed generation. Unless this clarity is provided applicability at a finer level of granularity related to dispersed generation may be seen as required and such granularity will result in activities that have no benefit to

SAR Information
reliable operation of the BES. Furthermore applicability at a finer level of granularity will result in uneeded and ineffective collection, analysis, and reporting activities that may result in a detriment to reliability.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Reliability Coordinator	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 of 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 >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one 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.

Reliability Functions		
☐	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 all that apply).		
☒	1. Interconnected bulk power 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 power 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 power 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 power 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 power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☐	7. The security of the interconnected bulk power 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?		Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.		Yes

Reliability and Market Interface Principles	
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability 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

Related Standards	
Standard No.	Explanation
PRC-005-2, FAC-008-3, PRC-023-3/PRC-025-1/PRC-004-2a, VAR-002-2b and various IRO, MOD, PRC and TOP Standards	See explanation under technical analysis.

Related SARs	
SAR ID	Explanation
	N/A

Related SARs	

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	

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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-001-1.1(X)[1] is proposed for approval to align the applicability of PRC-001-1.1a with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 – Standards Applicability for Dispersed Generation Resources standards drafting team (SDT) has coordinated with the other SDTs currently reviewing this standard and has recommended revisions to Requirement R3.1 to account for the unique characteristics of dispersed power producing resources.[2] Given the timing of concurrent standards development of PRC, TOP, and IRO projects, PRC-001-1.1a may be retired pursuant to an Implementation Plan of a successor version of PRC-001. If this occurs, PRC-001-1.1(X) will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The standard version number currently includes an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

[2] The terms "dispersed generation resources" and "dispersed power producing resources" are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. Title: System Protection Coordination

2. Number: PRC-001-1.1(X)

3. Purpose:

To ensure system protection is coordinated among operating entities.

4. Applicability

4.1. Balancing Authorities

4.2. Transmission Operators

4.3. Generator Operators

5. Effective Date:

See the Implementation Plan for this standard.

B. Requirements

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of Protection System schemes applied in its area.

R2. Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:

R2.1. If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.

R2.2. If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.

R3. A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.

R3.1. Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.

- Requirement R3.1 is not applicable to the individual generating units of dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

Rationale for the Applicability Exclusion in Requirement R3.1

Coordination of new or changes to protective systems associated with dispersed power producing resources identified through Inclusion I4 of the BES definition are typically performed on the interconnecting facilities. New or changes to protective systems associated with these facilities should be coordinated with the TOP as these protective systems typically must be closely coordinated with the transmission protective systems to ensure the overall protection systems operates as designed. While the protective systems implemented on the individual generating units of dispersed power producing resources at these dispersed power producing facilities (i.e. individual wind turbines or solar panels/inverters) may in some cases need to be coordinated with other protective systems within the same dispersed power producing facility, new or changes to these protective systems do not need to be coordinated with the transmission protective systems, as this coordination would not provide reliability benefits to the BES.

R3.2. Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.

R4. Each Transmission Operator shall coordinate Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.

R5. A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others:

R5.1. Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's Protection Systems.

R5.2. Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' Protection Systems.

R6. Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.

C. Measures

M1. Each Generator Operator and Transmission Operator shall have and provide upon request evidence that could include but is not limited to, revised fault analysis study, letters of agreement on settings, notifications of changes, or other equivalent evidence that will be used to confirm that there was coordination of new protective systems or changes as noted in Requirements 3, 3.1, and 3.2.

M2. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, documentation, electronic

logs, computer printouts, or computer demonstration or other equivalent evidence that will be used to confirm that it monitors the Special Protection Systems in its area. (Requirement 6 Part 1)

M3. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, operator logs, phone records, electronic-notifications or other equivalent evidence that will be used to confirm that it notified affected Transmission Operator and Balancing Authorities of changes in status of one of its Special Protection Systems. (Requirement 6 Part 2)

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 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 Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1.

Each Transmission Operator and Balancing Authority shall keep 90 days of historical data (evidence) for Measures 2 and 3.

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

None.

2. Levels of Non-Compliance for Generator Operators:

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: Failed to provide evidence of coordination when installing new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority as specified in R3.1.

3. Levels of Non-Compliance for Transmission Operators:

3.1. Level 1: Not applicable.

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable.

3.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

3.4.1 Failed to provide evidence of coordination when installing new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities as specified in R3.2.

3.4.2 Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

4. Levels of Non-Compliance for Balancing Authorities:

4.1. Level 1: Not applicable.

4.2. Level 2: Not applicable.

4.3. Level 3: Not applicable.

4.4. Level 4: Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

E. Regional Differences

None identified.

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	August 25, 2005	Fixed Standard number in Introduction from PRC-001-1 to PRC-001-0	Errata
1	November 1, 2006	Adopted by the NERC Board of Trustees	Revised
1.1	April 11, 2012	Errata adopted by the Standards Committee; (Capitalized "Protection System" in accordance with Implementation Plan for Project 2007-17 approval of revised definition of "Protection System")	Errata associated with Project 2007-17
1.1	September 9, 2013	Informational filing submitted to reflect the revised definition of Protection System in accordance with the Implementation Plan for the revised term.	
TBD (balloted as 1.1(X))	TBD	Standard revised in Project 2014-01	Applicability revised to clarify application of requirements to BES dispersed power producing resources

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Dispersed Generation Resources
PRC-001-1.1(X)

The standard version number currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

Standards Involved

Approval:

- PRC-001-1.1(X) – System Protection Coordination

Retirement:

- PRC-001-1.1a – System Protection Coordination

Prerequisite Approvals:

N/A

Background

In light of the adoption of a revised Bulk Electric System (BES) definition by the NERC Board of Trustees, changes to the applicability of certain Reliability Standards, including PRC-001, are necessary to align the standards with the implementation of the revised BES definition. The standard drafting team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Generation Resources has modified the applicability section and requirements of certain standards applicable to Generator Owners and Generator Operators to recognize the unique technical and reliability aspects of dispersed power producing resources in order to ensure the applicability of the standards is consistent with the reliable operation of the BES.[1]

General Considerations

PRC-001-1.1(X) is proposed for approval to align the applicability of PRC-001-1.1a with the revised definition of the BES. Specifically, the SDT has coordinated with the other SDTs currently reviewing this standard and has recommended revisions to Requirement R3.1 to account for the unique characteristics of dispersed power producing resources. Given the timing of concurrent standards development of PRC, TRP, and IRO projects, PRC-001-1.1a may be retired pursuant to an Implementation Plan of a successor version of PRC-001. If this occurs, PRC-001-1.1(X) will not go into effect.

Effective Date

PRC-001-1.1(X) shall become effective immediately after the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable

[1] The terms "dispersed generation resources" and "dispersed power producing resources" are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:

The existing standard, PRC-001-1.1a, shall be retired at midnight of the day immediately prior to the Effective Date of PRC-001-1.1(X).

Applicability:

This standard applies to the following functional entities:

- Transmission Operator
- Generator Operator
- Balancing Authority

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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-001-1.1(X)[1] is proposed for approval to align the applicability of PRC-001-1.1a with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 – Standards Applicability for Dispersed Generation Resources standards drafting team (SDT) has coordinated with the other SDTs currently reviewing this standard and has recommended revisions to Requirement R3.1 to account for the unique characteristics of dispersed power producing resources.[2] Given the timing of concurrent standards development of PRC, TOP, and IRO projects, PRC-001-1.1a may be retired pursuant to an Implementation Plan of a successor version of PRC-001. If this occurs, PRC-001-1.1(X) will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The standard version number currently includes an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

[2] The terms "dispersed generation resources" and "dispersed power producing resources" are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. **Title:** **System Protection Coordination**

2. **Number:** PRC-001-1.1(X)

3. **Purpose:**

   To ensure system protection is coordinated among operating entities.

4. **Applicability**

   4.1. Balancing Authorities

   4.2. Transmission Operators

   4.3. Generator Operators

5. **Effective Date:** ~~January 1, 2007~~

   See the Implementation Plan for this standard.

B. Requirements

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of Protection System schemes applied in its area.

R2. Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:

R2.1. If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.

R2.2. If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.

R3. A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.

R3.1. Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.

- Requirement R3.1 is not applicable to the individual generating units of dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

Rationale for the Applicability Exclusion in Requirement R3.1

Coordination of new or changes to protective systems associated with dispersed power producing resources identified through Inclusion I4 of the BES definition are typically performed on the interconnecting facilities. New or changes to protective systems associated with these facilities should be coordinated with the TOP as these protective systems typically must be closely coordinated with the transmission protective systems to ensure the overall protection systems operates as designed. While the protective systems implemented on the individual generating units of dispersed power producing resources at these dispersed power producing facilities (i.e. individual wind turbines or solar panels/inverters) may in some cases need to be coordinated with other protective systems within the same dispersed power producing facility, new or changes to these protective systems do not need to be coordinated with the transmission protective systems, as this coordination would not provide reliability benefits to the BES.

R3.2. Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.

R4. Each Transmission Operator shall coordinate Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.

R5. A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others:

R5.1. Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's Protection Systems.

R5.2. Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' Protection Systems.

R6. Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.

C. Measures

M1. Each Generator Operator and Transmission Operator shall have and provide upon request evidence that could include but is not limited to, revised fault analysis study, letters of agreement on settings, notifications of changes, or other equivalent evidence that will be used to confirm that there was coordination of new protective systems or changes as noted in Requirements 3, 3.1, and 3.2.

M2. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, documentation, electronic

logs, computer printouts, or computer demonstration or other equivalent evidence that will be used to confirm that it monitors the Special Protection Systems in its area. (Requirement 6 Part 1)

M3. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, operator logs, phone records, electronic-notifications or other equivalent evidence that will be used to confirm that it notified affected Transmission Operator and Balancing Authorities of changes in status of one of its Special Protection Systems. (Requirement 6 Part 2)

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 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 Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1.

Each Transmission Operator and Balancing Authority shall keep 90 days of historical data (evidence) for Measures 2 and 3.

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

None.

2. Levels of Non-Compliance for Generator Operators:

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: Failed to provide evidence of coordination when installing new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority as specified in R3.1.

3. Levels of Non-Compliance for Transmission Operators:

3.1. Level 1: Not applicable.

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable.

3.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

3.4.1 Failed to provide evidence of coordination when installing new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities as specified in R3.2.

3.4.2 Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

4. Levels of Non-Compliance for Balancing Authorities:

4.1. Level 1: Not applicable.

4.2. Level 2: Not applicable.

4.3. Level 3: Not applicable.

4.4. Level 4: Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

E. Regional Differences

None identified.

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	August 25, 2005	Fixed Standard number in Introduction from PRC-001-1 to PRC-001-0	Errata
1	November 1, 2006	Adopted by the NERC Board of Trustees	Revised
1.1	April 11, 2012	Errata adopted by the Standards Committee; (Capitalized "Protection System" in accordance with Implementation Plan for Project 2007-17 approval of revised definition of "Protection System")	Errata associated with Project 2007-17
1.1	September 9, 2013	Informational filing submitted to reflect the revised definition of Protection System in accordance with the Implementation Plan for the revised term.	
TBD (balloted as 1.1(X))	TBD	Standard revised in Project 2014-01	Applicability revised to clarify application of requirements to BES dispersed power producing resources

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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-019-2 is proposed for approval to align the applicability section of PRC-019-1 with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 – Standards Applicability for Dispersed Generation Resources standards drafting team has recommended revisions to the Facilities section to clarify that facilities that solely regulate voltage at the individual generating unit are subject to the requirements. Given the timing of concurrent standards development of PRC projects, PRC-019-1 may be retired pursuant to an Implementation Plan of a successor version of PRC-019. If this occurs, PRC-019-2 will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.[1]

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The terms “dispersed generation resources” and “dispersed power producing resources” are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. **Title:** Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

2. **Number:** PRC-019-2

3. **Purpose:** To verify coordination of generating unit Facility or synchronous condenser voltage regulating controls, limit functions, equipment capabilities and Protection System settings.

4. **Applicability:**

   4.1. Functional Entities

   4.1.1 Generator Owner

   4.1.2 Transmission Owner that owns synchronous condenser(s)

   4.2. Facilities

   For the purpose of this standard, the term, "applicable Facility" shall mean any one of the following:

   4.2.1 Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

   4.2.2 Individual synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

   4.2.3 Generating plant/ Facility consisting of one or more units that are connected to the Bulk Electric System at a common bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

   4.2.3.1 This includes individual dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition where voltage regulating control for the facility is performed solely at the individual resources.

Rationale for Facilities section 4.2.3.1

For those dispersed power producing facilities that only perform voltage regulating control at the individual unit level, the SDT believes that coordination should take place at the individual power producing resource level. These facilities need to consider the Protection Systems at the individual units and their compatibility with the reactive and voltage limitations of the units. Where voltage regulating control is done at an aggregate level, applicability is already included under Facilities section 4.2.3.

4.2.4 Any generator, regardless of size, that is a blackstart unit material to and designated as part of a Transmission Operator's restoration plan.

5. Effective Date:

See the Implementation Plan for this standard.

B. Requirements

R1. At a maximum of every five calendar years, each Generator Owner and Transmission Owner with applicable Facilities shall coordinate the voltage regulating system controls, (including in-service[2] limiters and protection functions) with the applicable equipment capabilities and settings of the applicable Protection System devices and functions. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Assuming the normal automatic voltage regulator control loop and steady-state system operating conditions, verify the following coordination items for each applicable Facility:

1.1.1. The in-service limiters are set to operate before the Protection System of the applicable Facility in order to avoid disconnecting the generator unnecessarily.

1.1.2. The applicable in-service Protection System devices are set to operate to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits.

R2. Within 90 calendar days following the identification or implementation of systems, equipment or setting changes that will affect the coordination described in Requirement R1, each Generator Owner and Transmission Owner with applicable Facilities shall perform the coordination as described in Requirement R1. These possible systems, equipment or settings changes include, but are not limited to the following *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*:

- Voltage regulating settings or equipment changes;
- Protection System settings or component changes;
- Generating or synchronous condenser equipment capability changes; or
- Generator or synchronous condenser step-up transformer changes.

C. Measures

M1. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence (such as examples provided in PRC-019 Section G) that it coordinated the voltage regulating system controls, including in-service[3] limiters and protection functions, with the applicable equipment capabilities and settings of the applicable

[2] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

[3] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

Protection System devices and functions as specified in Requirement R1. This evidence should include dated documentation that demonstrates the coordination was performed.

M2. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence of the coordination required by the events listed in Requirement R2. This evidence should include dated documentation that demonstrates the specified intervals in Requirement R2 have been met.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Evidence Retention

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

The Generator Owner and Transmission Owner shall retain evidence of compliance with Requirements R1 and R2, Measures M1 and M2 for six years.

If a Generator Owner or Transmission Owner is found non-compliant, the entity shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last periodic audit report 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

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years but less than or equal to 5 calendar years plus 4 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 4 months but less than or equal to 5 calendar years plus 8 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 8 months but less than or equal to 5 calendar years plus 12 months after the previous coordination.	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 5 calendar years plus 12 months after the previous coordination.
R2	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 90 calendar days but less than or equal to 100 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 100 calendar days but less than or equal to 110 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 110 calendar days but less than or equal to 120 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 120 calendar days following the identification or implementation of a change in equipment or settings that affected the coordination.

E. Regional Variances

None.

F. Associated Documents

"Underexcited Operation of Turbo Generators", AIEE Proceedings T Section 881, Volume 67, 1948, Appendix 1, C. G. Adams and J. B. McClure.

,"Protective Relaying For Power Generation Systems", Boca Raton, FL, Taylor & Francis, 2006, Reimert, Donald

"Coordination of Generator Protection with Generator Excitation Control and Generator Capability", a report of Working Group J5 of the IEEE PSRC Rotating Machinery Subcommittee

"IEEE C37.102-2006 IEEE Guide for AC Generator Protection"

"IEEE C50.13-2005 IEEE Standard for Cylindrical-Rotor 50 Hz and 60 Hz Synchronous Generators Rated 10 MVA and Above"

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees	New
1	March 20, 2014	FERC Order issued approving PRC-019-1. (Order becomes effective on 7/1/16.)	

G. Reference

Examples of Coordination

The evidence of coordination associated with Requirement R1 may be in the form of:

- P-Q Diagram (Example in Attachment 1), or
- R-X Diagram (Example in Attachment 2), or
- Inverse Time Diagram (Example in Attachment 3) or,
- Equivalent tables or other evidence

This evidence should include the equipment capabilities and the operating region for the limiters and protection functions

Equipment limits, types of limiters and protection functions which could be coordinated include (but are not limited to):

- Field over-excitation limiter and associated protection functions.
- Inverter over current limit and associated protection functions.
- Field under-excitation limiter and associated protection functions.
- Generator or synchronous condenser reactive capabilities.
- Volts per hertz limiter and associated protection functions.
- Stator over-voltage protection system settings.
- Generator and transformer volts per hertz capability.
- Time vs. field current or time vs. stator current.

NOTE: This listing is for reference only. This standard does not require the installation or activation of any of the above limiter or protection functions.

For this example, the Steady State Stability Limit (SSSL) is the limit to synchronous stability in the under-excited region with fixed field current.

On a P-Q diagram using X_d as the direct axis saturated synchronous reactance of the generator, X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer and V_g as the generator terminal voltage (all values in per-unit), the SSSL can be calculated as an arc with the center on the Q axis with the magnitude of the center and radius described by the following equations

$$C = V^2_g/2*(1/X_s-1/X_d)$$

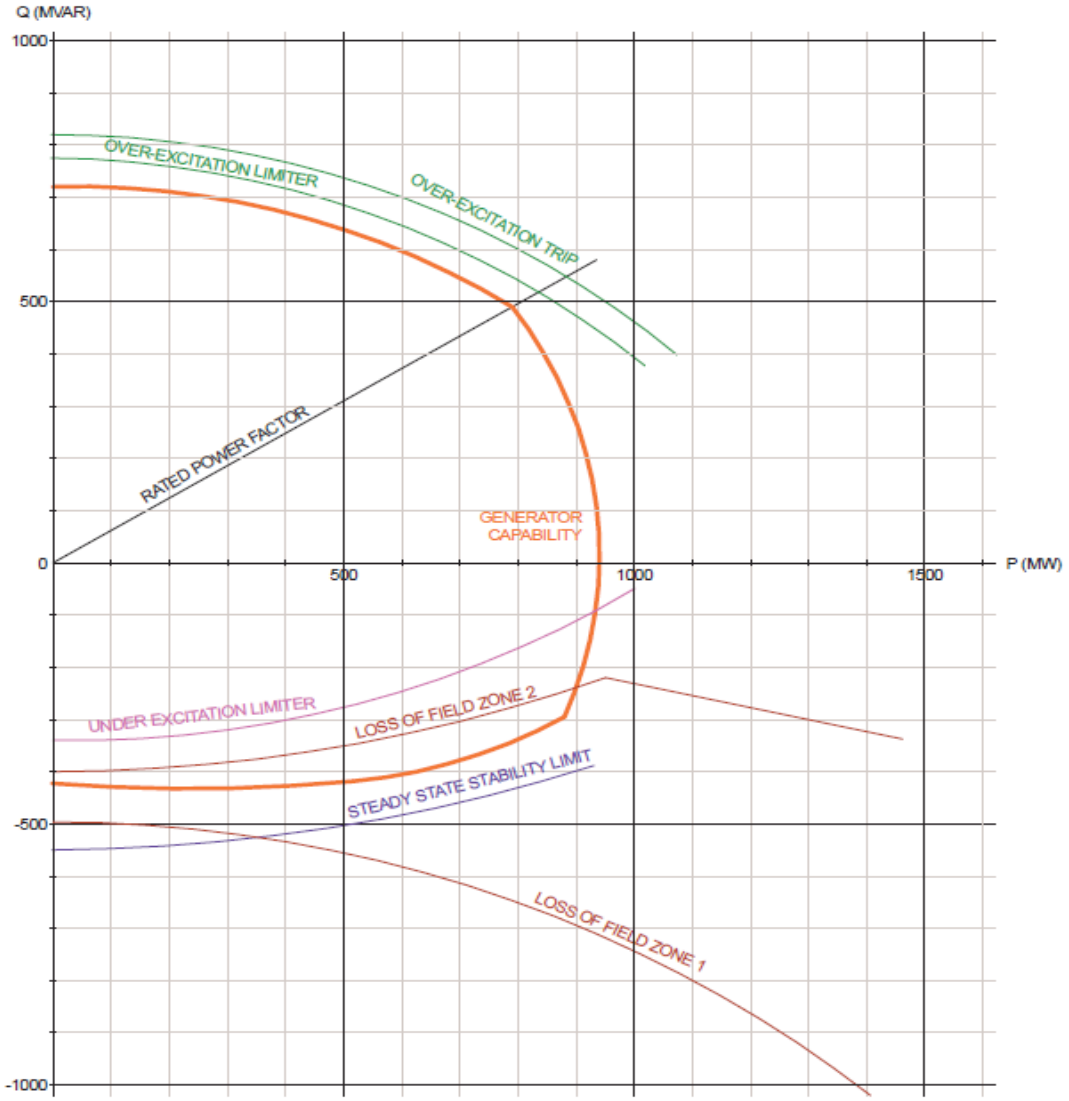
$$R = V^2_g/2*(1/X_s+1/X_d)$$

On an R-X diagram using X_d as the direct axis saturated synchronous reactance of the generator, and X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer the SSSL is an arc with the center on the X axis with the center and radius described by the following equations:

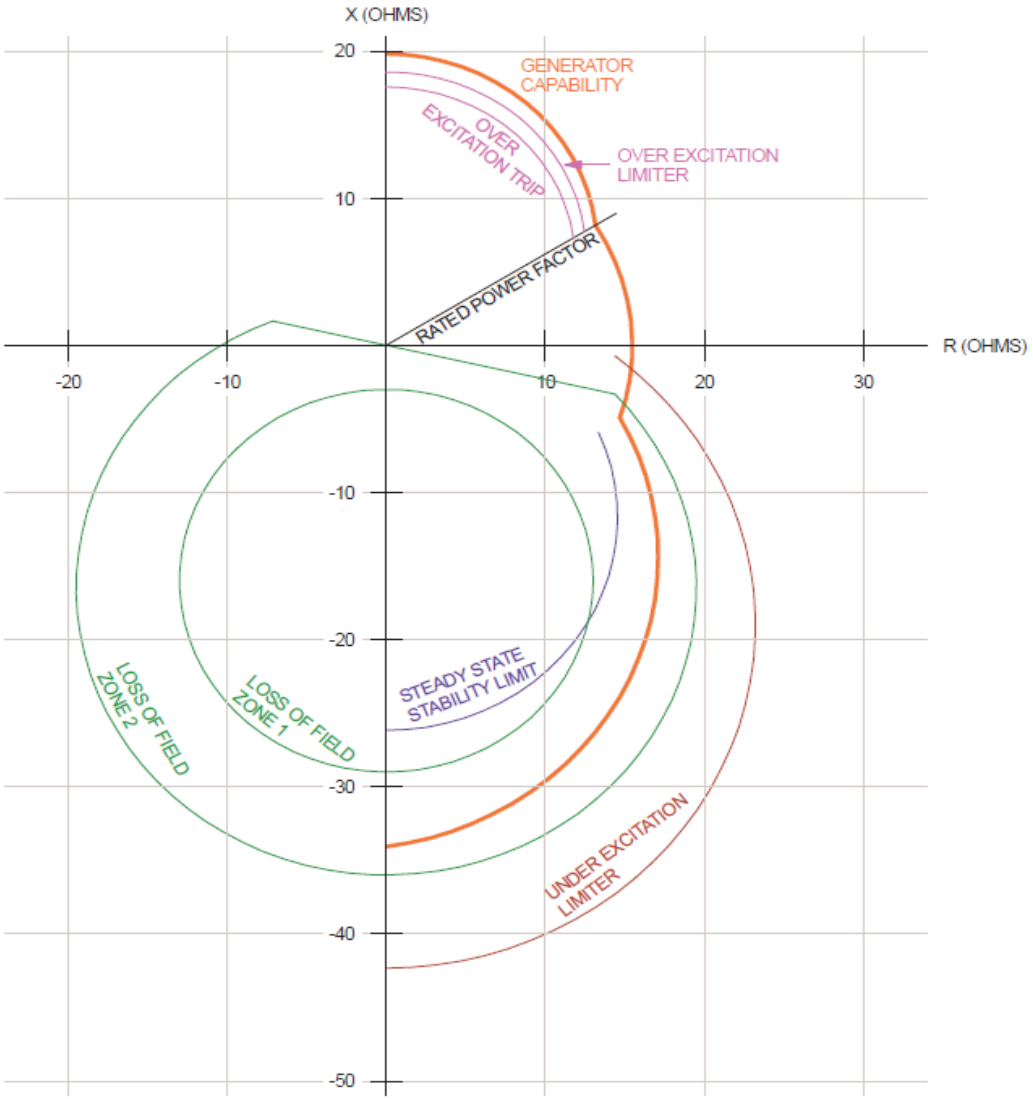
$$C = (X_d-X_s)/2$$

$$R = (X_d+X_s)/2$$

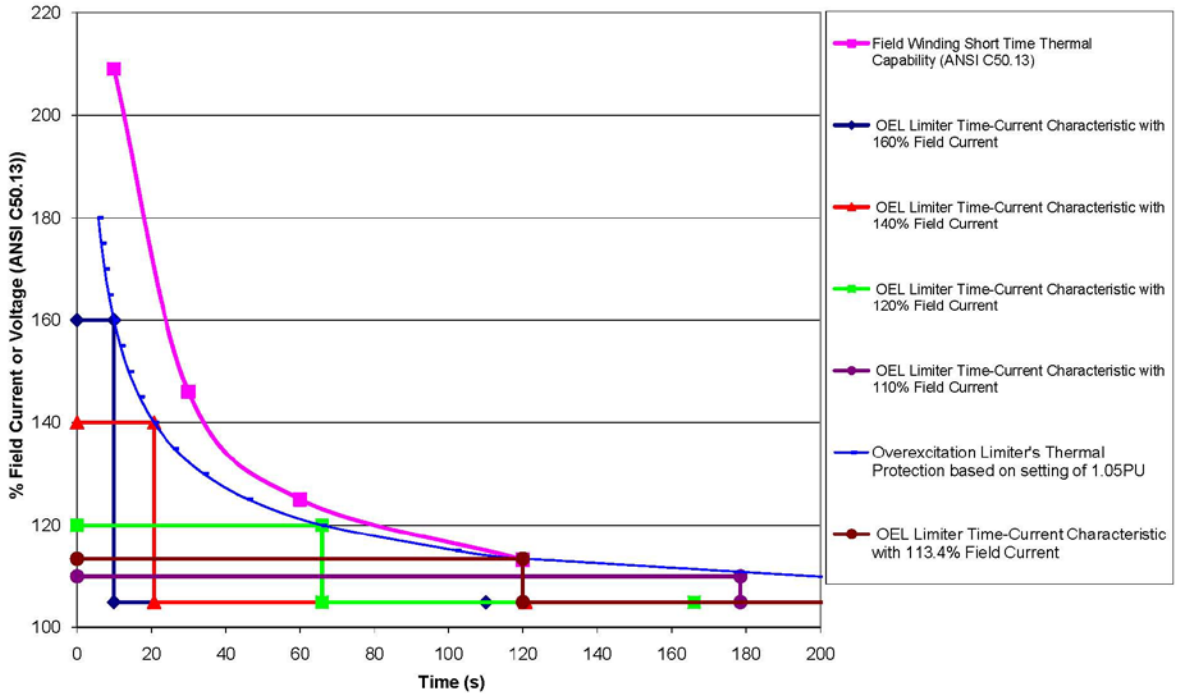
Section G Attachment 1 – Example of Capabilities, Limiters and Protection on a P-Q Diagram at nominal voltage and frequency



Section G Attachment 2 – Example of Capabilities, Limiters, and Protection on an R-X Diagram at nominal voltage and frequency



Section G Attachment 3 - Example of Capabilities, Limiters, and Protection on an Inverse Time Characteristic Plot



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Dispersed Generation Resources
PRC-019-2

Standards Involved

Approval:

- PRC-019-2 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

Retirement:

- PRC-019-1 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

Prerequisite Approvals:

N/A

Background

In light of the adoption of a revised Bulk Electric System (BES) definition by the NERC Board of Trustees, changes to the applicability sections of certain Reliability Standards, including PRC-019, are necessary to align the standards with the implementation of the revised BES definition. The standard drafting team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Generation Resources has modified the applicability section and requirements of certain standards applicable to Generator Owners and Generator Operators to recognize the unique technical and reliability aspects of dispersed power producing resources in order to ensure the applicability of the standards is consistent with the reliable operation of the BES.[1]

General Considerations

PRC-019-2 is proposed for approval to align the applicability section of PRC-019-1 with the revised definition of the BES. Specifically, the SDT has recommended revisions to the Facilities section to clarify that facilities that solely regulate voltage at the individual generating unit are subject to the requirements. Given the timing of concurrent standards development of PRC projects, PRC-019-1 may already be retired pursuant to an Implementation Plan of a successor version of PRC-. If this occurs, PRC-019-2 will not go into effect.

[1] The terms “dispersed generation resources” and “dispersed power producing resources” are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

Effective Date

PRC-019-2 shall become effective immediately after the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:

The existing standard, PRC-019-1, shall be retired at midnight of the day immediately prior to the Effective Date of PRC-019-2

Applicability:

This standard applies to the following functional entities:

- Transmission Owner that owns synchronous condenser(s)
- Generator Owner

Implementation Plan

All aspects of the Implementation Plan for PRC-019-1 will remain applicable to PRC-019-2 and are incorporated here by reference.

Cross References

The Implementation Plan for the revised definition of "Bulk Electric System" is available here.

The Implementation Plan for PRC-019-1 is available here.

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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-019-2 is proposed for approval to align the applicability section of PRC-019-1 with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 – Standards Applicability for Dispersed Generation Resources standards drafting team has recommended revisions to the Facilities section to clarify that facilities that solely regulate voltage at the individual generating unit are subject to the requirements. Given the timing of concurrent standards development of PRC projects, PRC-019-1 may be retired pursuant to an Implementation Plan of a successor version of PRC-019. If this occurs, PRC-019-2 will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.[1]

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The terms “dispersed generation resources” and “dispersed power producing resources” are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. **Title:** Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection

2. **Number:** PRC-019-21

3. **Purpose:** To verify coordination of generating unit Facility or synchronous condenser voltage regulating controls, limit functions, equipment capabilities and Protection System settings.

4. **Applicability:**

   4.1. Functional Entities

   4.1.1 Generator Owner

   4.1.2 Transmission Owner that owns synchronous condenser(s)

   4.2. Facilities

   For the purpose of this standard, the term, "applicable Facility" shall mean any one of the following:

   4.2.1 Individual generating unit greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

   4.2.2 Individual synchronous condenser greater than 20 MVA (gross nameplate rating) directly connected to the Bulk Electric System.

   4.2.3 Generating plant/ Facility consisting of one or more units that are connected to the Bulk Electric System at a common bus with total generation greater than 75 MVA (gross aggregate nameplate rating).

   4.2.3.1 This includes individual dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition where voltage regulating control for the facility is performed solely at the individual resources.

Rationale for Facilities section 4.2.3.1

For those dispersed power producing facilities that only perform voltage regulating control at the individual unit level, the SDT believes that coordination should take place at the individual power producing resource level. These facilities need to consider the Protection Systems at the individual units and their compatibility with the reactive and voltage limitations of the units. Where voltage regulating control is done at an aggregate level, applicability is already included under Facilities section 4.2.3.

4.2.4 Any generator, regardless of size, that is a blackstart unit material to and designated as part of a Transmission Operator's restoration plan.

5. Effective Date:

See the Implementation Plan for this standard.

~~**5.1.** In those jurisdictions where regulatory approval is required:~~

~~**5.1.1** By the first day of the first calendar quarter, two calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 40 percent of its applicable Facilities.~~

~~**5.1.2** By the first day of the first calendar quarter, three calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 60 percent of its applicable Facilities.~~

~~**5.1.3** By the first day of the first calendar quarter, four calendar years following applicable regulatory, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, approval each Generator Owner and Transmission Owner shall have verified at least 80 percent of its applicable Facilities.~~

~~**5.1.4** By the first day of the first calendar quarter, five calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified 100 percent of its applicable Facilities.~~

~~**5.2.** In those jurisdictions where regulatory approval is not required:~~

~~**5.2.1** By the first day of the first calendar quarter, two calendar years following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 40 percent of its applicable Facilities.~~

~~**5.2.2** By the first day of the first calendar quarter, three calendar years following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified at least 60 percent of its applicable Facilities.~~

~~**5.2.3** By the first day of the first calendar quarter, four calendar years following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator~~

~~Owner and Transmission Owner shall have verified at least 80 percent of its applicable Facilities.~~

~~5.2.4 By the first day of the first calendar quarter, five calendar years following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner and Transmission Owner shall have verified 100 percent of its applicable Facilities.~~

B. Requirements

R1. At a maximum of every five calendar years, each Generator Owner and Transmission Owner with applicable Facilities shall coordinate the voltage regulating system controls, (including in-service[2] limiters and protection functions) with the applicable equipment capabilities and settings of the applicable Protection System devices and functions. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

1.1. Assuming the normal automatic voltage regulator control loop and steady-state system operating conditions, verify the following coordination items for each applicable Facility:

1.1.1. The in-service limiters are set to operate before the Protection System of the applicable Facility in order to avoid disconnecting the generator unnecessarily.

1.1.2. The applicable in-service Protection System devices are set to operate to isolate or de-energize equipment in order to limit the extent of damage when operating conditions exceed equipment capabilities or stability limits.

R2. Within 90 calendar days following the identification or implementation of systems, equipment or setting changes that will affect the coordination described in Requirement R1, each Generator Owner and Transmission Owner with applicable Facilities shall perform the coordination as described in Requirement R1. These possible systems, equipment or settings changes include, but are not limited to the following *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*:

- Voltage regulating settings or equipment changes;
- Protection System settings or component changes;
- Generating or synchronous condenser equipment capability changes; or
- Generator or synchronous condenser step-up transformer changes.

C. Measures

[2] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

M1. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence (such as examples provided in PRC-019 Section G) that it coordinated the voltage regulating system controls, including in-service[3] limiters and protection functions, with the applicable equipment capabilities and settings of the applicable Protection System devices and functions as specified in Requirement R1. This evidence should include dated documentation that demonstrates the coordination was performed.

M2. Each Generator Owner and Transmission Owner with applicable Facilities will have evidence of the coordination required by the events listed in Requirement R2. This evidence should include dated documentation that demonstrates the specified intervals in Requirement R2 have been met.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Evidence Retention

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

The Generator Owner and Transmission Owner shall retain evidence of compliance with Requirements R1 and R2, Measures M1 and M2 for six years.

If a Generator Owner or Transmission Owner is found non-compliant, the entity shall keep information related to the non-compliance until mitigation is complete and approved or for the time period specified above, whichever is longer.

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

[3] Limiters or protection functions that are installed and activated on the generator or synchronous condenser.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years but less than or equal to 5 calendar years plus 4 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 4 months but less than or equal to 5 calendar years plus 8 months after the previous coordination.	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 5 calendar years plus 8 months but less than or equal to 5 calendar years plus 12 months after the previous coordination.	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 5 calendar years plus 12 months after the previous coordination.
R2	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 90 calendar days but less than or equal to 100 calendar days following the identification or implementation of a change in equipment	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 100 calendar days but less than or equal to 110 calendar days following the identification or implementation of a change in equipment	The Generator Owner or Transmission Owner coordinated equipment capabilities, limiters, and protection specified in Requirement R1 more than 110 calendar days but less than or equal to 120 calendar days following the identification or implementation of a change in equipment	The Generator Owner or Transmission Owner failed to coordinate equipment capabilities, limiters, and protection specified in Requirement R1 within 120 calendar days following the identification or implementation of a change in equipment or settings that

	or settings that affected the coordination.	or settings that affected the coordination.	or settings that affected the coordination.	affected the coordination.

E. Regional Variances

None.

F. Associated Documents

"Underexcited Operation of Turbo Generators", AIEE Proceedings T Section 881, Volume 67, 1948, Appendix 1, C. G. Adams and J. B. McClure.

,"Protective Relaying For Power Generation Systems", Boca Raton, FL, Taylor & Francis, 2006, Reimert, Donald

"Coordination of Generator Protection with Generator Excitation Control and Generator Capability", a report of Working Group J5 of the IEEE PSRC Rotating Machinery Subcommittee

"IEEE C37.102-2006 IEEE Guide for AC Generator Protection"

"IEEE C50.13-2005 IEEE Standard for Cylindrical-Rotor 50 Hz and 60 Hz Synchronous Generators Rated 10 MVA and Above"

Version History

Version	Date	Action	Change Tracking
1	February 7, 2013	Adopted by NERC Board of Trustees	New
1	March 20, 2014	FERC Order issued approving PRC-019-1. (Order becomes effective on 7/1/16.)	

G. Reference

Examples of Coordination

The evidence of coordination associated with Requirement R1 may be in the form of:

- P-Q Diagram (Example in Attachment 1), or
- R-X Diagram (Example in Attachment 2), or

- Inverse Time Diagram (Example in Attachment 3) or,
- Equivalent tables or other evidence

This evidence should include the equipment capabilities and the operating region for the limiters and protection functions

Equipment limits, types of limiters and protection functions which could be coordinated include (but are not limited to):

- Field over-excitation limiter and associated protection functions.
- Inverter over current limit and associated protection functions.
- Field under-excitation limiter and associated protection functions.
- Generator or synchronous condenser reactive capabilities.
- Volts per hertz limiter and associated protection functions.
- Stator over-voltage protection system settings.
- Generator and transformer volts per hertz capability.
- Time vs. field current or time vs. stator current.

NOTE: This listing is for reference only. This standard does not require the installation or activation of any of the above limiter or protection functions.

For this example, the Steady State Stability Limit (SSSL) is the limit to synchronous stability in the under-excited region with fixed field current.

On a P-Q diagram using X_d as the direct axis saturated synchronous reactance of the generator, X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer and V_g as the generator terminal voltage (all values in per-unit), the SSSL can be calculated as an arc with the center on the Q axis with the magnitude of the center and radius described by the following equations

$$C = V^2_g/2*(1/X_s-1/X_d)$$

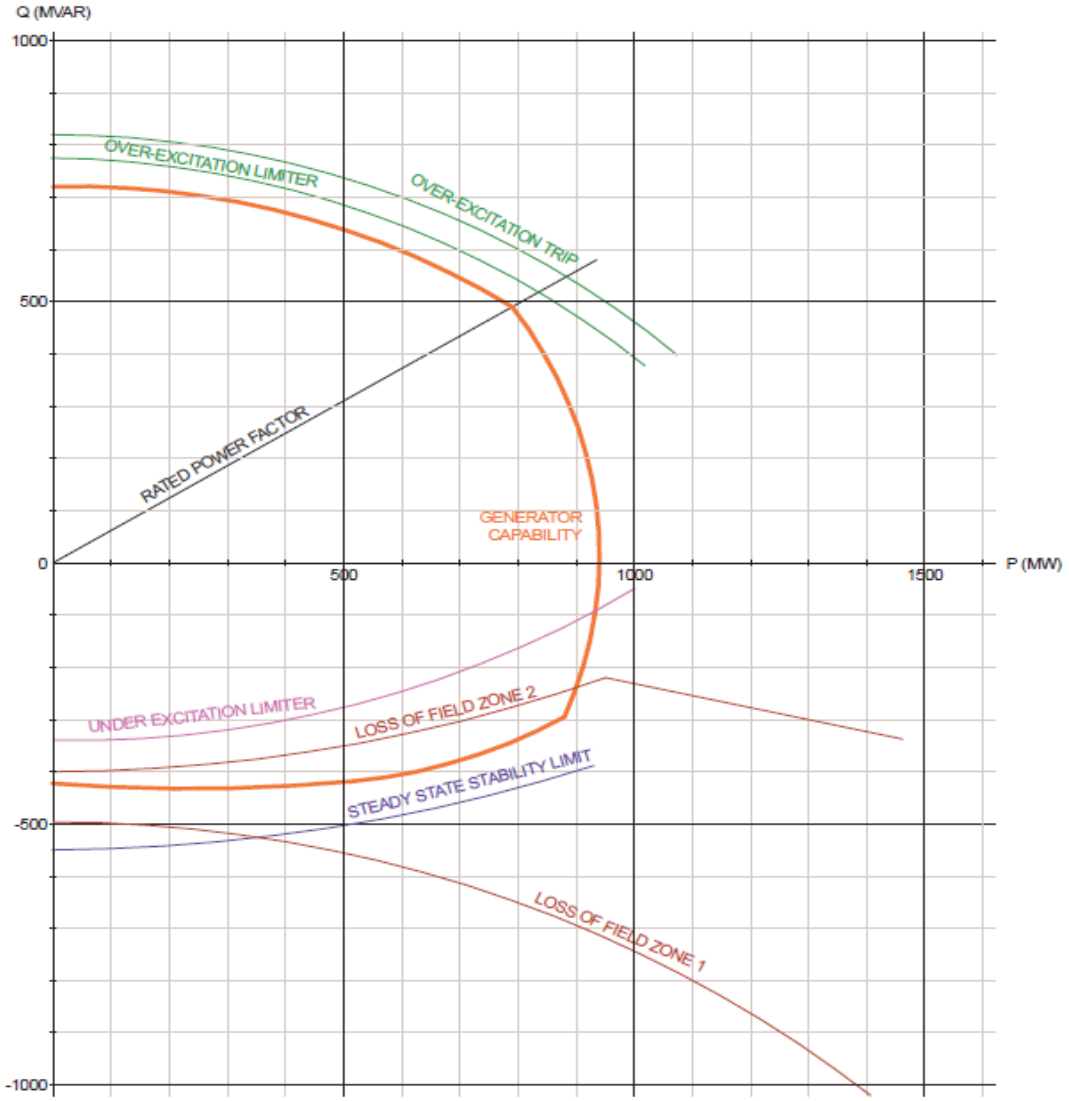
$$R = V^2_g/2*(1/X_s+1/X_d)$$

On an R-X diagram using X_d as the direct axis saturated synchronous reactance of the generator, and X_s as the equivalent reactance between the generator terminals and the "infinite bus" including the reactance of the generator step-up transformer the SSSL is an arc with the center on the X axis with the center and radius described by the following equations:

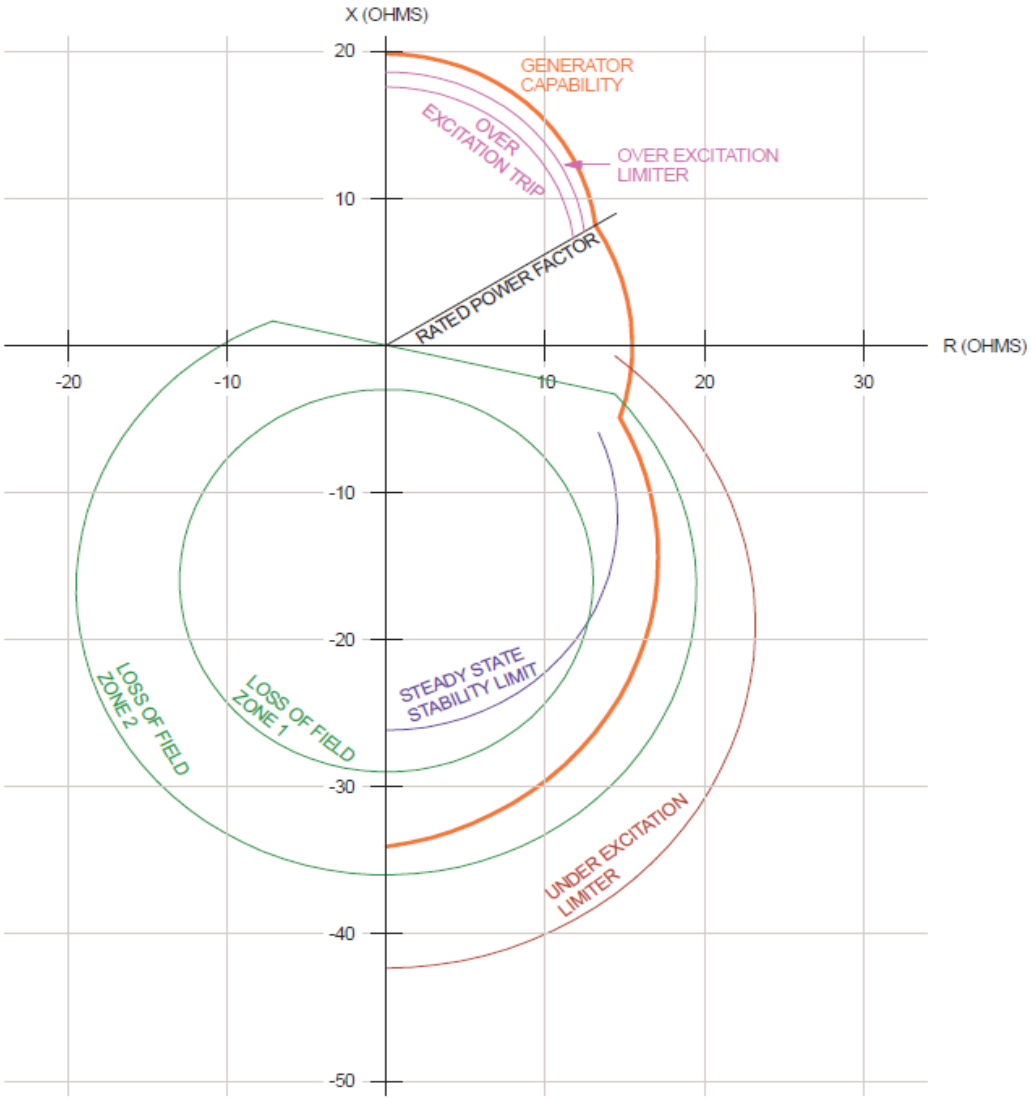
$$C = (X_d - X_s)/2$$

$$R = (X_d + X_s)/2$$

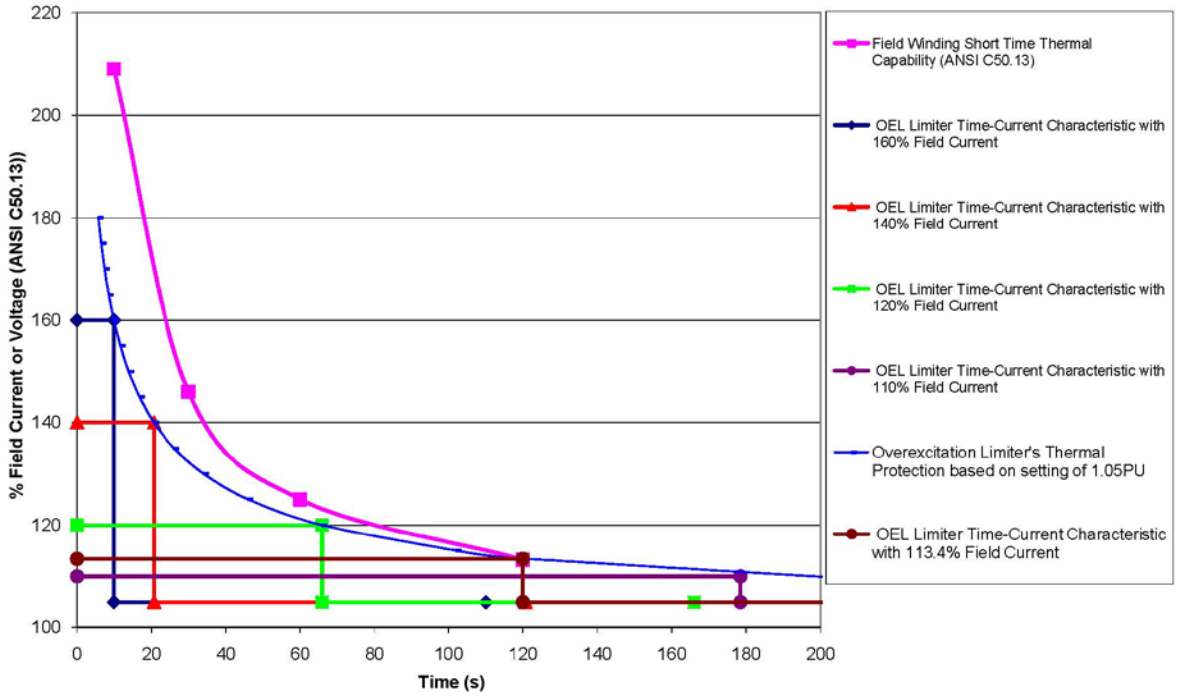
Section G Attachment 1 – Example of Capabilities, Limiters and Protection on a P-Q Diagram at nominal voltage and frequency



Section G Attachment 2 – Example of Capabilities, Limiters, and Protection on an R-X Diagram at nominal voltage and frequency



Section G Attachment 3 - Example of Capabilities, Limiters, and Protection on an Inverse Time Characteristic Plot



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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-024-1(X)[1] is proposed for approval to align the applicability section of PRC-024-1 with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 –Standards Applicability for Dispersed Generation Resources standards drafting team recommended changes to the requirements addressing the scope of applicability and also recommended changes to the Reliability Standard Audit Worksheet to address documentation options. Given the timing of concurrent standards development of PRC projects, PRC-024-1 may be retired pursuant to an Implementation Plan of a successor version of PRC-024. If this occurs, PRC-024-1(X) will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.[2]

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The standard version number currently includes an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

[2] The terms “dispersed generation resources” and “dispersed power producing resources” are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. **Title:** Generator Frequency and Voltage Protective Relay Settings

2. **Number: PRC-024-1(X)**

3. **Purpose:** Ensure Generator Owners set their generator protective relays such that generating units remain connected during defined frequency and voltage excursions.

4. **Applicability:**

   4.1. Generator Owner

5. **Effective Date:**

   See the Implementation Plan for this standard.

B. Requirements

R1. Each Generator Owner that has generator frequency protective relaying[3] activated to trip its applicable generating unit(s) shall set its protective relaying such that the generator frequency protective relaying does not trip the applicable generating unit(s) within the "no trip zone" of PRC-024 Attachment 1, subject to the following exceptions:[4] *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Generating unit(s) may trip if the protective functions (such as out-of-step functions or loss-of-field functions) operate due to an impending or actual loss of synchronism or, for asynchronous generating units, due to instability in power conversion control equipment.
- Generating unit(s) may trip if clearing a system fault necessitates disconnecting (a) generating unit(s).
- Generating unit(s) may trip within a portion of the "no trip zone" of PRC-024 Attachment 1 for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

[3] Each Generator Owner is not required to have frequency or voltage protective relaying (including but not limited to frequency and voltage protective functions for discrete relays, volts per hertz relays evaluated at nominal frequency, multi-function protective devices or protective functions within control systems that directly trip or provide tripping signals to the generator based on frequency or voltage inputs) installed or activated on its unit.

[4] For frequency protective relays associated with dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies to frequency protective relays applied on the individual power producing resources, as well as frequency protective relays applied on equipment from the individual power producing resource up to the point of interconnection.

Rationale for Footnotes 2 and 4

The SDT has determined it is appropriate to require that protective relay settings applied on both the individual generating units and aggregating equipment (including any non-Bulk Electric System collection system equipment) are set within the "no-trip zone" referenced in the requirements to maintain reliability of the BES. If any of the protective relay settings applied on these elements of the facility were to be excluded from this standard, the potential would exist for portions of or the entire generating capacity of the dispersed power producing facility to be lost during a voltage or frequency excursion.

R2. Each Generator Owner that has generator voltage protective relaying[3] activated to trip its applicable generating unit(s) shall set its protective relaying such that the generator voltage protective relaying does not trip the applicable generating unit(s) as a result of a voltage excursion (at the point of interconnection[5]) caused by an event on the transmission system external to the generating plant that remains within the "no trip zone" of PRC-024 Attachment 2.[6] If the Transmission Planner allows less stringent voltage relay settings than those required to meet PRC-024 Attachment 2, then the Generator Owner shall set its protective relaying within the voltage recovery characteristics of a location-specific Transmission Planner's study. Requirement R2 is subject to the following exceptions: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Generating unit(s) may trip in accordance with a Special Protection System (SPS) or Remedial Action Scheme (RAS).
- Generating unit(s) may trip if clearing a system fault necessitates disconnecting (a) generating unit(s).
- Generating unit(s) may trip by action of protective functions (such as out-of-step functions or loss-of-field functions) that operate due to an impending or actual loss of synchronism or, for asynchronous generating units, due to instability in power conversion control equipment.
- Generating unit(s) may trip within a portion of the "no trip zone" of PRC-024 Attachment 2 for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

[5] For the purposes of this standard, point of interconnection means the transmission (high voltage) side of the generator step-up or collector transformer.

[6] For voltage protective relays associated with dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies to voltage protective relays applied on the individual power producing resources, as well as voltage protective relays applied on equipment from the individual power producing resource up to the point of interconnection.

R3. Each Generator Owner shall document each known regulatory or equipment limitation[7] that prevents an applicable generating unit with generator frequency or voltage protective relays from meeting the relay setting criteria in Requirements R1 or R2 including (but not limited to) study results, experience from an actual event, or manufacturer's advice. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. The Generator Owner shall communicate the documented regulatory or equipment limitation, or the removal of a previously documented regulatory or equipment limitation, to its Planning Coordinator and Transmission Planner within 30 calendar days of any of the following:

- Identification of a regulatory or equipment limitation.
- Repair of the equipment causing the limitation that removes the limitation.
- Replacement of the equipment causing the limitation with equipment that removes the limitation.
- Creation or adjustment of an equipment limitation caused by consumption of the cumulative turbine life-time frequency excursion allowance.

R4. Each Generator Owner shall provide its applicable generator protection trip settings associated with Requirements R1 and R2 to the Planning Coordinator or Transmission Planner that models the associated unit within 60 calendar days of receipt of a written request for the data and within 60 calendar days of any change to those previously requested trip settings unless directed by the requesting Planning Coordinator or Transmission Planner that the reporting of relay setting changes is not required. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Generator Owner shall have evidence that generator frequency protective relays have been set in accordance with Requirement R1 such as dated setting sheets, calibration sheets or other documentation.

M2. Each Generator Owner shall have evidence that generator voltage protective relays have been set in accordance with Requirement R2 such as dated setting sheets, voltage-time curves, calibration sheets, coordination plots, dynamic simulation studies or other documentation.

M3. Each Generator Owner shall have evidence that it has documented and communicated any known regulatory or equipment limitations (excluding limitations noted in footnote 3) that resulted in an exception to Requirements R1 or R2 in accordance with Requirement R3 such as a dated email or letter that contains such documentation as study results, experience from an actual event, or manufacturer's advice.

[7] Excludes limitations that are caused by the setting capability of the generator frequency and voltage protective relays themselves but does not exclude limitations originating in the equipment that they protect.

M4. Each Generator Owner shall have evidence that it communicated applicable generator protective relay trip settings in accordance with Requirement R4, such as dated e-mails, correspondence or other evidence and copies of any requests it has received for that information.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Data 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.

The Generator Owner shall retain evidence of compliance with Requirement R1 through R4; for 3 years or until the next audit, whichever is longer.

If a Generator Owner is found non-compliant, the Generator Owner shall keep information related to the non-compliance until mitigation is complete and approved for the time period 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

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Generator Owner that has frequency protection activated to trip a generating unit, failed to set its generator frequency protective relaying so that it does not trip within the criteria listed in Requirement R1 unless there is a documented and communicated regulatory or equipment limitation per Requirement R3.
R2	N/A	N/A	N/A	The Generator Owner with voltage protective relaying activated to trip a generating unit, failed to set its voltage protective relaying so that it does not trip as a result of a voltage excursion at the point of interconnection, caused by an event external to the plant per the criteria specified in Requirement R2 unless there is a documented and communicated regulatory or equipment limitation per Requirement R3.
R3	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner failed to document any known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	limitation to its Planning Coordinator and Transmission Planner more than 30 calendar days but less than or equal to 60 calendar days of identifying the limitation.	limitation to its Planning Coordinator and Transmission Planner more than 60 calendar days but less than or equal to 90 calendar days of identifying the limitation.	limitation to its Planning Coordinator and Transmission Planner more than 90 calendar days but less than or equal to 120 calendar days of identifying the limitation.	OR The Generator Owner failed to communicate the documented limitation to its Planning Coordinator and Transmission Planner within 120 calendar days of identifying the limitation.
R4	The Generator Owner provided its generator protection trip settings more than 60 calendar days but less than or equal to 90 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 60 calendar days but less than or equal to 90 calendar days of a written request.	The Generator Owner provided its generator protection trip settings more than 90 calendar days but less than or equal to 120 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 90 calendar days but less than or equal to 120 calendar days of a written request.	The Generator Owner provided its generator protection trip settings more than 120 calendar days but less than or equal to 150 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 120 calendar days but less than or equal to 150 calendar days of a written request.	The Generator Owner failed to provide its generator protection trip settings within 150 calendar days of any change to those trip settings. OR The Generator Owner failed to provide trip settings within 150 calendar days of a written request.

E. Regional Variances

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	May 9, 2013	Adopted by the NERC Board of Trustees	

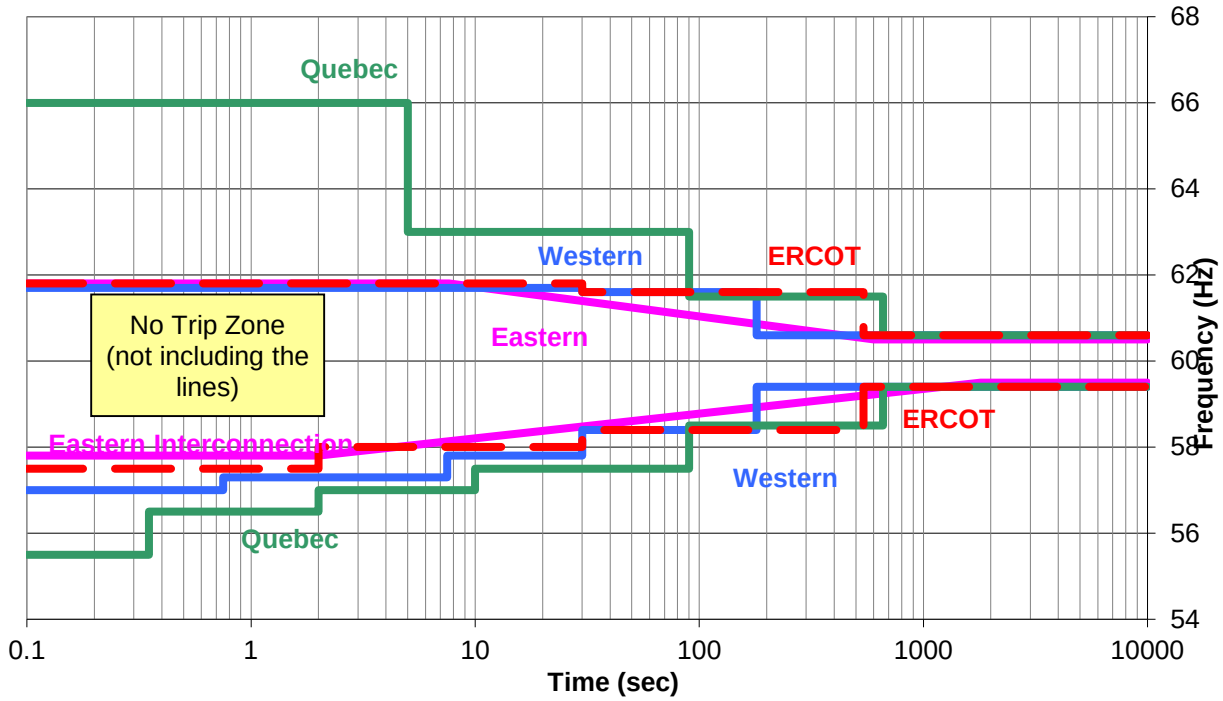
1	March 20, 2014	FERC Order issued approving PRC-024-1. (Order becomes effective on 7/1/16.)	

G. References

1. "The Technical Justification for the New WECC Voltage Ride-Through (VRT) Standard, A White Paper Developed by the Wind Generation Task Force (WGTF)," dated June 13, 2007, a guideline approved by WECC Technical Studies Subcommittee.

PRC-024 — Attachment 1

OFF NOMINAL FREQUENCY CAPABILITY CURVE



Curve Data Points:

Eastern Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.8	Instantaneous trip	≤57.8	Instantaneous trip
≥60.5	$10^{(90.935-1.45713*f)}$	≤59.5	$10^{(1.7373*f-100.116)}$
<60.5	Continuous operation	> 59.5	Continuous operation

Western Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.7	Instantaneous trip	≤57.0	Instantaneous trip
≥61.6	30	≤57.3	0.75
≥60.6	180	≤57.8	7.5
<60.6	Continuous operation	≤58.4	30
		≤59.4	180
		>59.4	Continuous operation

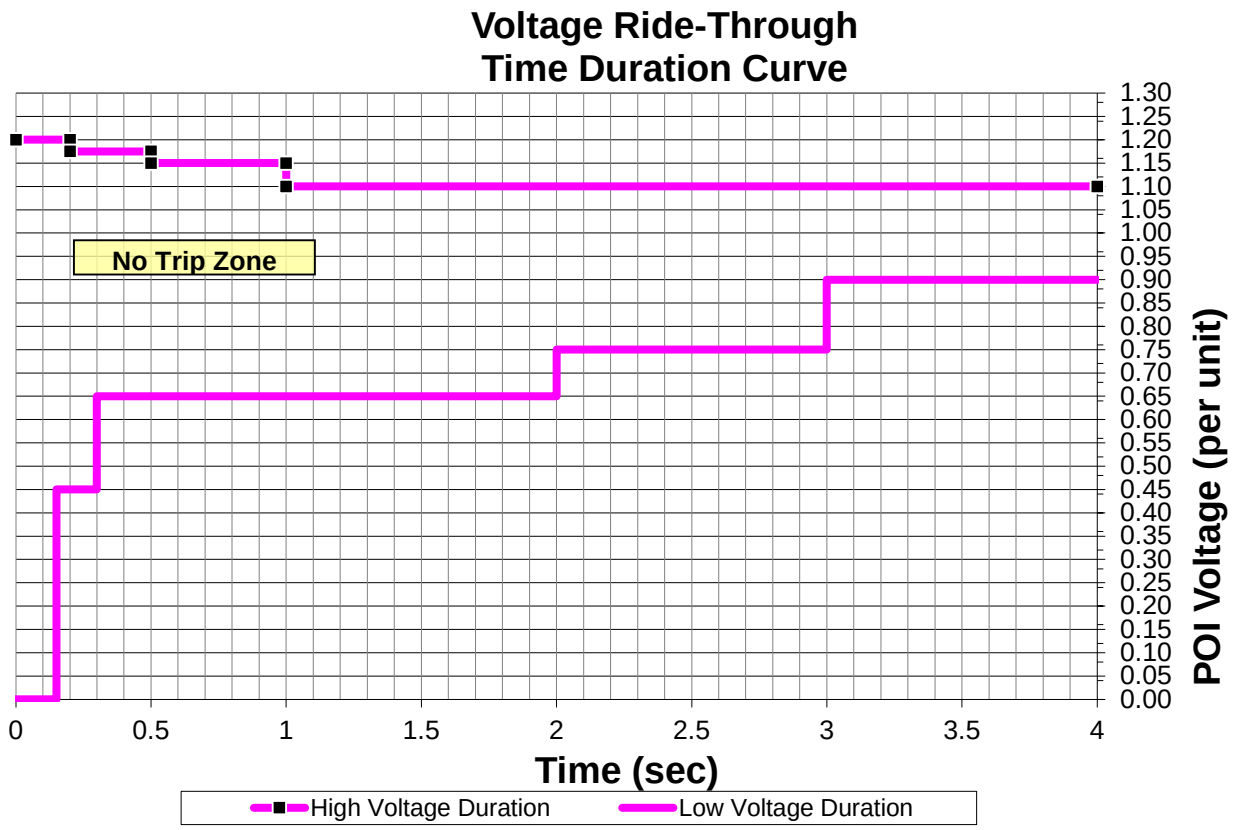
Quebec Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (Sec)
>66.0	Instantaneous trip	<55.5	Instantaneous trip
≥63.0	5	≤56.5	0.35
≥61.5	90	≤57.0	2
≥60.6	660	≤57.5	10
<60.6	Continuous operation	≤58.5	90
		≤59.4	660
		>59.4	Continuous operation

ERCOT Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.8	Instantaneous trip	≤57.5	Instantaneous trip
≥61.6	30	≤58.0	2
≥60.6	540	≤58.4	30
<60.6	Continuous operation	≤59.4	540
		>59.4	Continuous operation

PRC-024— Attachment 2



Ride Through Duration:

High Voltage Ride Through Duration		Low Voltage Ride Through Duration	
Voltage (pu)	Time (sec)	Voltage (pu)	Time (sec)
≥1.200	Instantaneous trip	<0.45	0.15
≥1.175	0.20	<0.65	0.30
≥1.15	0.50	<0.75	2.00
≥1.10	1.00	<0.90	3.00

Voltage Ride-Through Curve Clarifications

Curve Details:

1. The per unit voltage base for these curves is the nominal operating voltage specified by the Transmission Planner in the analysis of the reliability of the Interconnected Transmission Systems at the point of interconnection to the Bulk Electric System (BES).
2. The curves depicted were derived based on three-phase transmission system zone 1 faults with Normal Clearing not exceeding 9 cycles. The curves apply to voltage excursions regardless of the type of initiating event.
3. The envelope within the curves represents the cumulative voltage duration at the point of interconnection with the BES. For example, if the voltage first exceeds 1.15 pu at 0.3 seconds after a fault, does not exceed 1.2 pu voltage, and returns below 1.15 pu at 0.4 seconds, then the cumulative time the voltage is above 1.15 pu voltage is 0.1 seconds and is within the no trip zone of the curve.
4. The curves depicted assume system frequency is 60 Hertz. When evaluating Volts/Hertz protection, you may adjust the magnitude of the high voltage curve in proportion to deviations of frequency below 60 Hz.
5. Voltages in the curve assume minimum fundamental frequency phase-to-ground or phase-to-phase voltage for the low voltage duration curve and the greater of maximum RMS or crest phase-to-phase voltage for the high voltage duration curve.

Evaluating Protective Relay Settings:

1. Use either the following assumptions or loading conditions that are believed to be the most probable for the unit under study to evaluate voltage protection relay setting calculations on the static case for steady state initial conditions:
    a. All of the units connected to the same transformer are online and operating.
    b. All of the units are at full nameplate real-power output.
    c. Power factor is 0.95 lagging (i.e. supplying reactive power to the system) as measured at the generator terminals.
    d. The automatic voltage regulator is in automatic voltage control mode.
2. Evaluate voltage protection relay settings assuming that additional installed generating plant reactive support equipment (such as static VAr compensators, synchronous condensers, or capacitors) is available and operating normally.
3. Evaluate voltage protection relay settings accounting for the actual tap settings of transformers between the generator terminals and the point of interconnection.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Dispersed Generation Resources
PRC-024-1(X)

The standard version numbers currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

Standards Involved

Approval:

- PRC-024-1(X) – Generator Frequency and Voltage Protective Relay Settings

Retirement:

- PRC-024-1 – Generator Frequency and Voltage Protective Relay Settings

Prerequisite Approvals:

N/A

Background

In light of the adoption of a revised Bulk Electric System (BES) definition by the NERC Board of Trustees, changes to the applicability of certain Reliability Standards, including PRC-024, are necessary to align the standards with the revised BES definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Generation Resources has modified the applicability section or requirements of certain standards applicable to Generator Owners and Generator Operators to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the BES.

General Considerations

PRC-024-1(X) is proposed for approval to align the applicability of PRC-024-1 with the revised definition of the BES. Specifically, the SDT recommended changes to the requirements addressing the scope of applicability and also recommended changes to the Reliability Standard Audit Worksheet to address documentation options. Given the timing of concurrent standards development of PRC projects, PRC-024-1 may be retired pursuant to an Implementation Plan of a successor version of PRC-024. If this occurs, PRC-024-1(X) will not go into effect.

Effective Date

PRC-024-1(X) shall become effective immediately after the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first

calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:
The existing standard, PRC-024-1, shall be retired at midnight of the day immediately prior to the Effective Date of PRC-024-1(X).

Applicability:
This standard applies to the following functional entities:

- Generator Owner

Implementation Plan
All aspects of the Implementation Plan for PRC-024-1 will remain applicable to PRC-024-(X) and are incorporated here by reference.

Cross References
The Implementation Plan for the revised definition of "Bulk Electric System" is available here.

The Implementation Plan for PRC-024-1 is available here.

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 November 20 – December 19, 2013.
2. The Standards Committee authorized this posting on September 30, 2014.

Description of Current Draft

PRC-024-1(X)[1] is proposed for approval to align the applicability section of PRC-024-1 with the revised definition of the Bulk Electric System (BES). Specifically, the Project 2014-01 –Standards Applicability for Dispersed Generation Resources standards drafting team recommended changes to the requirements addressing the scope of applicability and also recommended changes to the Reliability Standard Audit Worksheet to address documentation options. Given the timing of concurrent standards development of PRC projects, PRC-024-1 may be retired pursuant to an Implementation Plan of a successor version of PRC-024. If this occurs, PRC-024-1(X) will not go into effect. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the requirements of this standard to dispersed power producing resources.[2]

Anticipated Actions	Anticipated Date
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	December 2014
Final ballot	January 2015
BOT adoption	February 2015

[1] The standard version number currently includes an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to adoption by the NERC Board of Trustees.

[2] The terms “dispersed generation resources” and “dispersed power producing resources” are used interchangeably in Project 2014-01 because the former term was used in the Standards Authorization Request for the project, while the latter term is in line with terminology used in the revised definition of the BES.

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

A. Introduction

1. **Title:** Generator Frequency and Voltage Protective Relay Settings

2. **Number:** **PRC-024-1(X)**

3. **Purpose:** Ensure Generator Owners set their generator protective relays such that generating units remain connected during defined frequency and voltage excursions.

4. **Applicability:**

   4.1. Generator Owner

5. **Effective Date:**

   See the Implementation Plan for this standard.

~~In those jurisdictions where regulatory approval is required:~~

~~By the first day of the first calendar quarter, two calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner shall have verified at least 40 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, three calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner shall have verified at least 60 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, four calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner shall have verified at least 80 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, five calendar years following applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities, each Generator Owner shall have verified 100 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~In those jurisdictions where regulatory approval is not required:~~

~~By the first day of the first calendar quarter, two calendar years following Board of Trustees approval, each Generator Owner shall have verified at least 40 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, three calendar years following Board of Trustees approval, each Generator Owner shall have verified at least 60 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, four calendar years following Board of Trustees approval, each Generator Owner shall have verified at least 80 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

~~By the first day of the first calendar quarter, five calendar years following Board of Trustees approval, each Generator Owner shall have verified 100 percent of its Facilities are fully compliant with Requirements R1, R2, R3, and R4.~~

B. Requirements

R1. Each Generator Owner that has generator frequency protective relaying[3] activated to trip its applicable generating unit(s) shall set its protective relaying such that the generator frequency protective relaying does not trip the applicable generating unit(s) within the "no trip zone" of PRC-024 Attachment 1, subject to the following exceptions:[4] *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Generating unit(s) may trip if the protective functions (such as out-of-step functions or loss-of-field functions) operate due to an impending or actual loss of synchronism or, for asynchronous generating units, due to instability in power conversion control equipment.
- Generating unit(s) may trip if clearing a system fault necessitates disconnecting (a) generating unit(s).
- Generating unit(s) may trip within a portion of the "no trip zone" of PRC-024 Attachment 1 for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

Rationale for Footnotes 2 and 4

The SDT has determined it is appropriate to require that protective relay settings applied on both the individual generating units and aggregating equipment (including any non-Bulk Electric System collection system equipment) are set within the "no-trip zone" referenced in the requirements to maintain reliability of the BES. If any of the protective relay settings applied on these elements of the facility were to be excluded from this standard, the potential would exist for portions of or the entire generating capacity of the dispersed power producing facility to be lost during a voltage or frequency excursion.

R2. Each Generator Owner that has generator voltage protective relaying[3] activated to trip its applicable generating unit(s) shall set its protective relaying such that the generator voltage protective relaying does not trip the applicable generating unit(s) as a result of a voltage excursion (at the point of interconnection[5]) caused by an event on the

[3] Each Generator Owner is not required to have frequency or voltage protective relaying (including but not limited to frequency and voltage protective functions for discrete relays, volts per hertz relays evaluated at nominal frequency, multi-function protective devices or protective functions within control systems that directly trip or provide tripping signals to the generator based on frequency or voltage inputs) installed or activated on its unit.

[4] For frequency protective relays associated with dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies to frequency protective relays applied on the individual power producing resources, as well as frequency protective relays applied on equipment from the individual power producing resource up to the point of interconnection.

[5] For the purposes of this standard, point of interconnection means the transmission (high voltage) side of the generator step-up or collector transformer.

transmission system external to the generating plant that remains within the "no trip zone" of PRC-024 Attachment 2.[6] If the Transmission Planner allows less stringent voltage relay settings than those required to meet PRC-024 Attachment 2, then the Generator Owner shall set its protective relaying within the voltage recovery characteristics of a location-specific Transmission Planner's study. Requirement R2 is subject to the following exceptions: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Generating unit(s) may trip in accordance with a Special Protection System (SPS) or Remedial Action Scheme (RAS).
- Generating unit(s) may trip if clearing a system fault necessitates disconnecting (a) generating unit(s).
- Generating unit(s) may trip by action of protective functions (such as out-of-step functions or loss-of-field functions) that operate due to an impending or actual loss of synchronism or, for asynchronous generating units, due to instability in power conversion control equipment.
- Generating unit(s) may trip within a portion of the "no trip zone" of PRC-024 Attachment 2 for documented and communicated regulatory or equipment limitations in accordance with Requirement R3.

R3. Each Generator Owner shall document each known regulatory or equipment limitation[7] that prevents an applicable generating unit with generator frequency or voltage protective relays from meeting the relay setting criteria in Requirements R1 or R2 including (but not limited to) study results, experience from an actual event, or manufacturer's advice. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1. The Generator Owner shall communicate the documented regulatory or equipment limitation, or the removal of a previously documented regulatory or equipment limitation, to its Planning Coordinator and Transmission Planner within 30 calendar days of any of the following:

- Identification of a regulatory or equipment limitation.
- Repair of the equipment causing the limitation that removes the limitation.
- Replacement of the equipment causing the limitation with equipment that removes the limitation.
- Creation or adjustment of an equipment limitation caused by consumption of the cumulative turbine life-time frequency excursion allowance.

[6] For voltage protective relays associated with dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies to voltage protective relays applied on the individual power producing resources, as well as voltage protective relays applied on equipment from the individual power producing resource up to the point of interconnection.

[7] Excludes limitations that are caused by the setting capability of the generator frequency and voltage protective relays themselves but does not exclude limitations originating in the equipment that they protect.

R4. Each Generator Owner shall provide its applicable generator protection trip settings associated with Requirements R1 and R2 to the Planning Coordinator or Transmission Planner that models the associated unit within 60 calendar days of receipt of a written request for the data and within 60 calendar days of any change to those previously requested trip settings unless directed by the requesting Planning Coordinator or Transmission Planner that the reporting of relay setting changes is not required. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Generator Owner shall have evidence that generator frequency protective relays have been set in accordance with Requirement R1 such as dated setting sheets, calibration sheets or other documentation.

M2. Each Generator Owner shall have evidence that generator voltage protective relays have been set in accordance with Requirement R2 such as dated setting sheets, voltage-time curves, calibration sheets, coordination plots, dynamic simulation studies or other documentation.

M3. Each Generator Owner shall have evidence that it has documented and communicated any known regulatory or equipment limitations (excluding limitations noted in footnote 3) that resulted in an exception to Requirements R1 or R2 in accordance with Requirement R3 such as a dated email or letter that contains such documentation as study results, experience from an actual event, or manufacturer's advice.

M4. Each Generator Owner shall have evidence that it communicated applicable generator protective relay trip settings in accordance with Requirement R4, such as dated e-mails, correspondence or other evidence and copies of any requests it has received for that information.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

1.2. Data 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.

The Generator Owner shall retain evidence of compliance with Requirement R1 through R4; for 3 years or until the next audit, whichever is longer.

If a Generator Owner is found non-compliant, the Generator Owner shall keep information related to the non-compliance until mitigation is complete and approved for the time period 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

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Generator Owner that has frequency protection activated to trip a generating unit, failed to set its generator frequency protective relaying so that it does not trip within the criteria listed in Requirement R1 unless there is a documented and communicated regulatory or equipment limitation per Requirement R3.
R2	N/A	N/A	N/A	The Generator Owner with voltage protective relaying activated to trip a generating unit, failed to set its voltage protective relaying so that it does not trip as a result of a voltage excursion at the point of interconnection, caused by an event external to the plant per the criteria specified in Requirement R2 unless there is a documented and communicated regulatory or equipment limitation per Requirement R3.
R3	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner documented the known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2 and communicated the documented	The Generator Owner failed to document any known non-protection system equipment limitation that prevented it from meeting the criteria in Requirement R1 or R2.

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	limitation to its Planning Coordinator and Transmission Planner more than 30 calendar days but less than or equal to 60 calendar days of identifying the limitation.	limitation to its Planning Coordinator and Transmission Planner more than 60 calendar days but less than or equal to 90 calendar days of identifying the limitation.	limitation to its Planning Coordinator and Transmission Planner more than 90 calendar days but less than or equal to 120 calendar days of identifying the limitation.	OR The Generator Owner failed to communicate the documented limitation to its Planning Coordinator and Transmission Planner within 120 calendar days of identifying the limitation.
R4	The Generator Owner provided its generator protection trip settings more than 60 calendar days but less than or equal to 90 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 60 calendar days but less than or equal to 90 calendar days of a written request.	The Generator Owner provided its generator protection trip settings more than 90 calendar days but less than or equal to 120 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 90 calendar days but less than or equal to 120 calendar days of a written request.	The Generator Owner provided its generator protection trip settings more than 120 calendar days but less than or equal to 150 calendar days of any change to those trip settings. OR The Generator Owner provided trip settings more than 120 calendar days but less than or equal to 150 calendar days of a written request.	The Generator Owner failed to provide its generator protection trip settings within 150 calendar days of any change to those trip settings. OR The Generator Owner failed to provide trip settings within 150 calendar days of a written request.

E. Regional Variances

None

F. Associated Documents

None

Version History

Version	Date	Action	Change Tracking
1	May 9, 2013	Adopted by the NERC Board of Trustees	

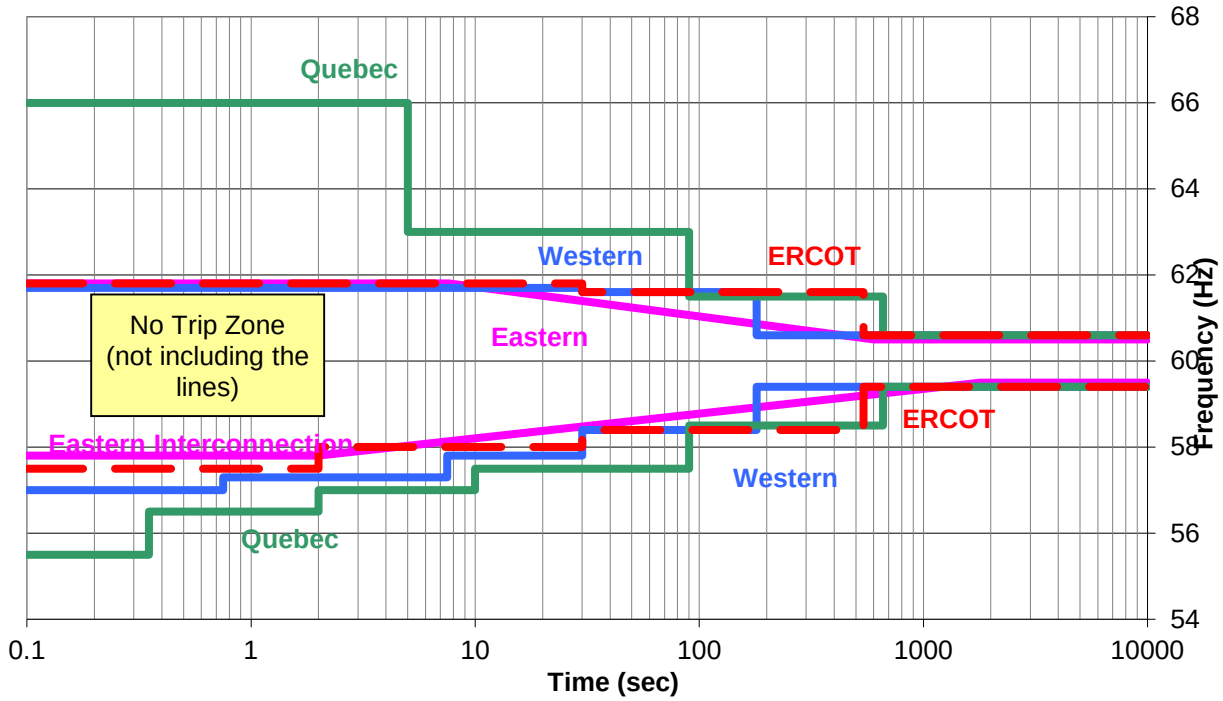
1	March 20, 2014	FERC Order issued approving PRC-024-1. (Order becomes effective on 7/1/16.)	

G. References

1. "The Technical Justification for the New WECC Voltage Ride-Through (VRT) Standard, A White Paper Developed by the Wind Generation Task Force (WGTF)," dated June 13, 2007, a guideline approved by WECC Technical Studies Subcommittee.

PRC-024 — Attachment 1

OFF NOMINAL FREQUENCY CAPABILITY CURVE



Curve Data Points:

Eastern Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.8	Instantaneous trip	≤57.8	Instantaneous trip
≥60.5	$10^{(90.935-1.45713*f)}$	≤59.5	$10^{(1.7373*f-100.116)}$
<60.5	Continuous operation	> 59.5	Continuous operation

Western Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.7	Instantaneous trip	≤57.0	Instantaneous trip
≥61.6	30	≤57.3	0.75
≥60.6	180	≤57.8	7.5
<60.6	Continuous operation	≤58.4	30
		≤59.4	180
		>59.4	Continuous operation

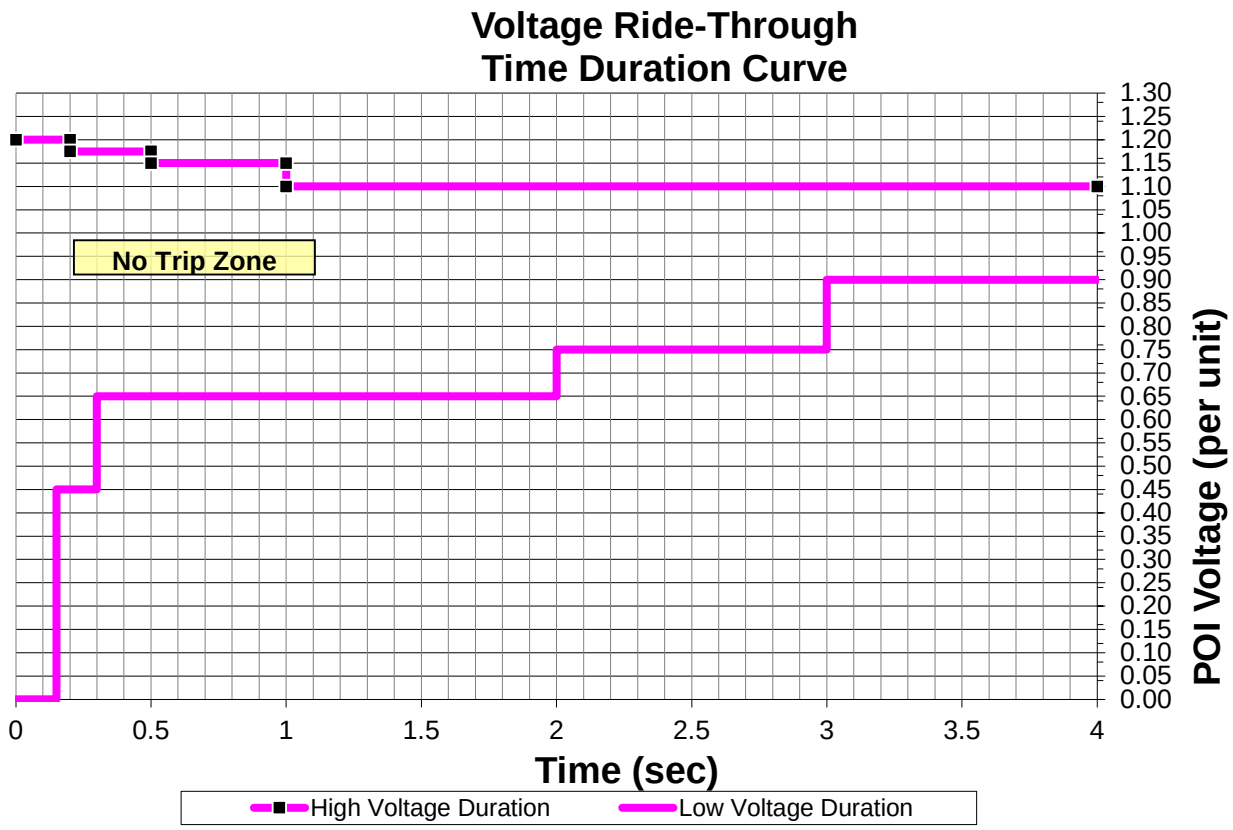
Quebec Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (Sec)
>66.0	Instantaneous trip	<55.5	Instantaneous trip
≥63.0	5	≤56.5	0.35
≥61.5	90	≤57.0	2
≥60.6	660	≤57.5	10
<60.6	Continuous operation	≤58.5	90
		≤59.4	660
		>59.4	Continuous operation

ERCOT Interconnection

High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Time (Sec)	Frequency (Hz)	Time (sec)
≥61.8	Instantaneous trip	≤57.5	Instantaneous trip
≥61.6	30	≤58.0	2
≥60.6	540	≤58.4	30
<60.6	Continuous operation	≤59.4	540
		>59.4	Continuous operation

PRC-024— Attachment 2



Ride Through Duration:

High Voltage Ride Through Duration		Low Voltage Ride Through Duration	
Voltage (pu)	**Time (sec)**	**Voltage (pu)**	**Time (sec)**
≥1.200	Instantaneous trip	<0.45	0.15
≥1.175	0.20	<0.65	0.30
≥1.15	0.50	<0.75	2.00
≥1.10	1.00	<0.90	3.00

Voltage Ride-Through Curve Clarifications

Curve Details:

1. The per unit voltage base for these curves is the nominal operating voltage specified by the Transmission Planner in the analysis of the reliability of the Interconnected Transmission Systems at the point of interconnection to the Bulk Electric System (BES).
2. The curves depicted were derived based on three-phase transmission system zone 1 faults with Normal Clearing not exceeding 9 cycles. The curves apply to voltage excursions regardless of the type of initiating event.
3. The envelope within the curves represents the cumulative voltage duration at the point of interconnection with the BES. For example, if the voltage first exceeds 1.15 pu at 0.3 seconds after a fault, does not exceed 1.2 pu voltage, and returns below 1.15 pu at 0.4 seconds, then the cumulative time the voltage is above 1.15 pu voltage is 0.1 seconds and is within the no trip zone of the curve.
4. The curves depicted assume system frequency is 60 Hertz. When evaluating Volts/Hertz protection, you may adjust the magnitude of the high voltage curve in proportion to deviations of frequency below 60 Hz.
5. Voltages in the curve assume minimum fundamental frequency phase-to-ground or phase-to-phase voltage for the low voltage duration curve and the greater of maximum RMS or crest phase-to-phase voltage for the high voltage duration curve.

Evaluating Protective Relay Settings:

1. Use either the following assumptions or loading conditions that are believed to be the most probable for the unit under study to evaluate voltage protection relay setting calculations on the static case for steady state initial conditions:
    a. All of the units connected to the same transformer are online and operating.
    b. All of the units are at full nameplate real-power output.
    c. Power factor is 0.95 lagging (i.e. supplying reactive power to the system) as measured at the generator terminals.
    d. The automatic voltage regulator is in automatic voltage control mode.
2. Evaluate voltage protection relay settings assuming that additional installed generating plant reactive support equipment (such as static VAr compensators, synchronous condensers, or capacitors) is available and operating normally.
3. Evaluate voltage protection relay settings accounting for the actual tap settings of transformers between the generator terminals and the point of interconnection.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

November 25, 2014

This Implementation Plan for the Reliability Standards developed as part of Project 2014-02 CIP Version 5 Revisions replaces the Implementation Plan for the versions of those CIP Reliability Standards adopted by the NERC Board of Trustees on November 13, 2014.

Requested Approvals

- CIP-003-7 — Cyber Security — Security Management Controls
- CIP-004-7 — Cyber Security — Personnel & Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems*
- CIP-007-7 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems*
- CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-3 — Cyber Security — Information Protection

Requested Withdrawals

- CIP-003-6 — Cyber Security — Security Management Controls

---

* The NERC Board of Trustees adopted Reliability Standards CIP-006-6 and CIP-009-6, and an associated implementation plan, on November 13, 2014. While these Reliability Standards are not being presented again for ballot or Board adoption, they are included herein for ease of reference and to provide a single implementation plan that contains all of the Reliability Standards adopted as part of Project 2014-02 CIP Version 5 Revisions.

- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact

	disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset	A Cyber Asset that is (i) capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Low Impact External Routable Connectivity (LERC)	Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The compliance date for those particular sections represents the date that entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-7 — Cyber Security — Security Management Controls

Reliability Standard CIP-003-7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-7, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

Compliance Date for CIP-003-7, Requirement R2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

Compliance Date for CIP-003-7, Attachment 1, Section 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Attachment 1, Section 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

Compliance Date for CIP-003-7, Attachment 1, Section 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Attachment 1, Section 2 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

Compliance Date for CIP-003-7, Attachment 1, Section 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Attachment 1, Section 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

Compliance Date for CIP-003-7, Attachment 1, Section 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-7, Attachment 1, Section 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-7.

2. CIP-004-7 — Cyber Security — Personnel & Training

   Reliability Standard CIP-004-7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[1]

   Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

[1] The NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-7 — Cyber Security — Systems Security Management

Reliability Standard CIP-007-7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-7, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-007-7, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with high and medium impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-7.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[2]

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the

[2] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-3 — Cyber Security — Configuration Change Management and Vulnerability Assessments

   Reliability Standard CIP-010-3 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-010-3, Requirement R4

   Registered Entities shall not be required to comply with Reliability Standard CIP-010-3, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-3.

7. CIP-011-3 — Cyber Security — Information Protection

   Reliability Standard CIP-011-3 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the compliance date for Reliability Standard CIP-010-3, Requirement R4, as applicable in the relevant jurisdiction.

The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the compliance date for Reliability Standard CIP-003-7, Requirement R2, as applicable in the relevant jurisdiction.

9. Standards for Retirement

CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.[3]

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.[4]

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-3 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the new standard is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[5] (Version 5 Plan) remain the same:

[3] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.
[4] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-7, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[5] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

~~September 3, 2014~~November 25, 2014

This Implementation Plan for the Reliability Standards developed as part of Project 2014-02 CIP Version 5 Revisions replaces the Implementation Plan for the versions of those CIP Reliability Standards adopted by the NERC Board of Trustees on November 13, 2014.

Requested Approvals

- CIP-003-~~6~~ 7 — Cyber Security — Security Management Controls
- CIP-004-~~6~~ 7 — Cyber Security — Personnel ~~and~~ & Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[*]~~-~~
- CIP-007-~~6~~ 7 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems~~-~~[*]
- CIP-010-~~2~~ 3 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-~~2~~ 3 — Cyber Security — Information Protection

Requested ~~Retirements~~Withdrawals

- CIP-003-~~5~~ 6 — Cyber Security — Security Management Controls

[*] The NERC Board of Trustees adopted Reliability Standards CIP-006-6 and CIP-009-6, and an associated implementation plan, on November 13, 2014. While these Reliability Standards are not being presented again for ballot or Board adoption, they are included herein for ease of reference and to provide a single implementation plan that contains all of the Reliability Standards adopted as part of Project 2014-02 CIP Version 5 Revisions.

- CIP-004-~~5~~ 6 — Cyber Security — Personnel ~~and~~ & Training
- ~~CIP-006-5 — Cyber Security — Physical Security~~
- CIP-007-~~5~~ 6 — Cyber Security — Systems Security Management
- ~~CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems~~
- CIP-010-~~1~~ 2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-~~1~~ 2 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Storage ~~Media~~media~~,~~ that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less~~, capable of transmitting~~

	~~executable code to:~~ to ~~(1)~~ a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a Protected Cyber Asset ~~that can be used to store, copy, move, or access data~~. ~~Removable Media are not Cyber Assets.~~ Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset	A Cyber Asset~~,~~ that is (i) capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is ~~(e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication)~~ directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to~~, capable of transmitting executable code to: (1)~~ a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a ~~Protected Cyber Asset~~PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that ~~allows~~ controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems. ~~The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.~~
Low Impact External Routable Connectivity (LERC)	Direct user-initiated interactive access or a direct device-to-device connection to a~~Bi-directional routable communications between~~ low impact BES Cyber System(s) ~~and~~ from a Cyber Asset~~s~~ outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. ~~Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from~~ Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular ~~element~~section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof) ~~of a proposed Reliability Standard~~, the additional time for compliance with that ~~element~~section is specified below. The compliance date for those particular ~~element~~sections represents the date that entities must begin to comply with that particular ~~element~~section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-~~6~~ 7 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-~~6~~ 7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-~~6~~7, Requirement R1, Part 1.2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

   Compliance Date for CIP-003-~~6~~7, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

   Compliance Date for CIP-003-~~6~~7, Attachment 1, ~~element~~Section 1

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Attachment 1, ~~element~~Section 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

Compliance Date for CIP-003-~~6~~7, Attachment 1, ~~element~~Section 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Attachment 1, ~~element~~Section 2 until the later of ~~April~~ September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

Compliance Date for CIP-003-~~6~~7, Attachment 1, ~~element~~Section 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Attachment 1, ~~element~~Section 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

Compliance Date for CIP-003-~~6~~7, Attachment 1, ~~element~~Section 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~6~~7, Attachment 1, ~~element~~Section 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-~~6~~7.

2. CIP-004-~~6~~ 7 — Cyber Security — Personnel ~~and~~ & Training

Reliability Standard CIP-004-~~6~~ 7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[1]

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-~~6~~ 7 — Cyber Security — Systems Security Management

Reliability Standard CIP-007-~~6~~ 7 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-~~6~~7, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with ~~the elements of~~ Reliability Standard CIP-007-~~6~~7, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a

[1] The NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

PSP and inside an ESP and associated with ~~High~~ high and ~~Medium~~ medium ~~Impact~~ impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-~~6~~7.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[2]

   Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-~~2~~ 3 — Cyber Security — Configuration Change Management and Vulnerability Assessments

   Reliability Standard CIP-010-~~2~~ 3 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-010-~~2~~3, Requirement R4

   Registered Entities shall not be required to comply with Reliability Standard CIP-010-~~2~~3, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-~~2~~3.

7. CIP-011-~~2~~ 3 — Cyber Security — Information Protection

   Reliability Standard CIP-011-~~2~~ 3 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable

[2] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the ~~same~~ compliance date ~~as when~~for Reliability Standard CIP-010-~~2~~3, Requirement R4, as applicable in the relevant jurisdiction~~is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction~~.

The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the ~~same~~ compliance date ~~as when~~for Reliability Standard CIP-003-~~6~~7, Requirement R2, as applicable in the relevant jurisdiction~~is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction~~.

9. Standards for Retirement

CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.[3]

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-7 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.[4]

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-3 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the new standard is becoming effective.
~~Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.~~

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[5] (Version 5 Plan) remain the same:

[3] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-~~6~~7, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[4] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

[5] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period and Ballot	November 2014
Final Ballot is Conducted	January 2015
Board of Trustees (Board) Adoption	February 2015
Filing to Applicable Regulatory Authorities	February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-003-7

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-7.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

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 Reliability 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.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their list of assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of 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 CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 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 so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior

Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-7, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-7, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-7, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-7, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-7, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-7, Requirement R2,	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-7, Requirement R2, Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-7, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-7, Requirement R2, Attachment 1, Section 3. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-7, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to CIP-003-7,	The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-7, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to CIP-003-7,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-7, Requirement R2, Attachment 1, Section 3. (R2)	Requirement R2, Attachment 1, Section 2. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document this change in less than 40 calendar days of the change. (R3)	days but did document this change in less than 50 calendar days of the change. (R3)	less than 60 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-003-7 - Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-7 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1 - Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2 - Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing the LEAP.

Section 3 - Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections for any LEAP are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4 - Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should 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 Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through

successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- 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
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate 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

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- 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

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to 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

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability 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 R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse

or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems or the low impact BES Cyber System itself or LEAPs, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or

control houses. User authorization programs and lists of authorized users for physical access are not required although would help meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term “electronic access control” is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of the communication within its low impact cyber security plan.

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP even though there technically is LERC. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.” The intent of “direct” in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for “device-to-device connection,” LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems “behind” it, however, should not allow uncontrolled access from one asset to all other assets sharing the LEAP.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and

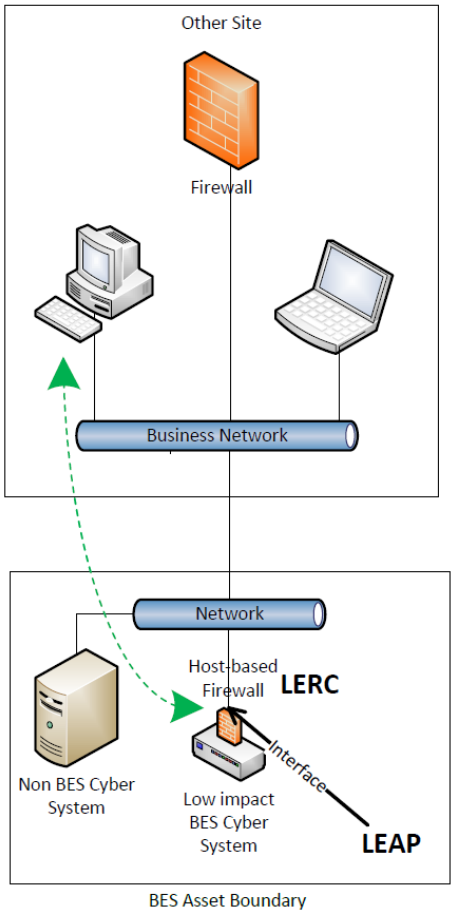
outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.

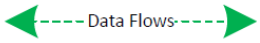
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

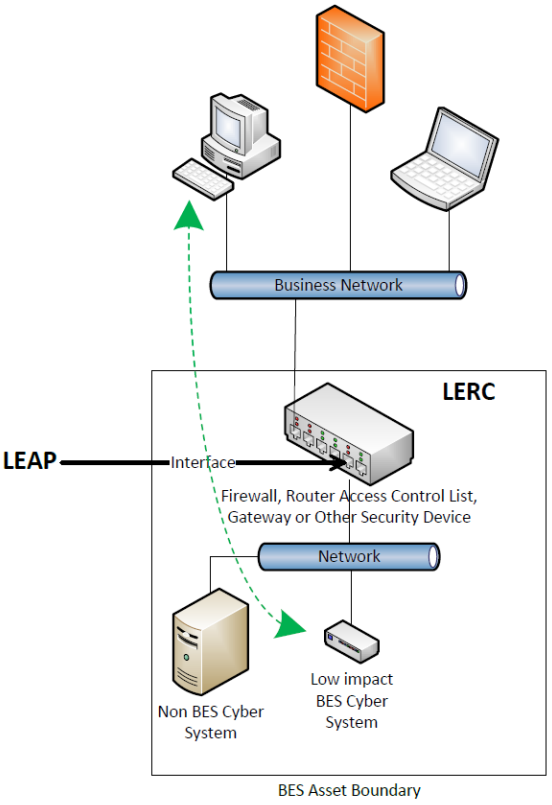
The following diagrams provide reference examples to depict the rationale for identifying whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.





REFERENCE MODEL - 1

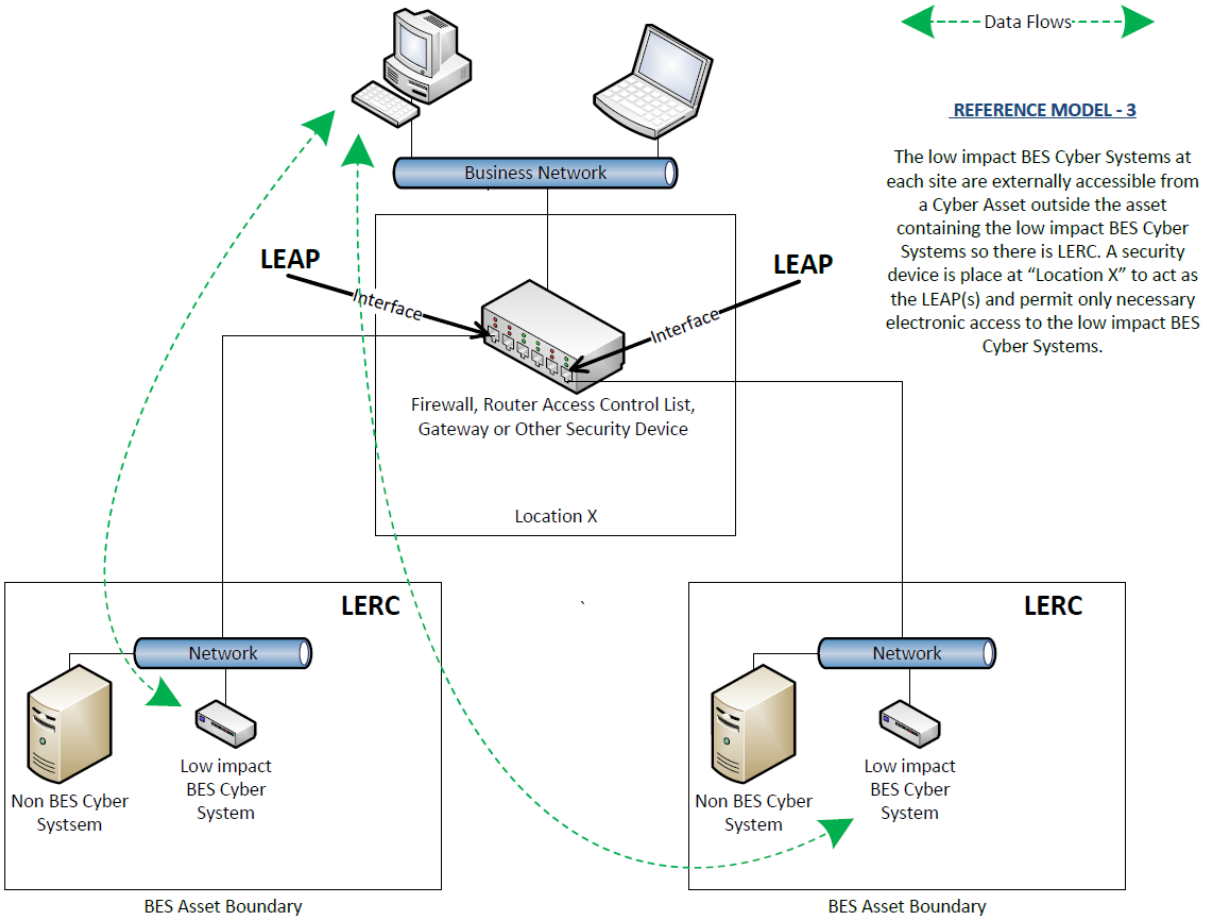
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

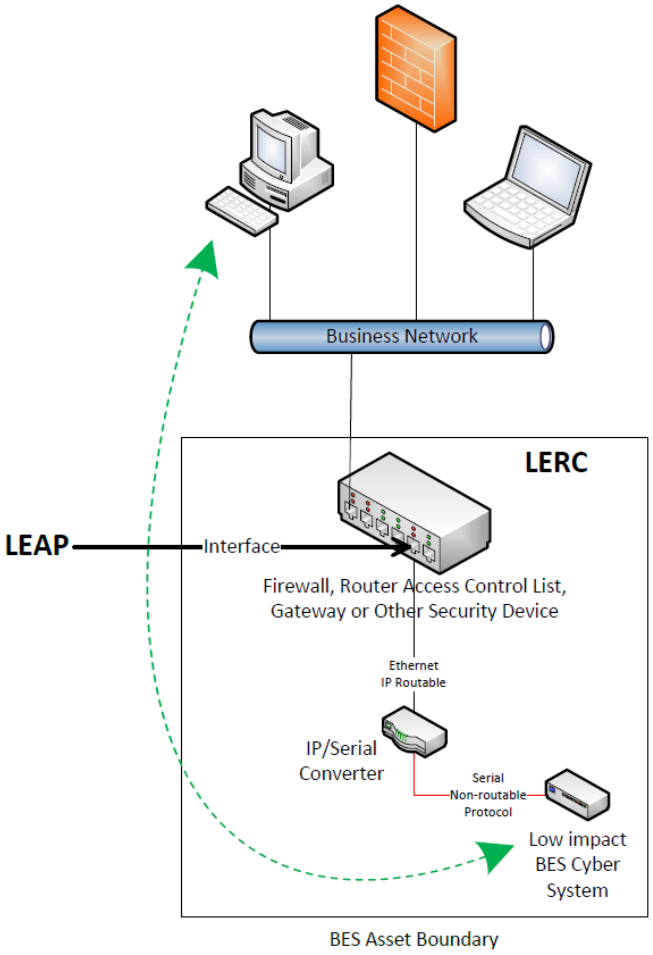


Data Flows

REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

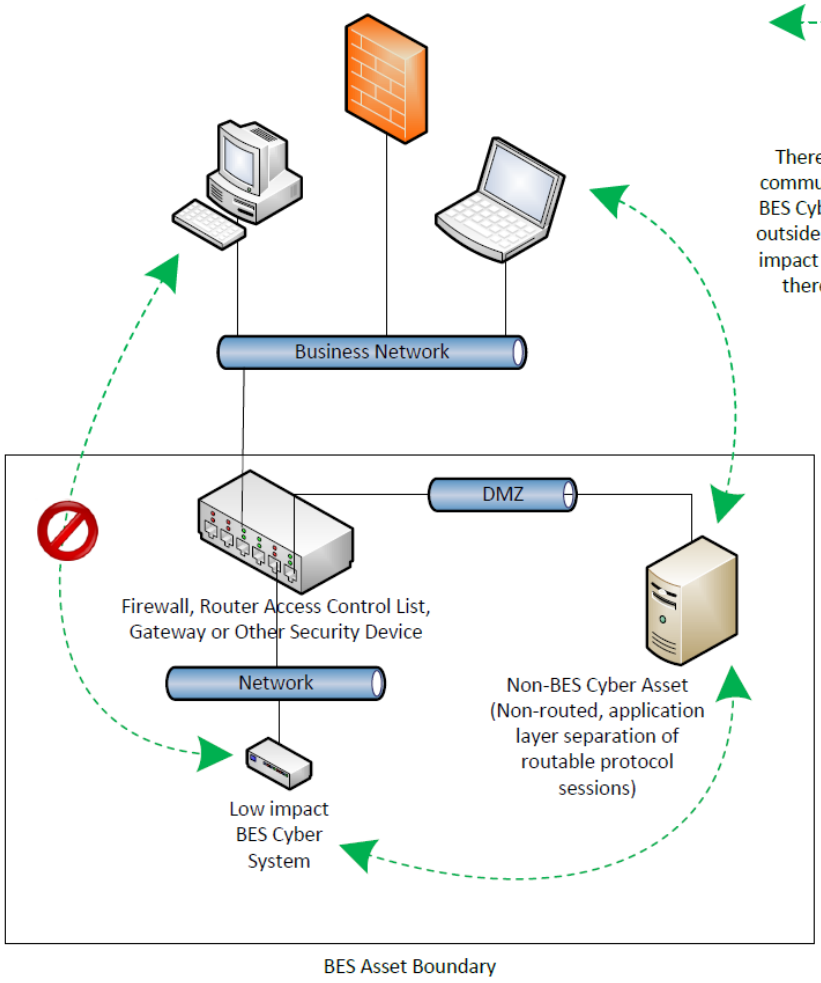

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

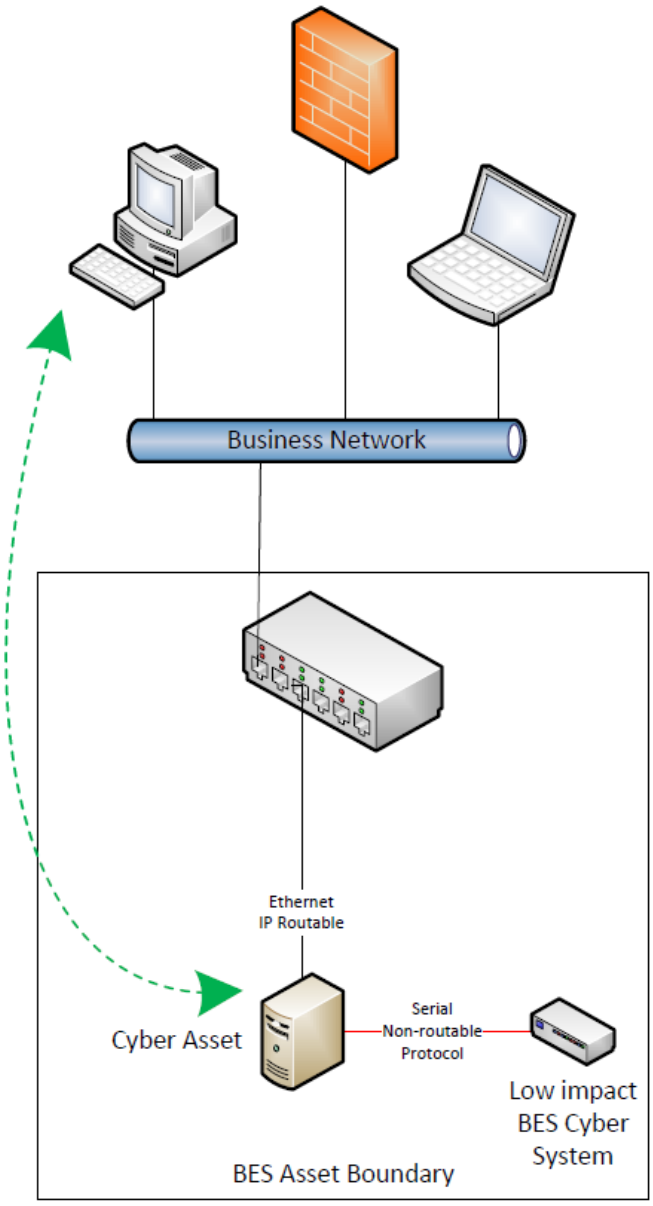


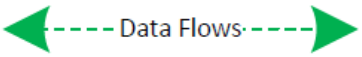
Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

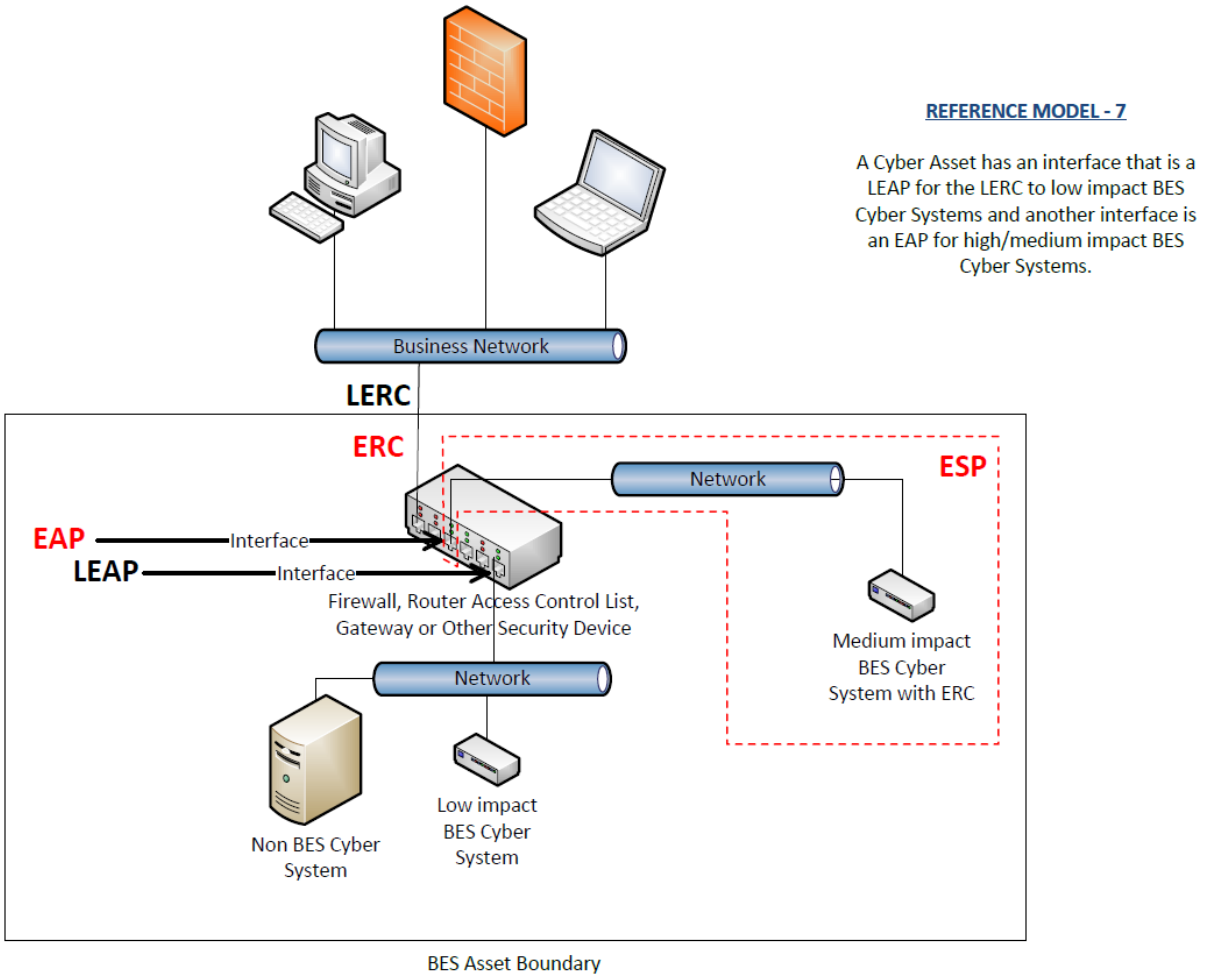

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary





REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement 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 its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows 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.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period and Ballot	~~September~~ November 2014
Final Ballot is Conducted	~~October/November 2014~~January 2015
Board of Trustees (Board) Adoption	~~November 2014~~February 2015
Filing to Applicable Regulatory Authorities	~~December 2014~~February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
~~6~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-~~6~~7

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~6~~7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

~~Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~ See Implementation Plan for CIP-003-7.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require ~~a minimum level of~~ organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

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 Reliability 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.

Responsible Entities can implement common controls that meet requirements for multiple high, ~~and~~ medium, and low impact BES Cyber Systems. For example, a single ~~training~~ cyber security awareness program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save

the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within ~~regional~~ Regional ~~reliability~~ Reliability ~~standards~~ Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the ~~standard's~~ requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to ~~its~~ a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the ~~standard's~~ requirements.

Annual review and approval of the cyber security ~~policy~~ policies ensures that the ~~policy~~ policies ~~is~~ are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident ~~Response~~response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives ~~The requirement to implement a cyber security plan~~ for assets containing low impact BES Cyber Systems. ~~provides a minimum set of cyber security controls for assets containing low impact BES Cyber Systems. Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised. To that end,~~ The ~~Requirement R2 requires Responsible Entities to implement documented~~ cyber security plan(s) ~~covering~~ covers four subject matter areas: ~~–~~ (1) cyber security awareness~~,~~; (2) physical ~~access~~ security controls~~,~~; (3) electronic access controls~~,~~; and (4) ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response. ~~In response to directives in FERC Order No. 791, Requirement R2 provides for the specific elements that must be included in the cyber security plan(s). Attachment 1 provides these elements. These~~ This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for ~~sufficient~~ operational, procedural, and technical safeguards for ~~assets containing~~ low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the ~~Bulk Power System~~BES, Attachment 1 provides Responsible Entities flexibility on how to apply the ~~required~~ security controls to meet the security objectives. Additionally, ~~the SDT recognizes that~~because many Responsible Entities have ~~multiple~~ multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their ~~and has provided the ability to use~~ high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, ~~the objective criteria within~~ Attachment 1.

Responsible Entities will ~~utilize~~ use their list of assets ~~that~~ containing low impact BES Cyber System(s) (~~that is created~~ developed pursuant to ~~as a result of applying~~ CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there ~~continues to be~~ is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the ~~elements~~ sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the ~~elements~~ sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per ~~element~~ section are located in Attachment 2.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of 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 CIP ~~senior~~ Senior ~~manager~~ Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 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 so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior

Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 1. (R2) OR The Responsible Entity documented	The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-~~6~~7, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-7,	one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) ~~OR~~ ~~The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing~~	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for ~~Low Impact External Routable Connectivity~~LERC, but failed to ~~establish~~ implement a ~~Low Impact Electronic Access Point~~LEAP~~,~~ or permit inbound and outbound access ~~and deny all other access, or other electronic access~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R2, Attachment 1, Section 4. (R2)	~~low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, element 4.~~ (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent	~~controls that provide equal or greater level of protection~~ according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 3. (R2) OR The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-7, Requirement R2, Attachment 1, ~~element~~ Section 3. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical ~~access~~ security controls according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 2. (R2)	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical ~~access~~ security controls according to CIP-003-7, Requirement R2, Attachment 1, ~~element~~ Section 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (R3)	document this change in less than 50 calendar days of the change. (R3)	less than 60 calendar days of the change. (R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-003-~~6~~ 7 - Attachment 1

Required ~~Elements~~ Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the ~~elements~~ sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with ~~multiple~~ multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the ~~elements~~ sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber S~~s~~ecurity ~~awareness~~Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, ~~its~~ cyber security practices (which may include associated physical security practices)~~, using one or a combination of the following methods:~~

- ~~Direct communications (for example, e-mails, memos, computer-based training);~~
- ~~Indirect communications (for example, posters, intranet, or brochures); or~~
- ~~Management support and reinforcement (for example, presentations or meetings).~~

Section 2. Physical ~~access s~~Security ~~controls~~Controls: Each Responsible Entity shall ~~implement controls to restrict~~control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset~~,~~ and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.~~, based on need as determined by the Responsible Entity, through one or more of the following:~~

- ~~Access controls;~~
- ~~Monitoring controls; or~~

~~Other operational, procedural, or technical physical security controls.~~

Section 3. Electronic ~~access~~ Access C~~c~~ontrols: Each Responsible Entity shall ~~implement controls to restrict electronic access for Low Impact External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection~~:

3.1 For ~~any Low Impact External Routable Connectivity~~LERC, if any, ~~establish~~ implement a ~~Low Impact BES Cyber System Electronic Access Point~~ LEAP ~~that~~ to permit~~s~~ only necessary inbound and outbound bi-directional routable protocol access ~~and denies all other access~~; and

~~**3.2** Authentication~~ Implement authentication ~~of~~ for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

~~**3.2**~~

3.2

Section 4. Cyber Security Incident ~~response~~Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents~~.~~;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law~~.~~;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals~~.~~;

4.4 Incident handling for Cyber Security Incidents~~.~~;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident~~.~~; and

~~Record retention related to Reportable Cyber Security Incidents.~~

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-~~6~~ 7 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

~~Element~~ Section 1 - Cyber ~~security~~ Security ~~awareness~~Awareness: An example of evidence for ~~element~~ Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation ~~has been provided~~ through one or more of the following methods: ~~dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.~~

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

~~Element~~ Section 2 - Physical ~~s~~Security ~~c~~Controls: Examples of evidence~~s~~ for ~~element~~ Section 2 may include, but are not limited to:

- Documentation of the selected ~~one or more~~ access control(s) (e.g., card key, ~~special~~ locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls ~~to restrict~~ that control physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    ~~b.~~ The Cyber Asset, if any, containing the ~~Low Impact BES Cyber System Electronic Access Point~~LEAP.
    ~~c.~~b. ~~Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access.~~

~~Element~~ Section 3 - Electronic ~~a~~Access ~~c~~Controls: Examples of evidence for ~~element~~ Section 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections ~~(e.g. IP addresses, ports, services)~~ for any ~~Low Impact BES Cyber System Electronic Access Point~~LEAP are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).~~; or~~
- ~~Documentation of other electronic access controls that provide an equal or greater level of protection.~~

~~Element~~ Section 4 - Cyber Security Incident ~~r~~Response: An example of evidence for ~~element~~ Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed~~;~~ either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security ~~incident~~ Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);
2. ~~the~~ to ~~identification~~ identify and document~~ation of~~ the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and

~~5. to retain records related to Reportable Cyber Security Incidents (e.g., security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).~~

~~6.~~5. to update, as needed, ~~Also include dated revised~~ Cyber Security Incident response plan(s) ~~that identify that the plan(s) were updated~~ within 180 calendar days after ~~a~~ completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, ~~The~~ the number of policies and their ~~specific language~~content ~~are~~ should 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. ~~If a Responsible Entity has any high or medium impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1.1. If a Responsible Entity has any assets from CIP-002 containing low impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the four topical areas required by Requirement R1.2.~~ The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering ~~these~~ the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

~~For~~ Responsible Entities that have ~~multiple~~ multiple-impact rated BES Cyber Systems~~, they~~ are not required to create separate cyber security policies for high~~, or~~ medium~~, and~~ or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-~~004~~ 003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards~~from CIP-004 through CIP-011~~, but ~~rather to put together~~to develop a holistic cyber security policy appropriate ~~to~~ for its organization. ~~The assessment through the Compliance Monitoring and Enforcement Program of~~ Elements of a policy ~~items~~ that extend beyond the scope of ~~CIP-004 through CIP-011~~NERC's cyber security Reliability Standards ~~should~~ will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, ~~T~~the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any~~policy~~:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- 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
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate 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

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- 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

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to 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 Standard Drafting Team (SDT) has removed r~~Requirements relating to exceptions to a Responsible Entity's security policies were removed ~~since~~ because it is a general management issue that is not within the scope of a reliability requirement. ~~The SDT considers i~~It ~~to be~~is an internal policy requirement and not a reliability requirement. However, ~~the SDT encourages~~

Responsible Entities are encouraged to continue this practice as a component of ~~its~~ their cyber security ~~policy~~policies.

In this and all subsequent required approvals in the NERC CIP Reliability 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 R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of ~~all~~ low impact BES Cyber Systems. The ~~SDT is~~ protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES~~balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed~~.~~ The intent is that ~~such~~ the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four ~~main~~ subject matter areas, as ~~detailed~~ identified in Attachment 1, that must be covered by ~~this~~ the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for ~~Low Impact External Routable Connectivity~~LERC and Dial-up Connectivity, and ~~cyber security incident~~(4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the ~~elements~~ sections that must be in the cyber security plan(s). The ~~SDT's~~ intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems ~~and not~~ rather than maintain two separate programs. Guidance for each of the ~~4~~ four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. ~~It is up to t~~The entity ~~as to~~has the discretion to determine the topics to be addressed and ~~how it~~the manner in which it will communicate ~~schedules~~ these topics. ~~The~~ As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered ~~and~~ according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.)~~ that were used~~. The ~~SDT does not intend that the~~ Responsible Entity ~~must~~ is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be ~~used~~ included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something,

say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement ~~controls~~ methods to ~~restrict~~ control physical access to (1) ~~the~~ low impact BES Cyber Systems at ~~a BES~~ assets containing low impact BES Cyber System(s) and (2) ~~Low Impact BES Cyber System Electronic Access Points~~ LEAPs, if any ~~(see Electronic Access Controls section below)~~. If the LEAP is located within the BES asset and inherits the same controls outlined in ~~element~~ Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls. ~~If the LEAP is located at another location, possibly a location without any BES Cyber Systems, then separate documentation and implementation of the physical security controls of the LEAP are required.~~

The Responsible Entity has the flexibility in the ~~controls~~ selection of the methods used to meet the objective to ~~restrict~~ control physical access to the asset(s) containing low impact BES Cyber Systems ~~at a~~or the low impact BES ~~asset~~ Cyber System itself or LEAPs, if any.~~,~~ The Responsible Entity may ~~using~~ use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may ~~utilize~~ use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) ~~and/~~or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although would help meet the security objective.

The objective is to ~~restrict~~ control the physical access based on need ~~and~~ as determined by the Responsible Entity. ~~t~~The need can be ~~established~~ documented at the policy level ~~based on higher level operational or business needs~~ for access to the site or systems. ~~The SDT intent is that this need at the higher level be documented such that the requirement cannot be interpreted to mean that any and all access must be restricted.~~ The requirement does not ~~imply that a~~ obligate an entity to ~~specific~~ specify a ~~business~~ need ~~must be documented~~ for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (~~i~~1) alarm systems to detect motion or entry into a controlled area, or (~~ii~~2) human observation of a controlled area. Monitoring does not necessarily ~~imply~~ require logging and maintaining logs~~,~~ but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level ~~as determined by the entity's controls~~to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber

Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of the communication within its low impact cyber security plan.

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP even though there technically is LERC. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~Where Low Impact External Routable Connectivity (LERC) or Dial-up Connectivity exists, the Responsible Entity must document and implement controls that include the LERC and Dial-up Connectivity to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. Two glossary terms are included in order to help clarify and simplify the language in Attachment 1. The SDT's intent in creating these terms is to avoid confusion with the similar concepts and requirements (ESP, EAP, ERC, EACMS) needed for high and medium impact BES Cyber Systems by utilizing separate terms that apply only to assets containing low impact BES Cyber Systems.~~

~~**Low Impact External Routable Connectivity (LERC) –** includes any bi-directional routable protocol based connectivity between low impact BES Cyber Systems within a BES asset and Cyber Assets outside the BES asset containing the low impact BES Cyber Systems. The SDT, in order to avoid future technology issues, is specifically excluding from the definition direct Intelligent Electronic Device (IED) to IED communication used for protection and/or control between low impact BES Cyber Systems at different BES assets, such as IEC 61850 messaging. The SDT does not intend for the requirement to have an electronic access point even though there is LERC or to preclude the use of such time-sensitive (for example 4 ms or less) reliability enhancing functions if they use a routable protocol in the future.~~

~~**Low Impact BES Cyber System Electronic Access Point (LEAP) –**~~ When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber

System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of~~is~~ the interface on a Cyber Asset that ~~allows and~~ controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based~~a~~ firewall, the internal interface on a router that has implemented an access control list (ACL), or ~~an internal interface on a unidirectional gateway that physically enforces outbound-only data flows~~other security device. ~~LEAP are not to be considered EACMS or meet EACMS specific requirements (as utilized for the Electronic Security Perimeter protecting high and medium impact BES Cyber Systems). However they are required, as per element 2 of the cyber security plan elements, to have physical security controls.~~ The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required ~~is not prescriptive and does not have~~ to reside at the ~~BES~~ asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish~~. This flexibility is included so that the standard does not~~ nor ~~require~~ a unique physical LEAP per ~~BES asset. Responsible Entities can have a single LEAP that controls the LERC from more than one BES~~ asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. ~~However the LERC between assets "behind" the LEAP and another asset containing a low impact BES Cyber System must also pass through the single LEAP.~~ Locating the ~~LEAP~~ Cyber Asset with multiple LEAPs at an external location with multiple ~~BES~~ assets containing low impact BES Cyber Systems "behind" it, however, should not allow ~~unfettered~~ uncontrolled access from one ~~BES~~ asset to all other ~~BES~~ assets sharing the LEAP. ~~It is also not the intent of the SDT where low impact BES Cyber Systems do not have any LERC that additional connectivity be established nor that a LEAP be established.~~

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

~~The electronic access controls should address the risk of using the asset's LERC or Dial-up Connectivity to gain access to the low impact BES Cyber Systems. For LERC, a LEAP shall be~~

~~implemented that permits only necessary inbound and outbound access and denies all other access.~~

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP ~~that denies all traffic by default~~ with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services) ~~for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems~~.
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

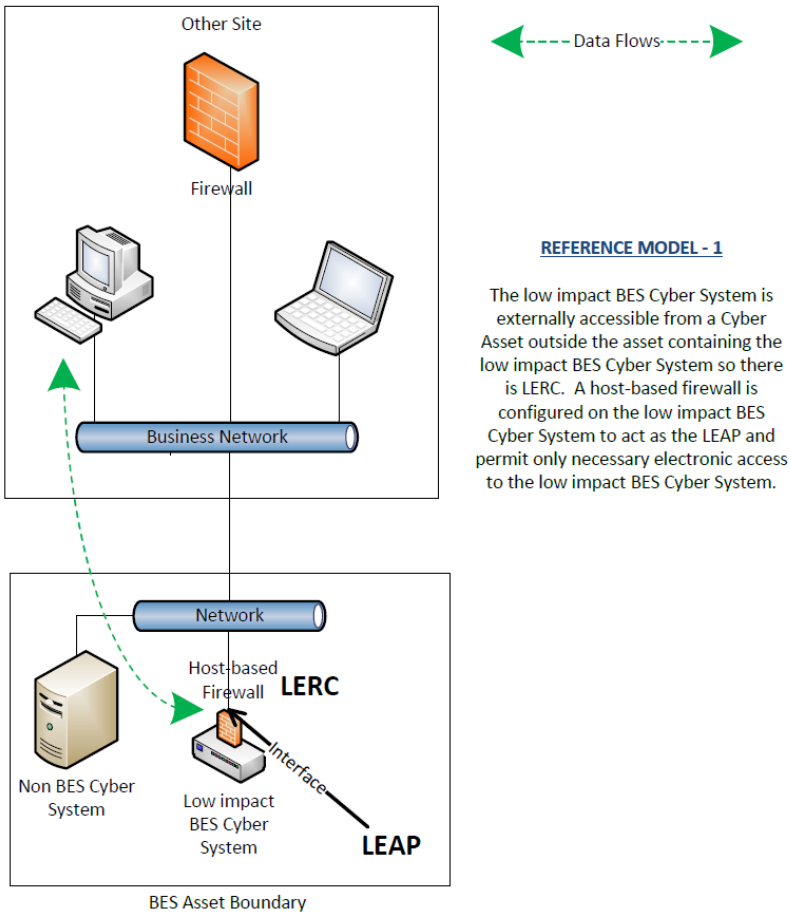
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

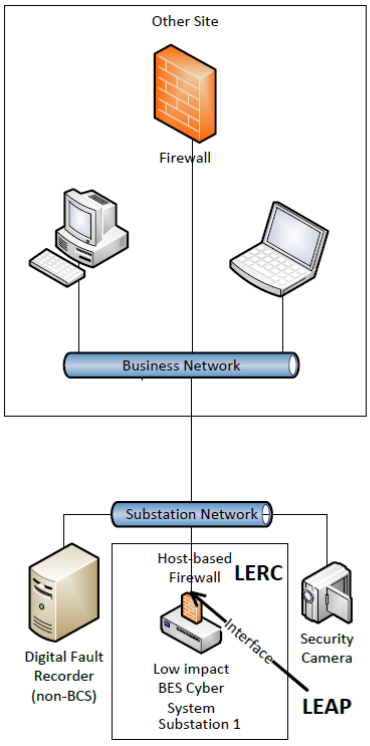
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has ~~external routable connectivity~~LERC due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier ~~which~~ that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would

not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

The following diagrams provide reference examples to depict the rationale for identifying whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.~~The SDT also notes it uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.~~

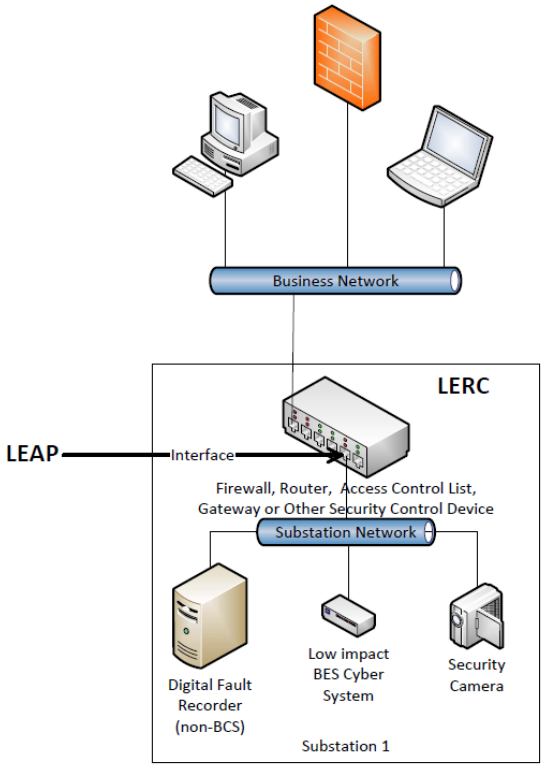
~~The following diagrams explain the SDT's rationale.~~





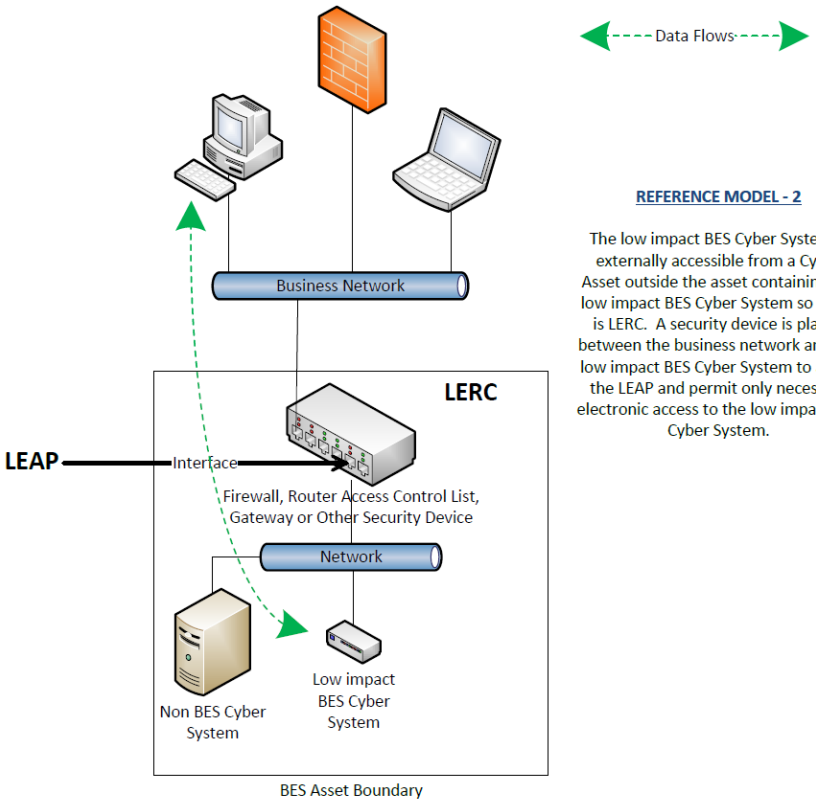
REFERENCE MODEL - 1

The low impact BES Cyber System is behind a LEAP. In this example, the LEAP is the network interface on the low impact BES Cyber System. The host-based firewall restricts electronic access for Low Impact External Routable Connectivity (LERC).



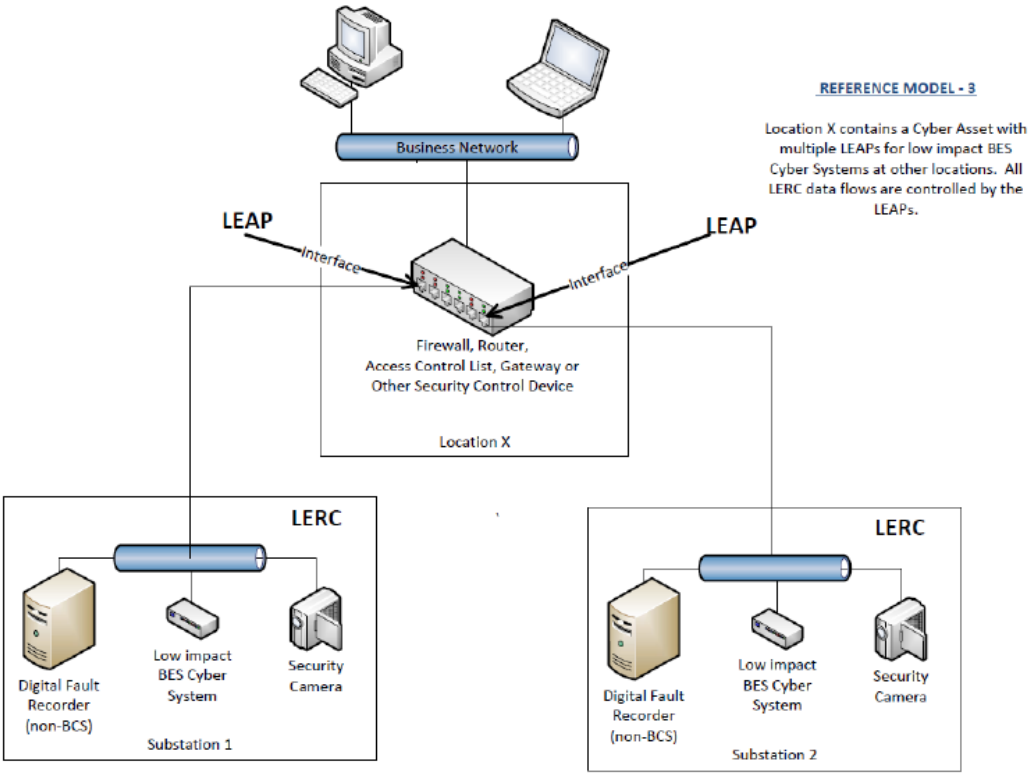
REFERENCE MODEL - 2

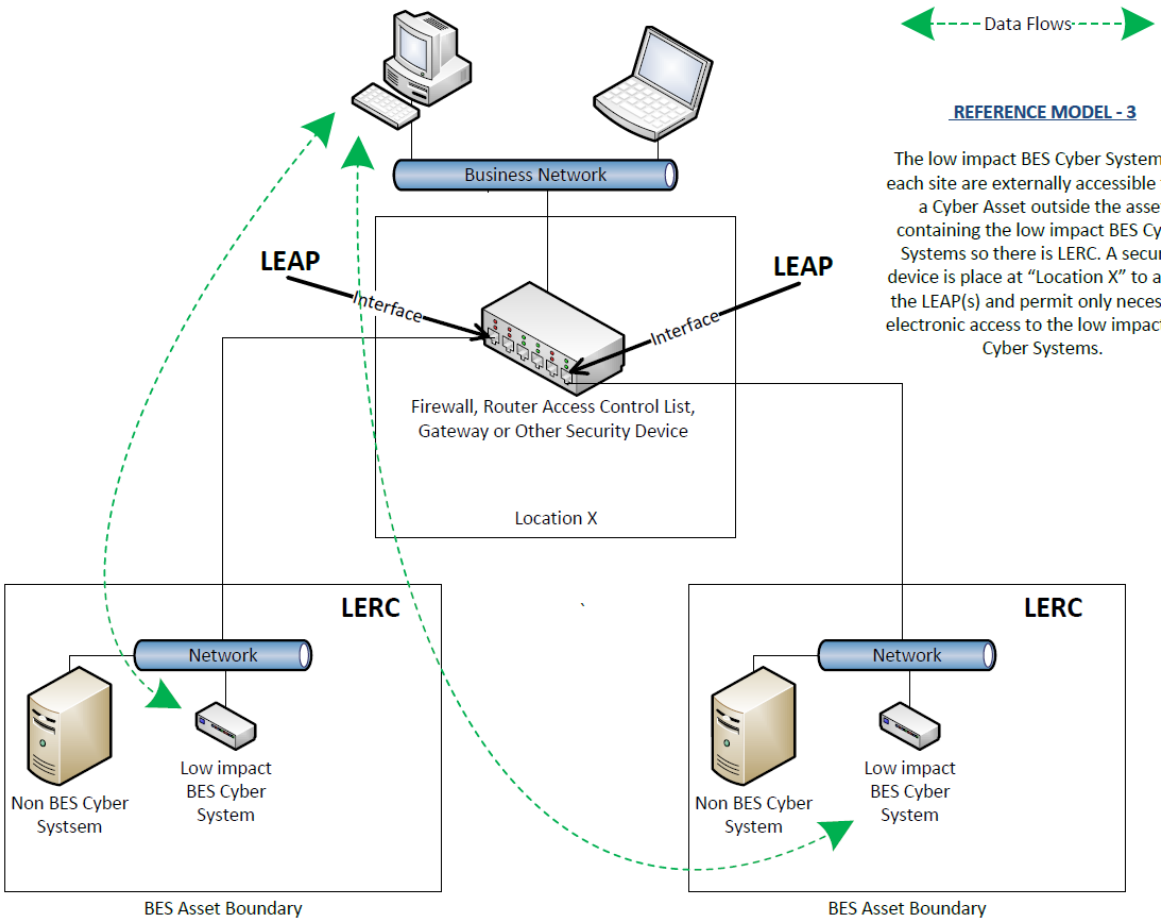
All LERC to the low impact BES Cyber System is controlled by an LEAP.

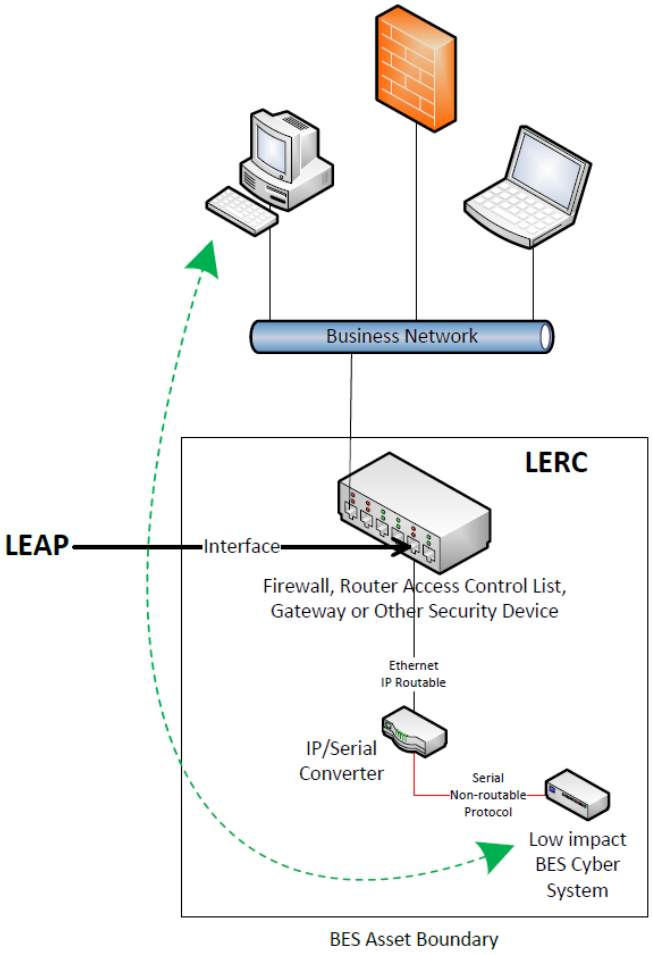


REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.


REFERENCE MODEL - 3
Location X contains a Cyber Asset with multiple LEAPs for low impact BES Cyber Systems at other locations. All LERC data flows are controlled by the LEAPs.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router, Access Control List, Gateway or Other Security Control Device
Location X
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 1
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 2

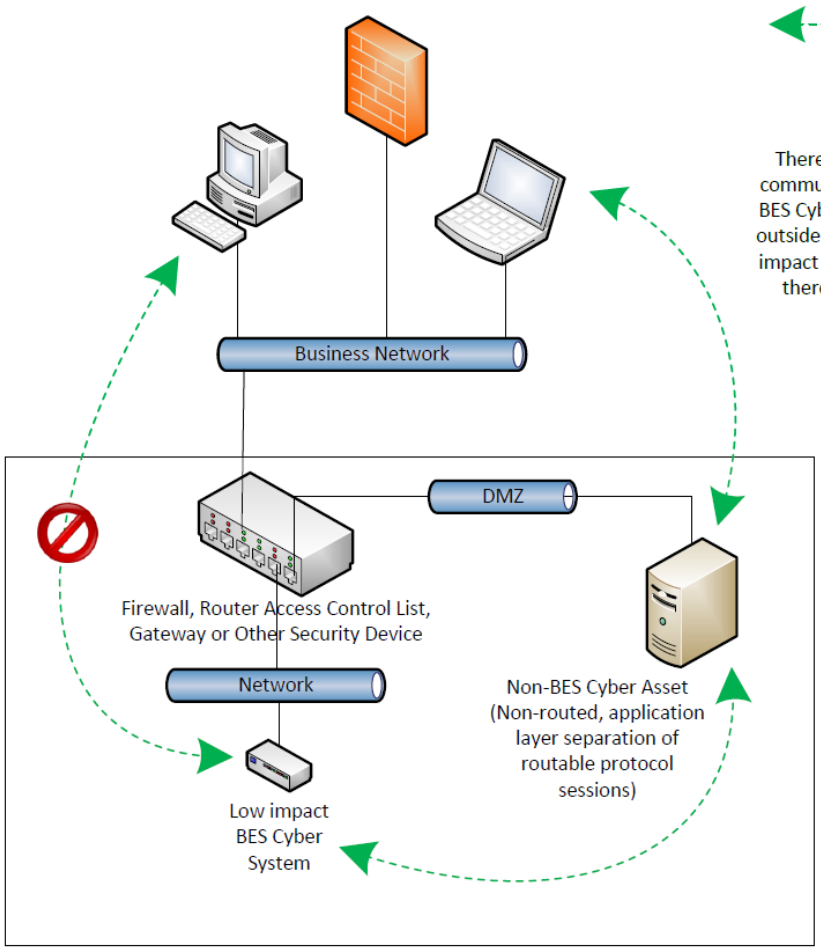

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

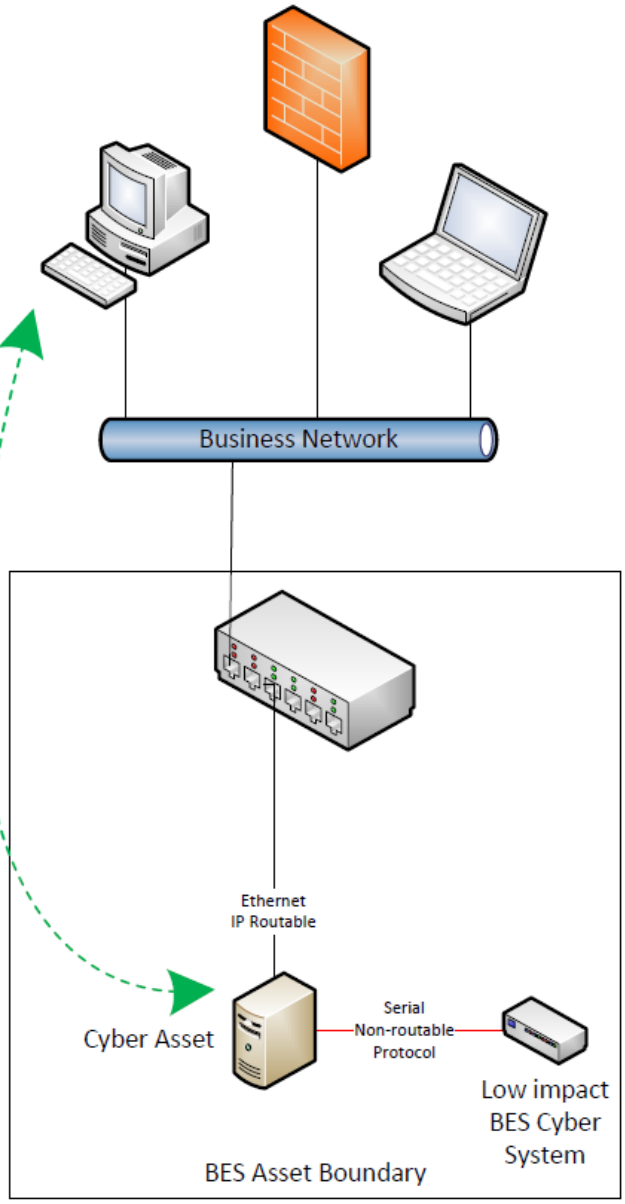


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

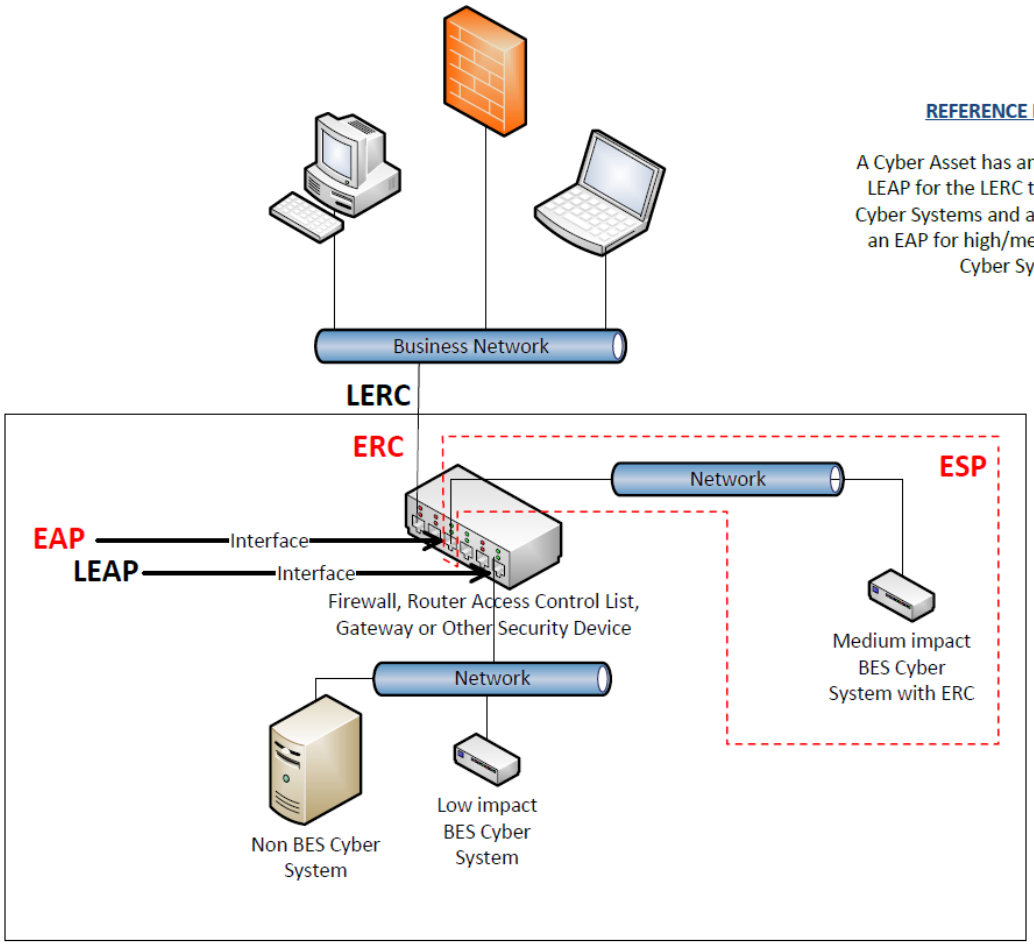

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan(s) that include each of the topics listed in Section 4. ~~For assets that do not have LERC, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is i~~If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement ~~there is~~ a ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan that will guide the entity ~~through~~ in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as ~~well as~~do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise ~~if~~ provided the entity's response plan is followed. ~~It is the intent of the SDT~~The intent of the requirement is for entities to ~~have~~ keep the ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan(s) ~~kept~~ current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

~~In the event of a Reportable Cyber Security Incident, Attachment 1, element 4.6 specifies entities must retain relevant records for Reportable Cyber Security Incidents. Example evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes. Entities should refer to their handling procedures to determine the types of evidence to retain. The evidence retention period for records related to Reportable Cyber Security Incidents is defined in Section C.1.2 of this Standard, which is the same for all requirements in CIP-003-6.~~

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that ~~this~~ the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity ~~should have~~ significant flexibility to adapt this requirement to ~~their~~ its existing organizational structure. A Responsible Entity may satisfy this requirement 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 its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records ~~provides~~ shows 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.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations ~~up~~ up ~~to~~ to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	November 2014
Final Ballot is Conducted	January 2015
Board of Trustees (Board) Adoption	February 2015
Filing to Applicable Regulatory Authorities	February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-004-7

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting 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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-7.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to

provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 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.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 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 requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement 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 covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 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 requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive 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.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity 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 included in the delegations referenced in CIP-003-7. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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-003-7 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 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 access 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 SDT intends that 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – 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-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. 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.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES 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 directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., 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 physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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 (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of 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.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of 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 revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			locations, privileges were incorrect or unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR	termination action. (5.3)	date and time of the termination action. (5.3)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce 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 and evidence, when dated, 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.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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 CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

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, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed 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, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

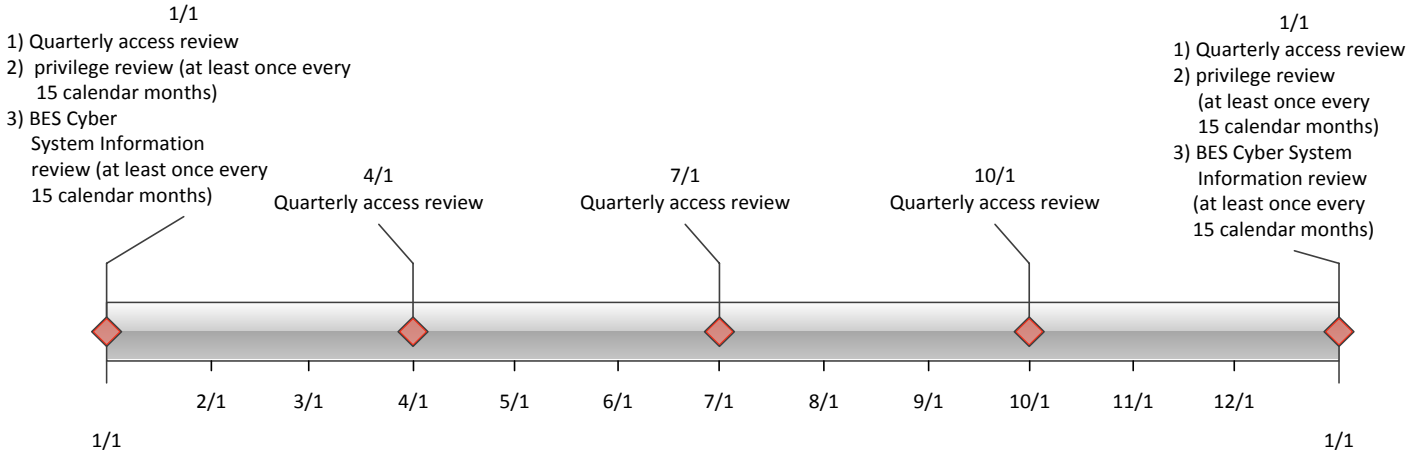
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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 where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. 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 privilege review at least once every 15 calendar months 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 Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

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 scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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 resources 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 resources personnel are notified of the termination and work 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 resources 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	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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 Requirement R5.1 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 (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should 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.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~final~~ an additional comment period and ballot. The draft includes modifications to meet FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	November 2014
Final Ballot is Conducted	~~October 2014~~January 2015
Board of Trustees (Board) Adoption	~~November 2014~~February 2015
Filing to Applicable Regulatory Authorities	~~December 2014~~February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-~~6~~7

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting 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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~6~~7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-~~6~~7.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to

provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 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.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 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 requirement parts in *CIP-004-~~6~~ 7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~ 7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or

CIP-004-~~6~~ 7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement 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 covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~6~~ 7 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 requirement parts in *CIP-004-~~6~~ 7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~ 7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~6~~ 7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive 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.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~6~~ 7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity 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 included in the delegations referenced in CIP-003-~~6~~7. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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-~~6~~ 7 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 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 access 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 SDT intends that 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R4 – 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-~~6~~ 7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~6~~ 7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~6~~ 7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. 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.

CIP-004-~~6~~ 7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES 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 directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., 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 physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System 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 (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~ 7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~ 7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~6~~ 7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~6~~ 7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of 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.

CIP-004-~~6~~ 7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of 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 revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~6~~ 7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its~~one~~ BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its~~two~~ BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its~~two~~ BES Cyber System Information storage locations, privileges were	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~three~~ BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~three~~ BES Cyber System Information storage locations, privileges	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~four or more~~ BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its~~one~~ BES Cyber System Information storage	incorrect or unnecessary. (4.4)	were incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~four or more~~ BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			locations, privileges were incorrect or unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR	termination action. (5.3)	date and time of the termination action. (5.3)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce 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 and evidence, when dated, 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.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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 CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

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, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed 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, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

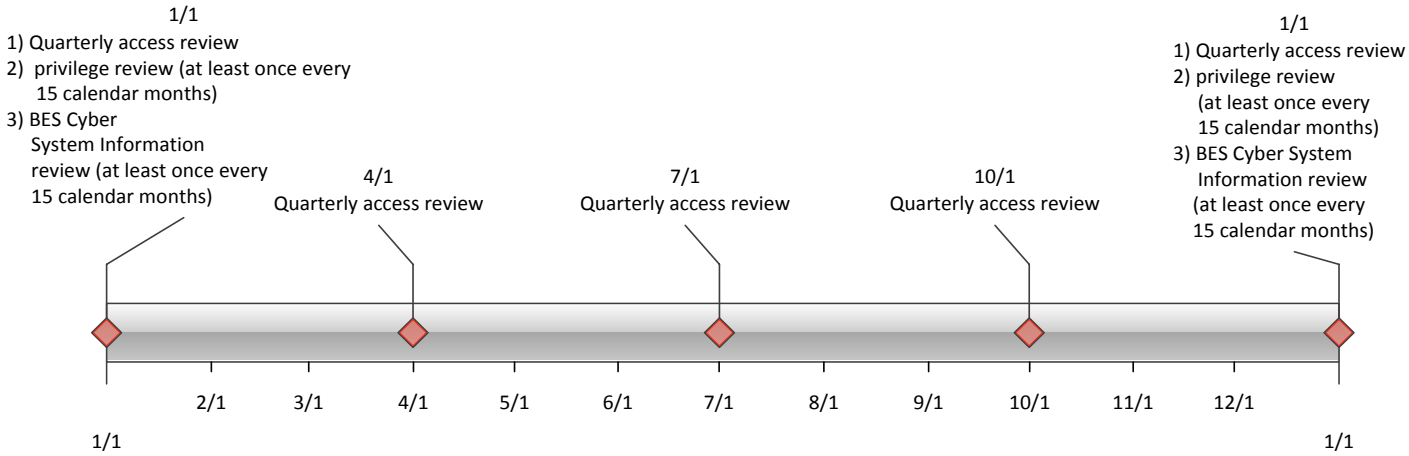
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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 where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. 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 privilege review at least once every 15 calendar months 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 Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this 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 Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

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 scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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 resources 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 resources personnel are notified of the termination and work 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 resources 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	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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 Requirement R5.1 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 (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should 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.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for additional comment period and ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	January 2015
Board of Trustees (Board) Adoption	February 2015
Filing to Applicable Regulatory Authorities	February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-007-7

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-7.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **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.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement 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 services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 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 requirement parts in *CIP-007-7 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement 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.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 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 requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets 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.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 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 requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement 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 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 for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 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 requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) 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. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement 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. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

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.

Rationale for Requirement R5 (continued):

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.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 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 requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-7 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level 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 'needed.'

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 Physical Security Perimeter 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, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

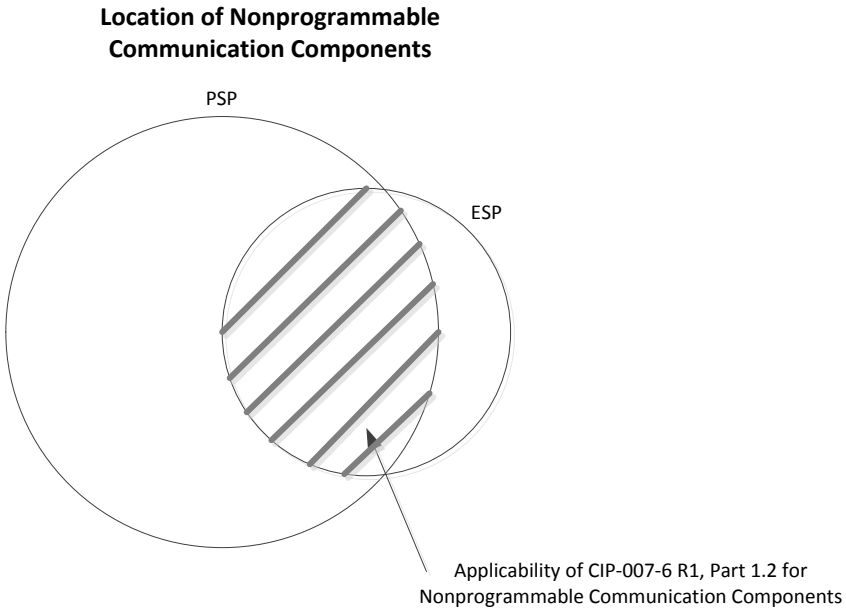
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-7 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement 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; the 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. Standalone 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 lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process 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. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. 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, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. 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. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. 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 requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. 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." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. 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:

3.1. 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 as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets 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 antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-3. The protections required here in CIP-007-7, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. 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 ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 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 of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. 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
- Failure of security event logging mechanisms
- 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 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately 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 Database.
- 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.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic 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 and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. 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. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

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.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for additional comment period and ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	November 2014
Final Ballot is Conducted	~~October 2014~~January 2015
Board of Trustees (Board) Adoption	~~November 2014~~February 2015
Filing to Applicable Regulatory Authorities	~~December 2014~~February 2015

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 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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	

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-~~6~~7

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting ~~Bulk Electric System (~~BES~~)~~ Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~6~~7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-~~6~~7.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **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.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement 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 services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 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 requirement parts in *CIP-007-~~6~~ 7 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ 7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~6~~ 7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement 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.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 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 requirement parts in *CIP-007-~~6~~ 7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ 7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~6~~ 7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~ 7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~6~~ 7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets 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.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 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 requirement parts in *CIP-007-~~6~~ 7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ 7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~6~~ 7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement 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 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 for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 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 requirement parts in *CIP-007-~~6~~ 7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ 7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) 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. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~ 7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement 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. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

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.

Rationale for Requirement R5 (continued):

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.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 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 requirement parts in *CIP-007-~~6~~ 7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ 7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or	CIP-007-~~6~~ 7 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ 7 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level 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 'needed.'

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 Physical Security Perimeter 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, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

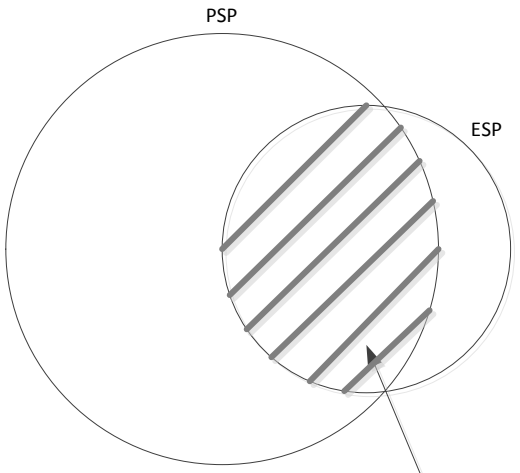
- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-~~6~~ 7 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement 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; the 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. Standalone 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 lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process 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. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. 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, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. 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. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. 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 requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. 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." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. 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:

3.1. 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 as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets 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 antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-3. The protections required here in CIP-007-7, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. 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 ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 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 of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. 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
- Failure of security event logging mechanisms
- 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~~ Removable ~~media~~ Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately 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 Database.
- 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.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic 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 and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. 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. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

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.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period and Ballot	November 2014
Final Ballot is Conducted	January 2015
Board of Trustees (Board) Adoption	February 2015
Filing to Applicable Regulatory Authorities	February 2015

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	

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 Change Management and Vulnerability Assessments

2. Number: CIP-010-3

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-3:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-010-3.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement 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 process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 4. EACMS; 5. PACS; and 6. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, 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.	An example of evidence may include, but is not limited to, a list of cyber 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.

Rationale for Requirement 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 process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [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 requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: **Section 1.** EACMS; and **Section 2.** PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, 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.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), 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.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 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 any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, 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).

Rationale for R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-3 and CIP-007-7 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

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

b. 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented 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,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented 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,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	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. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4,	authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3,	Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	Attachment 1, Sections 1.3 and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1 and 2.2. (R4)	Requirement R4, Attachment 1, Sections 1.3 and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Sections 2.1 and 2.2. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-7. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-7 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) 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, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) 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 BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, 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:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify 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.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;

- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device

cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4,Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks, and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to

prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period and Ballot	September November 2014
Final Ballot is Conducted	October/November 2014January 2015
Board of Trustees (Board) Adoption	November 2014February 2015
Filing to Applicable Regulatory Authorities	December 2014February 2015

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
~~2~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~
2	11/13/14	Adopted by the NERC Board of Trustees.	

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 Change Management and Vulnerability Assessments

2. Number: CIP-010-~~2~~3

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-~~2~~3:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.~~See Implementation Plan for CIP-010-3.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, ~~etc~~etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement 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 process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~ 3 -Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~2~~ 3 -Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~ 3 -Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~2~~ 3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 4. EACMS; 5. PACS; and 6. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~2~~ 3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~2~~ 3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, 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.	An example of evidence may include, but is not limited to, a list of cyber 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.

Rationale for Requirement 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 process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~ 3 -Table R2 – Configuration Monitoring. [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 requirement parts in *CIP-010-~~2~~ 3 -Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~ 3 -Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: **Section 1.** EACMS; and **Section 2.** PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~ 3 -Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~2~~ 3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~ 3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment~~,~~; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~2~~ 3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, 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.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), 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.

CIP-010-~~2~~ 3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 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 any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, 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).

Rationale for R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with ~~tools~~ Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, ~~the~~ Requirement R4 ~~is a new requirement~~was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-~~1~~ 3 and CIP-007-~~5~~7 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: ~~This is a new requirement.~~ All requirements related to Transient ~~Devices~~ Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the ~~elements~~ sections in Attachment 1~~, except under CIP Exceptional Circumstances~~. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable ~~elements~~ sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per ~~element~~ section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

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

b. 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented 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,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented 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,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	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. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media ~~elements~~ sections according to CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~element~~ Section 3. (R4) OR	implement the Removable Media ~~elements~~ sections according to CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~element~~ Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of ~~security~~ software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets ~~Owned or Managed~~ managed by the Responsible Entity according to	authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of ~~security~~ software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets ~~Owned or Managed~~ managed by the Responsible Entity according to	Removable Media according to CIP-010-~~2~~3, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets ~~Owned or Managed~~ managed by the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~element~~ Section 1.~~1~~2. (R4)	CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~elements~~ Sections ~~1.2,~~ 1.3~~,~~ and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of ~~security~~ software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets ~~Owned or Managed~~ managed by ~~Vendors or Contractors~~a party other than the Responsible Entity according to CIP-010-	CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~elements~~ Sections ~~1.2,~~ 1.3~~,~~ and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of ~~security~~ software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets ~~Owned or Managed~~ managed by ~~Vendors or Contractors~~a party other than the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~2~~3, Requirement R4, Attachment 1, ~~elements~~ Sections 2.1 and 2.2. (R4)	Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1, ~~elements~~ Sections 2.1 and 2.2. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-010-~~2~~ 3 - Attachment 1

Required ~~Elements~~ Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the ~~elements~~ sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) ~~Owned or~~ Managed by the Responsible Entity.

1.1. Transient Cyber Asset ~~management~~Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset ~~authorization~~Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall ~~specify~~authorize:

1.2.1. ~~Authorized users~~Users, either individually or by group or role;

1.2.2. ~~Authorized locations~~Locations, either individually or by group; and

1.2.3. ~~Authorized uses~~Uses, which shall be limited to what is necessary to perform business functions.

1.3. ~~Security~~ Software ~~vulnerability~~ Vulnerability ~~mitigation~~Mitigation: Use one or a combination of the following methods to achieve the objective of ~~To mitigate~~ mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset ~~security vulnerabilities~~ (per Transient Cyber Asset capability)~~, each Responsible Entity shall use one or a combination of the following methods~~:

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate ~~security~~ software vulnerabilities.

1.4. Introduction of ~~malicious~~ Malicious ~~code~~ Code ~~mitigation~~Mitigation: Use one or a combination of the following methods to achieve the objective of ~~To mitigate~~ mitigating the introduction of malicious code (per Transient Cyber Asset capability)~~, each Responsible Entity shall use one or a combination of the following methods~~:

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or

- ~~Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected; or~~
- Other method(s) to mitigate the introduction of malicious code.

1.5. ~~Risk of unauthorized~~ Unauthorized ~~use~~ Use ~~mitigation~~Mitigation: Use one or a combination of the following methods to achieve the objective of ~~To mitigate~~ mitigating the risk of unauthorized use of Transient Cyber Asset(s)~~, each Responsible Entity shall use one or a combination of the following methods~~:

- ~~Transient Cyber Asset resides within a location with restricted~~ Restrict physical access;
- Full-disk encryption with authentication;
- ~~Multi-factor authentication;~~
- ~~Theft recovery tools;~~ or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) ~~Owned or~~ Managed by ~~Vendors or Contractors~~ a Party Other than the Responsible Entity.

2.1 ~~Security~~ Software ~~vulnerability~~ Vulnerabilities ~~mitigation~~Mitigation: Use one or a combination of the following methods to achieve the objective of ~~To mitigate~~ mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset ~~security vulnerabilities~~ (per Transient Cyber Asset capability)~~, each Responsible Entity shall use one or a combination of the following methods~~:

- Review of installed security patch(es);
- Review of security patching process used by the ~~vendor or contractor~~party~~, other than the Responsible Entity, managing the Transient Cyber Asset(s)~~;
- Review of other vulnerability mitigation performed by the ~~vendor or contractor~~party~~, other than the Responsible Entity, managing the Transient Cyber Asset(s)~~; or
- Other method(s) to mitigate ~~security~~ software vulnerabilities.

2.2 Introduction of m~~M~~alicious code mitigation: Use one or a combination of the following methods to achieve the objective of ~~To mitigate~~ mitigating malicious code (per Transient Cyber Asset capability)~~, each Responsible Entity shall use one or a combination of the following methods~~:

- Review of antivirus update level;
- Review of antivirus update process used by the party~~vendor or contractor~~;
- Review of application whitelisting used by the party~~vendor or contractor~~;

- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party~~vendor or contractor~~; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate ~~security~~ software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary~~,~~ and implement such actions prior to connecting the ~~vendor- or contractor-owned~~ Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media ~~authorization~~Authorization: For each individual or group of Removable Media, each Responsible Entity shall ~~specify~~authorize:

3.1.1. ~~Authorized users~~Users, either individually or by group or role; and

3.1.2. ~~Authorized locations~~Locations, either individually or by group.

3.2. Malicious ~~code~~ Code ~~mitigation~~Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

~~**3.1.3.**~~**3.2.2.** Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~To mitigate malicious code, each Responsible Entity shall scan Removable Media outside of the BES Cyber System~~.

CIP-010-~~2~~ 3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

~~Element~~ Section 1.1: Examples of evidence for ~~element~~ Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) ~~Owned or Managed~~ managed by the Responsible Entity or part of a security policy.

~~Element~~ Section 1.2: Examples of evidence for ~~element~~ Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show~~s~~ authorization of Transient Cyber Asset(s) ~~Owned or Managed~~ managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document. ~~The documentation must identify the Transient Cyber Asset, individually or by group of Transient Cyber Asset(s) along with the authorized users, either individually or by group or role, the authorized locations, either individually or by group and the authorized uses associated with what is necessary to perform business functions.~~

~~Element~~ Section 1.3: ~~____~~ Examples of evidence for ~~element~~ Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate ~~security~~ software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the ~~security~~ software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability. ~~If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.~~

~~Element~~ Section 1.4: Examples of evidence for ~~element~~ Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the

Transient Cyber Asset does not have the capability. ~~If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.~~

~~Element~~ Section 1.5: Examples of evidence for ~~element~~ Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; ~~method(s) of the theft recovery tools;~~ or documentation of other method(s) to mitigate the risk of unauthorized use. ~~If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.~~

~~Element~~ Section 2.1: Examples of evidence for ~~element~~ Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); ~~memorandums~~memoranda, electronic mail, policies or contracts from ~~vendors or contractors~~parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the ~~vendor or contractor~~party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity ~~of~~ that the ~~vendor or contractor~~ practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate ~~security~~ software vulnerabilities for Transient Cyber Asset(s) ~~Owned of Managed~~ managed by ~~Vendors or Contractors~~a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability. ~~If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.~~

~~Element~~ Section 2.2: Examples of evidence for ~~element~~ Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed ~~the~~ antivirus update level; ~~memorandums~~memoranda, electronic mail, system documentation, policies or contracts from ~~vendors or contractors~~the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the ~~vendor or contractor~~party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance ~~by the Responsible Entity of~~ that the practices of the party other than the Responsible Entity ~~vendor or contractor practices~~ are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) ~~Owned or Managed~~ managed by ~~Vendors or Contractors~~a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability. ~~If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.~~

~~Element~~ Section 2.3: Examples of evidence for ~~element~~ Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~vendor or contractor owned~~ Transient Cyber Asset managed by a party other than the Responsible Entity.

~~Element~~ Section 3.1: Examples of evidence for ~~element~~ Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

~~Element~~ Section 3.2: Examples of evidence for ~~element~~ Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.~~documentation of the method(s) used to mitigate malicious code such as results of scans of the media, or documented confirmation by the entity that the media was deemed to be free of malicious code. Confirmation can be documented through email or within change management record(s).~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~6~~7. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~6~~ 7 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) 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, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) 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 BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, 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:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify 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.

Requirement R4:

~~Most~~ Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks~~. Because of this~~, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas ~~that are needed~~ to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. ~~These assets~~Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;

- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, ~~element~~ Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application~~s~~ of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. ~~These are broken down as follows:~~

~~Transient Cyber Asset(s) Owned or Managed by the Responsible Entity~~

~~Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors~~

~~Removable Media~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to perform the security functions that the system is capable of doing. The use of this phrase is to eliminate the need for a technical feasibility exception when it is understood that the device cannot perform a function. Using the example of malicious code, many types of appliances are not capable of implementing antivirus software and therefore the software would not be required since it is not a capability of the device.~~

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the ~~device~~Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement ~~4~~ R4, Attachment 1, Section 1 - Transient Cyber Asset(s) ~~Owned or~~ Managed by the Responsible Entity

~~Element~~ Section 1.1: Entities have a high level of control for the assets that they ~~own or~~ manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

~~Element~~ Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct ~~ownership or~~ management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks, and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and ~~wires~~ wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about

authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g.~~,~~ wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e.~~,~~ high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP ~~Requirements~~requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

~~Element~~ Section 1.3: Entities are to document and implement their process(es) to mitigate ~~security~~ software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in ~~security~~ software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how ~~their~~ its Transient Cyber Asset(s) will be used. It is possible for an entity to have ~~their~~ its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike~~,~~ CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom~~er~~ live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate ~~security~~ software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the ~~security~~ software vulnerability mitigation objective.

~~Element~~ Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage ~~their~~ Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, ~~it is possible that~~ entities ~~can~~ may choose ~~for devices that do not regularly connect to receive scheduled updates,~~ to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset ~~of~~ or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

~~Element~~ Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks ~~of~~ that unauthorized use ~~to~~ of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- ~~Transient Cyber Asset resides within a location with r~~For restricted physical access~~.~~, t~~T~~he intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect ~~manages unauthorized physical access to~~ the ~~device~~Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be ~~used~~ employed to protect a Transient Cyber Asset from unauthorized ~~physical access~~use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents ~~anything~~ data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain ~~T~~theft recovery ~~tools~~ solutions ~~that~~ can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and ~~or~~ lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset.~~s~~ Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use~~.if they are stolen or lost~~.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) ~~Owned or~~ Managed by ~~Vendors or Contractors~~a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are ~~owned or~~ managed by ~~vendors or contractors~~parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not ~~own or~~ manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties ~~vendors and contractors~~ to provide support services to BES Cyber Systems and BES

Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department ~~Of~~ of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] ~~Elements from the p~~Procurement language may unify ~~vendor~~ the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP p~~P~~rogram ~~elements~~ attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the ~~vendor's~~ other party's support. Entities should consider ~~the elements of~~ the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

~~Element~~ Section 2.1: Entities are to document and implement their process(es) to mitigate ~~security~~ software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the ~~vendor or contractor managed~~ Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of ~~security~~ software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the ~~vendor or contractor~~other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of ~~security~~ software vulnerabilities to applicable systems.
- Conduct a review of other processes that the ~~vendor or contactor~~other party uses to mitigate the risk of ~~security~~ software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate ~~security~~ software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of ~~security~~ software vulnerabilities.

~~Element~~ Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the antivirus or endpoint security processes of the ~~vendor or contactor~~other party to ensure that their processes are adequate to the Responsible Entity to ~~reduce~~ mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the ~~vendor or contactor~~other party to ~~reduce~~ mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the ~~vendor or contactor~~other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

~~Element~~ Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the ~~vendor or contractor owned~~ Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this ~~element~~ section is to ensure that after conducting the selected review from ~~elements~~ Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible ~~Entities~~ Entity's security posture, the ~~vendor or contactor~~other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

~~Element~~ Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether ~~These~~ these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

~~Element~~ Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on ~~scanning~~ the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it~~The scanning~~ is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious

code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	November 2014
Final Ballot is Conducted	January 2015
Board of Trustees (Board) Adoption	February 2015
Filing to Applicable Regulatory Authorities	February 2015

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	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.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	

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-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-3.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset 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 requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement 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. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that 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, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four 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 or other media, 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 that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~final~~ an additional comment period and ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	November 2014
Final Ballot is Conducted	~~October 2014~~January 2015
Board of Trustees (Board) Adoption	~~November 2014~~February 2015
Filing to Applicable Regulatory Authorities	~~December 2014~~February 2015

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	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.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	

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-~~2~~3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~2~~3:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-~~2~~3.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it 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.

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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~2~~ 3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~2~~ 3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~ 3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~2~~ 3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~ 3 Table R2 – BES Cyber Asset 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 requirement parts in *CIP-011-~~2~~ 3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~ 3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~2~~ 3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~ 3 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement 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. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that 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, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the ~~responsible~~ Responsible ~~entity~~ Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four 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 or other media, 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 that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791
November 25, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-7, Requirements R2 and R4; CIP-004-7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-3, Requirements R1 and R2; and CIP-011-3, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-7 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria

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

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	surrounding the controls for some entities based on asset-type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-7, Requirements R1 and R2 to the following areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The cyber security plan must cover the 4 areas as specified in Attachment 1 of CIP-003-7: a. **Cyber Security Awareness:** Attachment 1, Section 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. b. **Physical Security Controls:** Attachment 1, Section 2 and its subparts require physical access controls to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in Section 3. c. **Electronic Access Controls:** Attachment 1, Section 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. d. **Cyber Security Incident Response:** Attachment 1, Section 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Asset(s) managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		more specific and recognize the relatively higher frequency in which these devices will be used. In the scenario in which a party other than the Responsible Entity manages the Transient Cyber Assets, the required sections of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code. The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security section is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-3 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by user(s), location(s) and use prior to connecting them to the BES Cyber System. Transient Cyber Assets managed by another party do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		2. Software authorization: The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. **3. Security patch management:** In CIP-010-3 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-3 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-3 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-3 to protect and securely handle BES Cyber System Information. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. high, medium, low impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-3 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-3 Requirement R4.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-7 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." However, the scope of the requirements modifications as well as the existing requirements has more targeted components than the broad concept of

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		communication networks. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards. The decision to meet the directive without defining the term communication networks does not imply the absence of protection for communication networks components nor do the additional requirements associated with nonprogrammable components denote meaning to the term. Communication networking components associated with BES Cyber Systems and within an Electronic Security Perimeter have the same level of protection applied as the BES Cyber Assets themselves. Additionally, CIP-005-5 communication protections continue to apply at the Electronic Security Perimeter. The drafting team did not find an additional Glossary term useful in the currently applied communication networks protection.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by	NERC modified the VRF assignment for CIP-006-6, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	NERC modified the VRF assignment for CIP-004-7, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained sections. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-7, Requirements R2 and R4; CIP-004-7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-3, Requirements R1 and R2; and CIP-011-3, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-7, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-7, Requirement R4**. This standard includes requirements for personnel

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-6, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791

~~September 3, 2014~~November 25, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-~~6~~7, Requirements R2 and R4; CIP-004-~~6~~7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-~~6~~7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-~~2~~3, Requirements R1 and R2; and CIP-011-~~2~~3, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-~~6~~ 7 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria

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

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	surrounding the controls for some entities based on asset-type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-~~6~~7, Requirements R1 and R2 to the following areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The cyber security plan must cover the 4 areas as specified in Attachment 1 of CIP-003-~~6~~7: a. **Cyber Security Awareness:** Attachment 1, ~~element~~Section 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. b. **Physical Security Controls:** Attachment 1, ~~element~~Section 2 and its subparts require ~~controls to restrict~~ physical access controls to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in ~~element~~Section 3. c. **Electronic Access Controls:** Attachment 1, ~~element~~Section 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. d. **Cyber Security Incident Response:** Attachment 1, ~~element~~Section 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets ~~owned or~~ managed by the Responsible Entity, (ii) Transient Cyber Asset(s) ~~owned or~~ managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets ~~owned or~~ managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		controls for this scenario are more specific and recognize the relatively higher frequency in which these devices will be used. In the scenario in which ~~contractors or vendors~~a party other than the Responsible Entity manages the Transient Cyber Assets, the required ~~element~~sections of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code. The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security ~~element~~section is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-~~2~~ 3 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by user~~individual~~(s)~~, and~~ location(s) and use prior to connecting them to the BES Cyber System. ~~Vendor or contractor~~Transient Cyber Assets managed by another party~~Transient Cyber Assets~~ do not

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection. **2. Software authorization:** The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. **3. Security patch management:** In CIP-010-~~2~~ 3 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-~~2~~ 3 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-~~2~~ 3 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-~~2~~ 3 to protect and securely handle BES Cyber System Information. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. ~~High~~high, ~~Medium~~medium, ~~Low~~ low ~~Impact~~impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-~~2~~ 3

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-~~2~~ 3 Requirement R4.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-~~6~~ 7 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		is "Information system(s) implemented with a collection of interconnected components." However, the scope of ~~The~~ the requirements modifications as well as the existing requirements has~~ve~~ more targeted components than the broad concept of communication networks. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards. The decision to meet the directive without defining the term communication networks does not imply the absence of protection for communication networks components nor do the additional requirements associated with nonprogrammable components denote meaning to the term. Communication networking components associated with BES Cyber Systems and within an Electronic Security Perimeter have the same level of protection applied as the BES Cyber Assets themselves. Additionally, CIP-005-5 communication protections continue to apply at the Electronic Security Perimeter. The drafting team did not find an additional Glossary term useful in the currently applied communication networks protection.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to	NERC modified the VRF assignment for CIP-006-~~5~~6, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment	NERC modified the VRF assignment for CIP-004-~~5.1~~7, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained ~~element~~sections. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-~~6~~7, Requirements R2 and R4; CIP-004-~~6~~7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-~~6~~7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-~~2~~3, Requirements R1 and R2; and CIP-011-~~2~~3, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-~~5~~7, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-~~5.1~~7, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-~~5~~6, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		timeframe contained in the VSLs from 90-210 days to 90-120 days.

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. 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 standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. 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 standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls~~allows~~ Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems. ~~The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.~~

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a~~Bi-directional routable communications between~~ low impact BES Cyber System(s) ~~and~~ from a Cyber Asset~~s~~ outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. ~~Communication protocols created for~~ Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-~~-~~sensitive protection or control functions between Transmission station or substation ~~Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from~~ assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. 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 standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

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

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Removable Media: Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset: A Cyber Asset that is (i) capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. 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 standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

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

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Removable Media: Storage ~~Media~~media~~,~~ that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less~~, capable of transmitting executable code to:~~ to ~~(1)~~ a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a Protected Cyber Asset ~~that can be used to store, copy, move, or access data~~. ~~Removable Media are not Cyber Assets.~~ Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset: A Cyber Asset~~,~~ that is (i) capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is ~~(e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication)~~ directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less~~, capable of transmitting executable code to: (1)~~ to a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a ~~Protected Cyber Asset~~PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-7, CIP-004-7, CIP-006-6, CIP-007-7, CIP-009-6, CIP-010-3, and CIP-011-3 (CIP-002-5.1, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-7 R1	To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
NEW	CIP-003-7 R1.1	"For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003-7 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-7.
CIP-003-5 R1.2	CIP-003-7 R1.1.2	No change.
CIP-003-5 R1.3	CIP-003-7 R1.1.3	No change.
CIP-003-5 R1.4	CIP-003-7 R1.1.4	No change.
CIP-003-5 R1.5	CIP-003-7 R1.1.5	No change.
CIP-003-5 R1.6	CIP-003-7 R1.1.6	No change.
CIP-003-5 R1.7	CIP-003-7 R1.1.7	No change.
CIP-003-5 R1.8	CIP-003-7 R1.1.8	No change.
CIP-003-5 R1.9	CIP-003-7 R1.1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-7 R1.2	"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003-7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1."
CIP-003-5 R2.1	CIP-003-7 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-7, Requirement R1, Part 1.2.1.
CIP-003-5 R2.2	CIP-003-7 R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-7, Requirement R1, Part 1.2.2.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-7 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-7, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity."
CIP-003-5 R2.4	CIP-003-7 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-7, Requirement R1, Part 1.2.4.
NEW	CIP-003-7, Attachment 1	CIP-003-7 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003-7 R3	No change.
CIP-003-5 R4	CIP-003-7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-7 R1	No change.
CIP-004-5.1 R1.1	CIP-004-7 R1.1	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2	CIP-004-7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement “a cyber security training program(s).” That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-7 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-7 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-7 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-7 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-7 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-7 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-7 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-7 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-7 R2.1.8	No change.
CIP-004-5.1 R2.1.9	CIP-004-7 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity’s cyber security training program. The training must address cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-7 R2.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.3	CIP-004-7 R2.3	No change.
CIP-004-5.1 R3	CIP-004-7 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-7 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-7 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-7 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-7 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-7 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-7 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-7 R3.5	No change.
CIP-004-5.1 R4	CIP-004-7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-7 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-7 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-7 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-7 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-7 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-7 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-7 R4.4	No change.
CIP-004-5.1 R5	CIP-004-7 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R5.1	CIP-004-7 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-7 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-7 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-7 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-7 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-7 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-7 R1.1	No change.
CIP-007-5 R1.2	CIP-007-7 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-7 R2.1	No change.
CIP-007-5 R2.2	CIP-007-7 R2.2	No change.
CIP-007-5 R2.3	CIP-007-7 R2.3	No change.
CIP-007-5 R2.4	CIP-007-7 R2.4	No change.
CIP-007-5 R3	CIP-007-7 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-7 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-7 R3.2	No change.
CIP-007-5 R3.3	CIP-007-7 R3.3	No change.
CIP-007-5 R4	CIP-007-7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-7 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-7 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-7 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-7 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-7 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-7 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-7 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-7 R4.3	No change.
CIP-007-5 R4.4	CIP-007-7 R4.4	No change.
CIP-007-5 R5	CIP-007-7 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-7 R5.2	No change.
CIP-007-5 R5.3	CIP-007-7 R5.3	No change.
CIP-007-5 R4	CIP-007-7 R4	No change.
CIP-007-5 R5	CIP-007-7 R5	No change.
CIP-007-5 R5.1	CIP-007-7 R5.1	No change.
CIP-007-5 R5.2	CIP-007-7 R5.2	No change.
CIP-007-5 R5.3	CIP-007-7 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-7 R5.4	No change.
CIP-007-5 R5.5	CIP-007-7 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-7 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-7 R5.5.2	No change.
CIP-007-5 R6	CIP-007-7 R6	No change.
CIP-007-5 R7	CIP-007-7 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-3 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-3 R1.1	No change.
CIP-010-1 R1.2	CIP-010-3 R1.2	No change.
CIP-010-1 R1.3	CIP-010-3 R1.3	No change.
CIP-010-1 R1.4	CIP-010-3 R1.4	No change.
CIP-010-1 R1.5	CIP-010-3 R1.5	No change.
CIP-010-1 R1.2	CIP-010-3 R1.2	No change.
CIP-010-1 R1.3	CIP-010-3 R1.3	No change.
CIP-010-1 R1.4	CIP-010-3 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-3 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-3 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-3 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-3 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-3 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-3 R1.5.2	No change.
CIP-010-1 R2	CIP-010-3 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-3 R2.1	No change.
CIP-010-1 R3	CIP-010-3 R3	No change.
CIP-010-1 R3.1	CIP-010-3 R3.1	No change.
CIP-010-1 R3.2	CIP-010-3 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-3 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-3 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-3 R3.3	No change.
CIP-010-1 R3.4	CIP-010-3 R3.4	No change.
NEW	CIP-010-3 R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."
NEW	CIP-010-3, Attachment 1	CIP-010-3 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-3 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-3 R1.1	No change.
CIP-011-1 R1.2	CIP-011-3 R1.2	No change.
CIP-011-1 R2	CIP-011-3 R2	No change.
CIP-011-1 R2.1	CIP-011-3 R2.1	No change.
CIP-011-1 R2.2	CIP-011-3 R2.2	No change.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-~~6~~7, CIP-004-~~6~~7, CIP-006-6, CIP-007-~~6~~7, CIP-009-6, CIP-010-~~2~~3, and CIP-011-~~2~~ 3 (CIP-002-5.1, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-~~6~~ 7 R1	To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
NEW	CIP-003-~~6~~ 7 R1.1	"For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003-~~6~~ 7 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-~~6~~7.
CIP-003-5 R1.2	CIP-003-~~6~~ 7 R1.1.2	No change.
CIP-003-5 R1.3	CIP-003-~~6~~ 7 R1.1.3	No change.
CIP-003-5 R1.4	CIP-003-~~6~~ 7 R1.1.4	No change.
CIP-003-5 R1.5	CIP-003-~~6~~ 7 R1.1.5	No change.
CIP-003-5 R1.6	CIP-003-~~6~~ 7 R1.1.6	No change.
CIP-003-5 R1.7	CIP-003-~~6~~ 7 R1.1.7	No change.
CIP-003-5 R1.8	CIP-003-~~6~~ 7 R1.1.8	No change.
CIP-003-5 R1.9	CIP-003-~~6~~ 7 R1.1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-~~6~~ 7 R1.2	"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003-~~6~~ 7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1."
CIP-003-5 R2.1	CIP-003-~~6~~ 7 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-~~6~~7, Requirement R1, Part 1.2.1.
CIP-003-5 R2.2	CIP-003-~~6~~7~~,~~ R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-~~6~~7, Requirement R1, Part 1.2.2.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-~~6~~ 7 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-~~6~~7, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity."
CIP-003-5 R2.4	CIP-003-~~6~~ 7 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-~~6~~7, Requirement R1, Part 1.2.4.
NEW	CIP-003-~~6~~7, Attachment 1	CIP-003-~~6~~ 7 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003-~~6~~ 7 R3	No change.
CIP-003-5 R4	CIP-003-~~6~~ 7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-~~6~~ 7 R1	No change.
CIP-004-5.1 R1.1	CIP-004-~~6~~ 7 R1.1	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2	CIP-004-~~6~~ 7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement "a cyber security training program(s)." That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-~~6~~ 7 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-~~6~~ 7 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-~~6~~ 7 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-~~6~~ 7 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-~~6~~ 7 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-~~6~~ 7 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-~~6~~ 7 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-~~6~~ 7 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-~~6~~ 7 R2.1.8	No change.
CIP-004-5.1 R2.1.9	CIP-004-~~6~~ 7 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-~~6~~ 7 R2.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.3	CIP-004-~~6~~ 7 R2.3	No change.
CIP-004-5.1 R3	CIP-004-~~6~~ 7 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-~~6~~ 7 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-~~6~~ 7 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-~~6~~ 7 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-~~6~~ 7 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-~~6~~ 7 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-~~6~~ 7 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-~~6~~ 7 R3.5	No change.
CIP-004-5.1 R4	CIP-004-~~6~~ 7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-~~6~~ 7 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-~~6~~ 7 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-~~6~~ 7 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-~~6~~ 7 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-~~6~~ 7 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-~~6~~ 7 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-~~6~~ 7 R4.4	No change.
CIP-004-5.1 R5	CIP-004-~~6~~ 7 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R5.1	CIP-004-~~6~~ 7 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-~~6~~ 7 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-~~6~~ 7 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-~~6~~ 7 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-~~6~~ 7 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-~~6~~ 7 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R1.1	CIP-007-~~6~~ 7 R1.1	No change.
CIP-007-5 R1.2	CIP-007-~~6~~ 7 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-~~6~~ 7 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R2.1	CIP-007-~~6~~ 7 R2.1	No change.
CIP-007-5 R2.2	CIP-007-~~6~~ 7 R2.2	No change.
CIP-007-5 R2.3	CIP-007-~~6~~ 7 R2.3	No change.
CIP-007-5 R2.4	CIP-007-~~6~~ 7 R2.4	No change.
CIP-007-5 R3	CIP-007-~~6~~ 7 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R3.1	CIP-007-~~6~~ 7 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-~~6~~ 7 R3.2	No change.
CIP-007-5 R3.3	CIP-007-~~6~~ 7 R3.3	No change.
CIP-007-5 R4	CIP-007-~~6~~ 7 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R4.1	CIP-007-~~6~~ 7 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-~~6~~ 7 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-~~6~~ 7 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-~~6~~ 7 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-~~6~~ 7 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-~~6~~ 7 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-~~6~~ 7 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-~~6~~ 7 R4.3	No change.
CIP-007-5 R4.4	CIP-007-~~6~~ 7 R4.4	No change.
CIP-007-5 R5	CIP-007-~~6~~ 7 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-007-5 R5.2	CIP-007-~~6~~ 7 R5.2	No change.
CIP-007-5 R5.3	CIP-007-~~6~~ 7 R5.3	No change.
CIP-007-5 R4	CIP-007-~~6~~ 7 R4	No change.
CIP-007-5 R5	CIP-007-~~6~~ 7 R5	No change.
CIP-007-5 R5.1	CIP-007-~~6~~ 7 R5.1	No change.
CIP-007-5 R5.2	CIP-007-~~6~~ 7 R5.2	No change.
CIP-007-5 R5.3	CIP-007-~~6~~ 7 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-~~6~~ 7 R5.4	No change.
CIP-007-5 R5.5	CIP-007-~~6~~ 7 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-~~6~~ 7 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-~~6~~ 7 R5.5.2	No change.
CIP-007-5 R6	CIP-007-~~6~~ 7 R6	No change.
CIP-007-5 R7	CIP-007-~~6~~ 7 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-~~2~~ 3 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-010-1 R1.1	CIP-010-~~2~~ 3 R1.1	No change.
CIP-010-1 R1.2	CIP-010-~~2~~ 3 R1.2	No change.
CIP-010-1 R1.3	CIP-010-~~2~~ 3 R1.3	No change.
CIP-010-1 R1.4	CIP-010-~~2~~ 3 R1.4	No change.
CIP-010-1 R1.5	CIP-010-~~2~~ 3 R1.5	No change.
CIP-010-1 R1.2	CIP-010-~~2~~ 3 R1.2	No change.
CIP-010-1 R1.3	CIP-010-~~2~~ 3 R1.3	No change.
CIP-010-1 R1.4	CIP-010-~~2~~ 3 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-~~2~~ 3 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-~~2~~ 3 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-~~2~~ 3 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-~~2~~ 3 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-~~2~~ 3 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-~~2~~ 3 R1.5.2	No change.
CIP-010-1 R2	CIP-010-~~2~~ 3 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-010-1 R2.1	CIP-010-~~2~~ 3 R2.1	No change.
CIP-010-1 R3	CIP-010-~~2~~ 3 R3	No change.
CIP-010-1 R3.1	CIP-010-~~2~~ 3 R3.1	No change.
CIP-010-1 R3.2	CIP-010-~~2~~ 3 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-~~2~~ 3 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-~~2~~ 3 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-~~2~~ 3 R3.3	No change.
CIP-010-1 R3.4	CIP-010-~~2~~ 3 R3.4	No change.
NEW	CIP-010-~~2~~ 3 R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."
NEW	CIP-010-~~2~~3, Attachment 1	CIP-010-~~2~~ 3 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-~~2~~ 3 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-~~2~~ 3 R1.1	No change.
CIP-011-1 R1.2	CIP-011-~~2~~ 3 R1.2	No change.
CIP-011-1 R2	CIP-011-~~2~~ 3 R2	No change.
CIP-011-1 R2.1	CIP-011-~~2~~ 3 R2.1	No change.
CIP-011-1 R2.2	CIP-011-~~2~~ 3 R2.2	No change.

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
1	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren_in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 82.61% Approval: 80.73%			
2	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO_in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 83.01% Approval: 79.89%			
3	Project 2008-04	FAC-010_FAC-011_FAC-014_Order_705_in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 88.83% Approval: 95.43%			
4	Project 2008-07	Interpretation Request - EOP-002 - Brookfield_in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 89.67% Approval: 76.47%			
5	Project 2008-04	FAC-010_FAC-011_FAC-014_Order_705_rc	Recirculation Ballot	6/13/2008	6/22/2008	Quorum: 89.36% Approval: 95.21%			
6	Project 2008-09	Request for Interpretation - EOP-001-0 - RECM_in	Initial Ballot	6/19/2008	7/2/2008	Quorum: 84.82% Approval: 85.79%			
7	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren_rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.57% Approval: 79.13%			
8	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO_rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.98% Approval: 78.31%			
9	Pre-2006	IROL Standard - IRO-010_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.71% Approval: 88.40%			
10	Pre-2006	IROL Standard - IRO-009_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.63% Approval: 89.44%			
11	Pre-2006	IROL Standard - IRO-008_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.67% Approval: 91.71%			
12	Project 2006-07	ATC et al Standard - MOD-030_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.37% Approval: 56.56%			
13	Project 2006-07	ATC et al Standard - MOD-029_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.67% Approval: 92.62%			
14	Project 2006-07	ATC et al Standard - MOD-028_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.64% Approval: 79.47%			
15	Project 2006-07	ATC et al Standard - MOD-008_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.27% Approval: 80.44%			
16	Project 2006-07	ATC et al Standard - MOD-001_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.02% Approval: 75.97%			
17	Project 2008-10	Request for Interpretation - CIP-006-1 - Progress Energy_in	Initial Ballot	8/7/2008	8/16/2008	Quorum: 88.18% Approval: 21.52%			
18	Pre-2006	IROL Standard - IRO-008_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.72% Approval: 89.49%			
19	Pre-2006	IROL Standard - IRO-009_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.68% Approval: 86.53%			
20	Pre-2006	IROL Standard - IRO-010_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.75% Approval: 85.95%			
21	Project 2006-07	ATC et al Standards - MOD-001_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 94.87% Approval: 76.83%			
22	Project 2006-07	ATC et al Standard - MOD-008_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.15% Approval: 81.49%			
23	Project 2006-07	ATC et al Standard - MOD-028_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.54% Approval: 79.34%			
24	Project 2006-07	ATC et al Standard - MOD-029_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.56% Approval: 92.24%			
25	Project 2006-07	ATC et al Standard - MOD-030_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.24% Approval: 74.26%			
26	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting_in	Initial Ballot	9/9/2008	9/17/2008	Quorum: 85.78% Approval: 90.37%			
27	Project 2006-07	ATC et al Standard - MOD-004_in	Initial Ballot	9/11/2008	9/21/2008	Quorum: 79.26% Approval: 66.29%			
28	Project 2007-14	Permanent Changes to CI Timing Tables_in	Initial Ballot	9/12/2008	9/22/2008	Quorum: 79.74% Approval: 100.00%			
29	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002_rb	Re-ballot	10/6/2008	10/24/2008	Quorum: 82.61% Approval: 74.67%			
30	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission_in	Initial Ballot	10/21/2008	10/30/2008	Quorum: 83.33% Approval: 96.94%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
31	Project 2006-01	Project 2006-01 - PER-005-1_in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 90.13% Approval: 82.47%			
32	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings_in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 89.13% Approval: 70.01%			
33	Project 2006-07	ATC et al Standard - MOD-004_rc	Recirculation Ballot	10/28/2008	11/6/2008	Quorum: 91.49% Approval: 83.71%			
34	Project 2006-07	Project 2006-07 (ATC) MOD-030-2_in	Initial Ballot	12/1/2008	12/10/2008	Quorum: 83.77% Approval: 86.51%			
35	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings_rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 93.04% Approval: 57.37%			
36	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission_rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 87.62% Approval: 97.47%			
37	Project 2006-01	Project 2006-01 - PER-005-1_rc	Recirculation Ballot	12/12/2008	12/22/2008	Quorum: 91.48% Approval: 80.63%			
38	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE_in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.15% Approval: 97.39%			
39	Project 2008-16	TOP-004-2 VSL Revisions_in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.20% Approval: 93.93%			
40	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting_rc	Recirculation Ballot	1/6/2009	1/15/2009	Quorum: 91.47% Approval: 91.21%			
41	Project 2006-07	Project 2006-07 (ATC) MOD-030-2_rc	Recirculation Ballot	1/20/2009	1/29/2009	Quorum: 85.86% Approval: 86.39%			
42	Project 2008-16	TOP-004-2 VSL Revisions_rc	Recirculation Ballot	1/28/2009	2/6/2009	Quorum: 92.59% Approval: 96.06%			
43	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE_rc	Recirculation Ballot	2/6/2009	2/16/2009	Quorum: 93.81% Approval: 99.12%			
44	Project 2008-09	Interpretation Request - EOP-001 - R1 - RECM_in	Initial Ballot	2/27/2009	3/9/2009	Quorum: 89.67% Approval: 89.03%			
45	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro_in	Initial Ballot	3/19/2009	3/30/2009	Quorum: 89.78% Approval: 92.62%			
46	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions_in	Initial Ballot	4/1/2009	4/10/2009	Quorum: 91.90% Approval: 84.06%			
47	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1_in	Initial Ballot	4/8/2009	4/17/2009	Quorum: 92.70% Approval: 92.71%			
48	Project 2006-03	Project 2006-03 EOP-001_EOP-005_EOP-006 System Restoration and Blackstart_in	Initial Ballot	4/14/2009	4/23/2009	Quorum: 89.81% Approval: 76.63%			
49	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions_rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 94.37% Approval: 88.32%			
50	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro_rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 95.56% Approval: 92.81%			
51	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1_in	Initial Ballot	4/22/2009	5/1/2009	Quorum: 88.64% Approval: 84.77%			
52	Project 2006-03	Project 2006-03 EOP-001_EOP-005_EOP-006 System Restoration and Blackstart_rc	Recirculation Ballot	5/6/2009	5/18/2009	Quorum: 92.08% Approval: 75.39%			
53	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1_in	initial Ballot	5/25/2009	6/4/2009	Quorum: 85.13% Approval: 82.10%			
54	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1_rc	Recirculation Ballot	5/26/2009	6/5/2009	Quorum: 90.45% Approval: 85.76%			
55	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a_in	Initial Ballot	6/1/2009	6/11/2009	Quorum: 87.10% Approval: 95.71%			
56	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716_in	Initial Ballot	6/12/2009	6/22/2009	Quorum: 81.72% Approval: 94.09%			
57	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1_in	Initial Ballot	6/15/2009	6/24/2009	Quorum: 87.23% Approval: 83.94%			
58	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1_rc	Recirculation Ballot	7/7/2009	7/16/2009	Quorum: 92.77% Approval: 84.96%			
59	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1_rc	Recirculation Ballot	7/8/2009	7/17/2009	Quorum: 90.26% Approval: 82.25%			
60	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716_rc	Recirculation Ballot	7/10/2009	7/20/2009	Quorum: 87.10% Approval: 96.94%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
61	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1_rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 95.26% Approval: 95.62%			
62	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a_rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 91.24% Approval: 98.85%			
63	Project 2007-23	Project 2007-23 TPL Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 90.46%			
64	Project 2007-23	Project 2007-23 TOP Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.40% Approval: 89.14%			
65	Project 2007-23	Project 2007-23 PRC Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.32% Approval: 88.26%			
66	Project 2007-23	Project 2007-23 IRO Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.16% Approval: 90.15%			
67	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 88.63%			
68	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.64% Approval: 87.63%			
69	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.50% Approval: 85.78%			
70	Project 2007-23	Project 2007-23 BAL Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.28% Approval: 89.56%			
71	Project 2008-08	Project 2008-08 EOP Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 87.98% Approval: 87.31%			
72	Project 2009-17	Project 2009-17 Interpretation - Y-W Electric and Tri-State - PRC-004-1 and PRC-005-1_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 90.32% Approval: 62.15%			
73	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009_rb	Re-ballot	7/27/2009	8/14/2009	Quorum: 84.65% Approval: 74.79%			
74	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1_in	Initial Ballot	8/6/2009	8/17/2009	Quorum: 84.68% Approval: 68.92%			
75	Project 2007-23	Project 2007-23 TPL Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 89.28%			
76	Project 2007-23	Project 2007-23 BAL Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.04% Approval: 89.41%			
77	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.41% Approval: 84.64%			
78	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.67% Approval: 88.04%			
79	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.17% Approval: 88.73%			
80	Project 2007-23	Project 2007-23 IRO Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 90.77%			
81	Project 2007-23	Project 2007-23 PRC Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.31% Approval: 86.93%			
82	Project 2007-23	Project 2007-23 TOP Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.11% Approval: 88.26%			
83	Project 2008-08	Project 2008-08 EOP Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.70% Approval: 85.80%			
84	Order 706-B	Order 706-B Nuclear Implementation Plan_in	Initial Ballot	8/19/2009	8/28/2009	Quorum: 81.96% Approval: 97.37%			
85	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002_rc	Recirculation Ballot	8/20/2009	8/31/2009	Quorum: 86.96% Approval: 70.85%			
86	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.68% Approval: 80.37%			
87	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.92% Approval: 79.04%			
88	Project 2009-18	Project 2009-18 - Withdraw Three Midwest ISO Waivers_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 85.28% Approval: 99.62%			
89	Order 706-B	Order 706-B Nuclear Implementation Plan_rc	Recirculation Ballot	9/1/2009	9/10/2009	Quorum: 87.11% Approval: 97.18%			
90	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009_rc	Recirculation Ballot	9/2/2009	9/14/2009	Quorum: 86.31% Approval: 76.09%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
91	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards) in	Initial Ballot	9/10/2009	9/21/2009	Quorum: 87.45% Approval: 94.18%			
92	Project 2009-16	Project 2009-16 - Interpretation - WECC - CIP-007-1 in	Initial Ballot	9/9/2009	9/21/2009	Quorum: 85.31% Approval: 100.00%			
93	Project 2006-04	Project 2006-04 - Back-up Facilities - EOP-008-1_in	Initial Ballot	9/16/2009	9/28/2009	Quorum: 82.69% Approval: 72.86%			
94	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1_rc	Recirculation Ballot	9/29/2009	10/9/2009	Quorum: 89.92% Approval: 68.31%			
95	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 Revised R1 for Progress Energy	Initial Ballot	9/30/2009	10/12/2009	Quorum: 79.92% Approval: 74.47%			
96	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_rc	Recirculation Ballot	10/16/2009	10/26/2009	Quorum: 86.29% Approval: 83.25%			
97	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards) rc	Recirculation Ballot	11/2/2009	11/12/2009	Quorum: 88.70% Approval: 94.24%			
98	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 2 in	Initial Ballot	11/5/2009	11/16/2009	Quorum: 85.97% Approval: 98.07%			
99	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response _in	Initial Ballot	11/20/2009	11/30/2009	Quorum: 89.58% Approval: 88.07%			
100	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 1) in	Initial Ballot	11/19/2009	12/7/2009	Quorum: 85.83% Approval: 58.91%			
101	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. in	Initial Ballot	11/20/2009	12/7/2009	Quorum: 87.11% Approval: 93.40%			
102	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response _rc	Recirculation Ballot	12/3/2009	12/14/2009	Quorum: 93.33% Approval: 85.55%			
103	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers in	Initial Ballot	12/1/2009	12/14/2009	Quorum: 86.13% Approval: 72.11%			
104	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1 rc	Recirculation Ballot	12/11/2009	12/23/2009	Quorum: 90.08% Approval: 78.77%			
105	Project 2009-24	Project 2009-24 - Interpretation - FMPA - EOP-005-1 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 87.68% Approval: 17.79%			
106	Project 2009-25	Project 2009-25 - Interpretation - BPA - BAL-001-01.a and BAL-002-0 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 88.00% Approval: 34.28%			
107	Project 2009-26	Project 2009-26 - Interpretation - WECC - CIP-004-1 in	Initial Ballot	1/6/2010	1/19/2010	Quorum: 84.21% Approval: 42.24%			
108	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Initial Ballot	1/12/2010	1/22/2010	Quorum: 89.16% Approval: 75.16%			
109	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 84.98% Approval: 90.82%			
110	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 87.36% Approval: 91.79%			
111	Project 2009-29	Project 2009-29 - Interpretation - TOP-002-2a for FMPP in	Initial Ballot	2/11/2010	2/22/2010	Quorum: 84.34% Approval: 84.56%			
112	Project 2009-19	Project 2009-19 - Interpretation - BAL-002-0 Northwest Power Pool RSG in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.83% Approval: 48.60%			
113	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. rc	Recirculation Ballot	2/16/2010	2/26/2010	Quorum: 92.44% Approval: 91.90%			
114	Project 2009-30	Project 2009-30 - Interpretation - PRC-001-1 for WPSC in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.51% Approval: 48.74%			
115	Project 2006-02	Project 2006-02 - Assess Transmission Future Needs - TPL-001-1 in	Initial Ballot	2/19/2010	3/1/2010	Quorum: 91.38% Approval: 35.36%			
116	Project 2009-31	Project 2009-31 - Interpretation - TOP-001-1 for FMPP in	Initial Ballot	3/3/2010	3/16/2010	Quorum: 88.24% Approval: 98.27%			
117	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Recirculation Ballot	3/8/2010	3/18/2010	Quorum: 93.71% Approval: 78.15%			
118	Project 2009-32	Project 2009-32 - Interpretation - EOP-003-1 for FMPP_rb	Re-ballot	3/10/2010	3/31/2010	Quorum: 91.37% Approval: 77.66%			
119	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers (Revision 1) in	Initial Ballot	3/29/2010	4/8/2010	Quorum: 88.52% Approval: 63.43%			
120	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3 in	Initial Ballot	4/15/2010	4/26/2010	Quorum: 81.97% Approval: 98.64%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
121	SPM	Standards Process Manual Revisions_in	Initial Ballot	4/19/2010	4/29/2010	Quorum: 87.82% Approval: 80.48%			
122	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2)_in	Initial Ballot	4/28/2010	5/10/2010	Quorum: 83.15% Approval: 74.55%			
123	SPM	Standards Process Manual Revisions_rc	Recirculation Ballot	4/30/2010	5/10/2010	Quorum: 93.73% Approval: 86.69%			
124	Project 2010-11	Project 2010-11 SAR for TPL Table 1 Order_in	Initial Ballot	5/17/2010	5/27/2010	Quorum: 84.41% Approval: 63.75%			
125	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3_in	Initial Ballot	5/19/2010	6/1/2010	Quorum: 84.83% Approval: 90.83%			
126	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3_rc	Recirculation Ballot	6/22/2010	7/2/2010	Quorum: 89.10% Approval: 87.24%			
127	Project 2006-04	Project 2006-04 - Backup Facilities - Revision 1_in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 89.05% Approval: 79.45%			
128	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief_in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 87.04% Approval: 84.98%			
129	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Initial Ballot	7/7/2010	7/17/2010	Quorum: 86.94% Approval: 43.13%			
130	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Initial Ballot	7/8/2010	7/17/2010	Quorum:91.12 % Approval: 22.91%			
131	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	7/8/2010	7/17/2010	Quorum: 86.00% Approval: 28.00%			
132	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: Protection System definition	Initial Ballot	7/8/2010	7/17/2010	Quorum: 87.85% Approval: 39.35%			
133	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Initial Ballot	7/9/2010	7/19/2010	Quorum: 86.18% Approval: 65.93%			
134	Project 2006-04	Prokect 2006-04 - Backup Facilities - Revision 1_rc	Recirculation Ballot	7/16/2010	7/26/2010	Quorum: 93.43% Approval: 85.22%			
135	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	7/23/2010	8/2/2010	Quorum: 94.70% Approval: 58.61%			
136	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	7/24/2010	8/3/2010	Quorum: 92.99% Approval: 49.61%			
137	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief_rc	Recirculation Ballot	8/20/2010	8/30/2010	Quorum: 88.26% Approval: 93.93%			
138	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Initial Ballot	9/14/2010	9/24/2010	Quorum: 92.73% Approval: 79.17%			
139	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Initial Ballot	9/17/2010	9/27/2010	Quorum: 96.46% Approval: 21.77%			
140	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	9/24/2010	10/4/2010	Quorum: 85.71% Approval: 81.72%			
141	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	10/2/2010	10/14/2010	Quorum: 84.11% Approval: 84.52%			
142	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3_rc	Recirculation Ballot	10/4/2010	10/14/2010	Quorum: 88.11% Approval: 99.14%			
143	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP_rc	Recirculation Ballot	10/5/2010	10/15/2010	Quorum: 92.19% Approval: 94.78%			
144	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA_rc	Recirculation Ballot	10/6/2010	10/16/2010	Quorum: 91.21% Approval: 93.44%			
145	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Recirculation Ballot	10/18/2010	10/28/2010	Quorum: 89.84% Approval: 84.67%			
146	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 93.66% Approval: 43.33%			
147	Project 2010-10	Project 2010-10 FAC-013-2 Planning Transfer Capability_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 88.54% Approval: 39.85%			
148	2010 SPM	2010 Standard Processes Manual (Proposed Changes)_in	Initial Ballot	10/28/2010	11/7/2010	Quorum: 81.61% Approval: 93.72%			
149	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Recirculation Ballot	11/1/2010	11/11/2010	Quorum: 89.41% Approval: 86.83%			
150	2010 SPM	2010 Standard Processes Manual (Proposed Changes)_rc	Recirculation Ballot	11/9/2010	11/13/2010	Quorum: 87.00% Approval: 92.88%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
151	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2)_rc	Recirculation Ballot	11/19/2010	12/3/2010	Quorum: 87.81% Approval: 82.41%			
152	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_in	Initial Ballot	12/1/2010	12/10/2010	Quorum: 87.07% Approval: 77.06%			
153	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-3	Initial Ballot	12/2/2010	12/11/2010	Quorum: 84.46% Approval: 42.89%			
154	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Recirculation Ballot	12/2/2010	12/13/2010	Quorum: 95.50% Approval: 86.91%			
155	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Initial Ballot	12/7/2010	12/16/2010	Quorum: 88.00% Approval: 51.51%			
156	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Successive Ballot	12/10/2010	12/20/2010	Quorum: 79.88% Approval: 44.65%			
157	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	12/10/2010	12/20/2010	Quorum: 78.00% Approval: 53.00%			
158	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_rc	Recirculation Ballot	12/20/2010	12/30/2010	Quorum: 90.49% Approval: 80.56%			
159	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR_in	Recirculation Ballot	12/27/2010	1/5/2011	Quorum: 90.42% Approval: 83.33%			
160	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 22.09%	Oppose 12/16/11		
161	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 33.49%	Oppose 12/16/11		
162	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 26.82%	Oppose 12/16/11		
163	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 28.04%	Oppose 12/16/11		
164	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.60%	Oppose 12/16/11		
165	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 24.15%	Oppose 12/16/11		
166	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 94.02% Approval: 34.30%	Oppose 12/16/11		
167	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 27.28%	Oppose 12/16/11		
168	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 26.61%	Oppose 12/16/11		
169	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.88%	Oppose 12/16/11		
170	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.15% Approval: 42.06%	Oppose 12/16/11		
171	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.56% Approval: 25.34%	Oppose 12/16/11		
172	Project 2010-10	Project 2010-10: FAC Order 729_in	Initial Ballot	12/30/2010	1/8/2011	Quorum: 83.23% Approval: 58.16%			
173	Project 2010-10	Project 2010-10: FAC Order 729_rc	Recirculation Ballot	1/14/2011	1/23/2011	Quorum: 86.65% Approval: 68.98%			
174	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR_rc	Recirculation Ballot	1/26/2011	2/5/2011	Quorum: 93.29% Approval: 86.79%	Support 1/5/11		
175	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Successive Ballot	1/24/2011	2/14/2011	Quorum: 83.95% Approval: 65.71%	Support 2/11/11		
176	Project 2007-23	Project 2007-23 - Violation Severity Levels	Non-binding Poll	2/9/2011	2/22/2011	Quorum: 78.00% Approval: 72.00%	Support 10/28/10		
177	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Successive Ballot	2/18/2011	2/28/2011	Quorum: 79.28% Approval: 79.34%	Support 2/22/11		
178	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Recirculation Ballot	2/24/2011	3/6/2011	Quorum: 87.35% Approval: 68.83%	Support 2/11/11		
179	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Initial Ballot	2/25/2011	3/7/2011	Quorum: 87.10% Approval: 49.54%	Support 3/2/11		
180	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-4	Successive Ballot	4/19/2011	4/28/2011	Quorum: 79.66% Approval: 38.00%	Oppose 4/19/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
181	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Initial Ballot	4/21/2011	5/2/2011	Quorum: 86.01% Approval: 48.74%	Abstain 4/26/11		
182	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Non-binding Poll	4/21/2011	5/2/2011	Quorum: 75.58% Approval: 73.00%			
183	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Successive Ballot	5/3/2011	5/12/2011	Quorum: 78.33% Approval: 67.00%	No Recommendation		
184	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	5/3/2011	5/12/2011	Quorum: 75.00% Approval: 66.00%			
185	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Recirculation Ballot	5/12/2011	5/23/2011	Quorum: 91.25% Approval: 78.92%	Support 5/12/11		
186	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Successive Ballot	5/18/2011	5/31/2011	Quorum: 92.07% Approval: 73.99%			
187	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Non-binding Poll	5/18/2011	5/31/2011	Quorum: 86.79% Approval: 71.9%			
188	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Initial Ballot	5/31/2011	6/9/2011	Quorum: 88.47% Approval: 48.64%	Oppose 5/31/11		
189	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Non-binding Poll	5/31/2011	6/9/2011	Quorum: 84.18% Approval: 41.00%			
190	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Recirculation Ballot	6/20/2011	6/30/2011	Quorum: 82.97% Approval: 64.76%	Support 6/28/11		
191	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Non-binding Poll	6/20/2011	6/30/2011	Quorum: 52.63% Approval: 60.00%			
192	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	Recirculation Ballot	7/13/2011	7/22/2011	Quorum: 94.33% Approval: 75.37%			
193	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.99%	Support 7/22/11		
194	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 75.17%	Support 7/22/11		
195	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.27%	Support 7/22/11		
196	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 93.00%			
197	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.66% Approval: 93.00%			
198	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 89.00%			
199	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.25% Approval: 46.53%	No Consensus 7/28/11		
200	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.75% Approval: 56.00%			
201	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.82% Approval: 18.23%	No Consensus 7/28/11		
202	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.35% Approval: 20.79%			
203	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Initial Ballot	9/19/2011	9/29/2011	Quorum: 84.86% Approval: 61.10%	Support 9/21/11		
204	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	9/19/2011	9/29/2011	Quorum: 83.13% Approval: 68.68%			
205	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Definition of BES	Initial Ballot	9/30/2011	10/10/2011	Quorum: 92.97% Approval: 71.68%	No Consensus 10/3/11		
206	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Initial Ballot	9/30/2011	10/10/2011	Quorum: 89.53% Approval: 64.03%	No Consensus 10/7/111		
207	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Recirculation Ballot	10/4/2011	10/13/2011	Quorum: 87.17% Approval: 86.25%	Support 2/22/11		
208	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Initial Ballot	11/7/2011	11/16/2011	Quorum: 88.05% Approval: 85.53%	Support 11/8/11		
209	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Initial Ballot	11/8/2011	11/17/2011	Quorum: 91.20% Approval: 95.05%	Support 11/8/11		
210	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 88.22% Approval: 86.94%	Support 11/10/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
211	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Initial Ballot	11/9/2011	11/18/2011	Quorum: 85.08% Approval: 85.71%	Support 11/10/11		
212	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.82% Approval: 85.31%	Support 11/10/11		
213	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.29% Approval: 96.09%	Support 11/10/11		
214	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Successive Ballot	11/11/2011	11/21/2011	Quorum: 83.53% Approval: 95.99%	Support 11/14/11		
215	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System and Implementation Plan	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 95.92% Approval: 81.32%	Support 10/3/11		
216	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 93.02% Approval: 81.48%	Support 10/3/11		
217	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Initial Ballot	11/30/2011	12/9/2011	Quorum: 93.92% Approval: 30.82%	Oppose 12/5/11		
218	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Non-binding Poll	11/30/2011	12/9/2011	Quorum: 89.49% Approval: 36.00%			
219	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Initial Ballot	12/2/2011	12/12/2011	Quorum: 87.97% Approval: 36.21%	Oppose 12/5/11		
220	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	12/2/2011	12/12/2011	Quorum: 85.28% Approval: 45.00%			
221	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Recirculation Ballot	12/9/2011	12/19/2011	Quorum: 88.02% Approval: 96.04%	Support 11/14/11		
222	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Recirculation Ballot	12/12/2011	12/22/2011	Quorum: 90.10% Approval: 92.49%	Support 11/8/11		
223	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 92.00% Approval: 94.58%	Support 11/8/11		
224	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 88.48% Approval: 90.10%	Support 11/10/11		
225	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 87.17% Approval: 85.38%	Support 11/10/11		
226	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.91% Approval: 85.03%	Support 11/10/11		
227	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1a	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.65% Approval: 96.43%	Support 11/10/11		
228	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 59.93%	Oppose 1/9/12		
229	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 77.08 %	Support 1/9/12		
230	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 78.95%	Support 1/9/12		
231	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Non-binding Poll	1/4/2012	1/13/2012	Quorum: 78.27% Approval: 93.00%			
232	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Non-binding Poll	1/9/2012	1/18/2012	Quorum: 76.41% Approval: 71.42%			
233	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 67.61%			
234	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 70.28%			
235	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 54.64%	Oppose 2/7/12		
236	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 82.11% Approval: 80.62%	Support 2/7/12		
237	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 80.21%	Support 2/7/12		
238	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.35% Approval: 71.35%			
239	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.06% Approval: 90.86%			
240	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 79.77% Approval: 84.69%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
241	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Successive Ballot	3/14/2012	3/23/2012	Quorum: 88.55% Approval: 79.61%	Support 3/16/12		
242	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Initial Ballot	3/14/2012	3/23/2012	Quorum: 89.63% Approval: 94.71%	Support 3/16/12		
243	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR-002 for Constellation	Initial Ballot	3/14/2012	3/23/2012	Quorum: 86.92% Approval: 63.09%	Support 3/16/12		
244	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 81.45% Approval: 61.21%			
245	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 80.38% Approval: 41.09%			
246	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	3/19/2012	3/29/2012	Quorum: 84.32% Approval: 73.93%	Support 3/19/12		
247	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	3/19/2012	3/29/2012	Quorum: 81.93% Approval: 66.12%			
248	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.37% Approval: 85.18%	Support 4/5/12		
249	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.10% Approval: 85.01%	Support 4/5/12		
250	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.28% Approval: 41.09%	Oppose 4/16/12		
251	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 36.84%	Oppose 4/16/12		
252	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 48.70%%	Oppose 4/16/12		
253	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.82% Approval: 43.72%			
254	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.04% Approval: 38.56%			
255	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.53% Approval: 46.38%			
256	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1a	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.95% Approval: 92.41%	Support 4/16/12		
257	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28%% Approval: 75.44%			
258	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.02% Approval: 87.22%			
259	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28% Approval: 80.11%			
260	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.21% Approval: 69.84%			
261	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.48% Approval: 67.64%			
262	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 90.96% Approval: 80.08%	Support 3/16/12		
263	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 92.68% Approval: 94.61%	Support 3/16/12		
264	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.72% Approval: 87.34%			
265	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.94% Approval: 87.32%			
266	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1b	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 90.44% Approval: 93.23%			
267	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 76.84%	Abstain 4/19/12		
268	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 88.11%	Support 4/19/12		
269	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 80.79%	Support 4/19/12		
270	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.63% Approval: 37.37%	Abstain 5/17/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
271	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.45% Approval: 60.55%	Abstain 5/17/12		
272	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.40% Approval: 38.81%	Abstain 5/17/12		
273	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.98% Approval: 55.08%	Abstain 5/17/12		
274	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.22% Approval: 38.50%	Abstain 5/17/12		
275	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 45.78%	Abstain 5/17/12		
276	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.19% Approval: 67.19%	Abstain 5/17/12		
277	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 60.19%	Abstain 5/17/12		
278	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 47.92%	Abstain 5/17/12		
279	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 58.23%	Abstain 5/17/12		
280	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	5/11/2012	5/21/2012	Quorum: 85.12% Approval: 66.23%	Abstain 5/17/12		
281	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	5/11/2012	5/21/2012	Quorum: 84.09% Approval: 47.88%	Abstain 5/17/12		
282	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	5/15/2012	5/24/2012	Quorum: 84.43% Approval: 46.18%			
283	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	5/15/2012	5/24/2012	Quorum: 79.95% Approval: 52.67%			
284	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Initial Ballot	6/11/2012	6/20/2012	Quorum: 84.14% Approval: 21.11%	Oppose 6/13/12		
285	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	6/11/2012	6/20/2012	Quorum: 81.01% Approval: 28.30%			
286	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	6/18/2012	6/27/2012	Quorum: 79.46% Approval: 79.00%			
287	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	6/18/2012	6/27/2012	Quorum: 75.00% Approval: 70.21%			
288	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Successive Ballot	6/18/2012	6/27/2012	Quorum: 85.98% Approval: 68.22%	Support 6/26/12		
289	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Initial Ballot	6/26/2012	7/5/2012	Quorum: 84.24% Approval: 23.82%	Oppose 6/27/12		
290	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	6/26/2012	7/5/2012	Quorum: 82.26% Approval: 25.19%			
291	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.34% Approval: 81.71%			
292	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.04% Approval: 81.72%			
293	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 84.16% Approval: 79.16%			
294	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 83.87% Approval: 86.91%			
295	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	6/27/2012	7/9/2012	Quorum: 75.37% Approval: 72.16%	No Consensus 7/5/12		
296	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	6/27/2012	7/11/2012	Quorum: 75.37% Approval: 73.71%			
297	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Recirculation Ballot	7/18/2012	7/27/2012	Quorum: 90.97% Approval: 69.81%	Support 6/26/12		
298	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Non-binding Poll	7/18/2012	7/27/2012	Quorum: 81.31% Approval: 60.93%			
299	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Initial Ballot	7/20/2012	7/30/2012	Quorum: 80.39% Approval: 79.28%	Oppose 7/20/12		
300	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Non-binding Poll	7/20/2012	7/30/2012	Quorum: 78.26% Approval: 76.07%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
301	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Initial Ballot	7/24/2012	8/2/2012	Quorum: 83.11% Approval: 54.16%	Oppose 7/20/12		
302	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	8/17/2012	8/27/2012	Quorum: 78.11% Approval: 80.31%	Support 6/22/12		
303	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group	Successive Ballot	8/23/2012	9/4/2012	Quorum: 79.21% Approval: 87.78%	Support 2/22/10		
304	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Initial Ballot	8/29/2012	9/7/2012	Quorum: 86.71% Approval: 37.68%	Support 9/5/12		
305	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	8/29/2012	9/7/2012	Quorum: 84.17% Approval: 37.36%			
306	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Recirculation Ballot	9/6/2012	9/17/2012	Quorum: 80.35% Approval: 75.01%			
307	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols	Successive Ballot	9/11/2012	9/20/2012	Quorum: 77.70% Approval: 50.57%	Support 9/15/12		
308	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	9/11/2012	9/20/2012	Quorum: 84.05% Approval: 54.07%			
309	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Recirculation Ballot	9/12/2012	9/21/2012	Quorum: 85.36% Approval: 87.34%			
310	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	9/18/2012	9/27/2012	Quorum: 78.54% Approval: 63.40%	No Consensus 9/27/12		
311	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	9/18/2012	9/27/2012	Quorum: 78.93% Approval: 71.04%			
312	Project 2009-19	Project 2009-19 - Interpretation of BAL-002-0 NWPP Reserve Sharing Group	Recirculation Ballot	9/28/2012	10/8/2012	Quorum: 85.11% Approval: 90.34%	Support 2/22/10		
313	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 74.85%	Support 10/4/12		
314	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.37% Approval: 89.50%	Support 10/4/12		
315	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 85.58%	Support 10/4/12		
316	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 89.46%	Support 10/4/12		
317	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.11%	Support 10/4/12		
318	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 87.73%	Support 10/4/12		
319	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.74%	Support 10/4/12		
320	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.73%	Support 10/4/12		
321	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 84.60%	Support 10/4/12		
322	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.90%	Support 10/4/12		
323	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	10/1/2012	10/10/2012	Quorum: 78.93% Approval: 94.00%	Support 10/4/12		
324	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	10/1/2012	10/10/2012	Quorum: 79.13% Approval: 91.59%	Support 10/4/12		
325	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Initial Ballot	10/3/2012	10/12/2012	Quorum: 87.50% Approval: 63.25%	Support 10/4/12		
326	VRFs and VSLs	Revisions to Outstanding VRFs and VSLs	Non-binding Poll	10/10/2012	10/23/2012	Quorum: 78.57% Approval: 73.02%			
327	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Recirculation Ballot	10/15/2012	10/24/2012	Quorum: 81.08% Approval: 80.51%	Support 6/22/12		
328	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.55% Approval: 76.50%			
329	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.00% Approval: 57.24%			
330	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Successive Ballot	10/19/2012	10/31/2012	Quorum: 83.61% Approval: 68.31%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
331	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.34% Approval: 71.53%			
332	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.07% Approval: 70.64%			
333	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.88% Approval: 77.10%			
334	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.40% Approval: 52.72%			
335	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 77.94% Approval: 64.24%			
336	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.06% Approval: 68.93%			
337	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.51% Approval: 63.63%			
338	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 78.59%	Support 10/4/12		
339	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 92.75%	Support 10/4/12		
340	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 89.73%	Support 10/4/12		
341	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 93.73%	Support 10/4/12		
342	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.53%	Support 10/4/12		
343	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 91.79%	Support 10/4/12		
344	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.47%	Support 10/4/12		
345	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 94.60%	Support 10/4/12		
346	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 88.99%	Support 10/4/12		
347	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.67%	Support 10/4/12		
348	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation Plan	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 94.91%	Support 10/4/12		
349	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 93.23%	Support 10/4/12		
350	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Recirculation Ballot	10/24/2012	11/5/2012	Quorum: 85.14% Approval: 71.39%			
351	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	10/24/2012	11/5/2012	Quorum: 78.93% Approval: 71.04%			
352	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Successive Ballot	10/26/2012	11/6/2012	Quorum: 82.04% Approval: 76.08%	Support 11/5/12		
353	Project 2010-11	Project 2010-11 TPL footnote b Initial Ballot October 2012 in	Initial Ballot	11/9/2012	11/19/2012	Quorum: 80.45% Approval: 56.18%			
354	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Initial Ballot	11/26/2012	12/5/2012	Quorum: 84.81% Approval: 72.57%	Oppose 12/5/12		
355	Project 2013-02	Project 2013-02 - Paragraph 81	Initial Ballot	11/30/2012	12/10/2012	Quorum: 75.77% Approval: 96.45%	Support 12/10/12		
356	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	12/4/2012	12/13/2012	Quorum: 76.78% Approval: 53.57%	No Consensus 12/13/12		
357	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	12/4/2012	12/13/2012	Quorum: 77.22% Approval: 57.91%			
358	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Successive Ballot	12/7/2012	12/17/2012	Quorum: 76.47% Approval: 33.23%	Oppose 12/17/12		
359	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	12/7/2012	12/17/2012	Quorum: 75.58% Approval: 34.80%			
360	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Initial Ballot	12/11/2012	12/20/2012	Quorum: 84.50% Approval: 95.60%	Support 12/19/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
361	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Successive Ballot	12/11/2012	12/20/2012	Quorum: 83.24% Approval: 84.48%	Support 12/19/12		
362	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.89% Approval: 73.06%			
363	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 79.00% Approval: 79.36%			
364	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.68% Approval: 74.27%			
365	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 85.87% Approval: 73.63%			
366	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.19% Approval: 76.53%			
367	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	1/2/2013	1/11/2013	Quorum: 78.16% Approval: 60.31%	Support 1/11/13		
368	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	Non-binding Poll	1/2/2013	1/11/2013	Quorum: 76.38% Approval: 55.68%			
369	Project 2010-11	Project 2010-11 Successive Ballot December 2012_in	Successive Ballot	1/2/2013	1/11/2013	Quorum: 85.47% Approval: 65.77%	No Consensus 1/11/13		
370	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Initial Ballot	1/4/2013	1/14/2013	Quorum: 83.94% Approval: 21.80%	Oppose 1/11/13		
371	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Non-binding Poll	1/4/2013	1/14/2013	Quorum: 82.23% Approval: 24.27%			
372	Project 2013-02	Project 2013-02 - Paragraph 81	Recirculation Ballot	1/8/2013	1/17/2013	Quorum: 84.60% Approval: 95.22%	Support 12/10/12		
373	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Recirculation Ballot	1/14/2013	1/23/2013	Quorum: 87.13% Approval: 99.09%	Support 12/19/12		
374	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Recirculation Ballot	1/18/2013	1/28/2013	Quorum: 85.90% Approval: 85.57%	Support 12/19/12		
375	Project 2010-11	Project 2010-11 Recirculation Ballot Jan 2013_in	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 88.55% Approval: 69.63%	No Consensus 1/11/13		
376	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 85.67% Approval: 77.61%	Oppose 12/5/12		
377	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Successive Ballot	2/11/2013	2/20/2013	Quorum: 77.62% Approval: 50.66%	Support 9/5/12		
378	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	2/11/2013	2/20/2013	Quorum: 75.38% Approval: 50.60%			
379	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	2/15/2013	2/28/2013	Quorum: 78.80% Approval: 89.01%	Support 1/11/13		
380	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Non-binding Poll	2/15/2013	2/28/2013	Quorum: 76.38% Approval: 84.24%			
381	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Initial Ballot	3/1/2013	3/11/2013	Quorum: 76.36% Approval: 54.65%			
382	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Successive Ballot	3/13/2013	3/22/2013	Quorum: 77.48% Approval: 84.27%	No Consensus 3/22/13		NPCC to abstain - international nature of the ERO and BPS is not used in Reliability Standards
383	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.58% Approval: 97.18%	Support 3/14/13		
384	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.52% Approval: 98.89%	Support 3/14/13		
385	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Recirculation Ballot	3/18/2013	3/27/2013	Quorum: 81.33% Approval: 89.44%	Support 1/11/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
386	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	3/27/2013	4/5/2013	Quorum: 78.39% Approval: 57.50%	No Consensus 4/4/13		The RSC did not reach a full consensus however the majority of respondents had indicated they will support the standard - see comment form for further details. Some believe the standard is not necessary and that existing whitepapers alleviate the need for it. In recognition of the NERC BOT's expectations that COM-003 will be approved by the industry and brought before them for approval, NPCC has voted affirmatively and will supply comments for the record outlining our concerns.
387	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	3/27/2013	4/5/2013	Quorum: 77.97% Approval: 54.28%			
388	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.60% Approval: 66.98%	No Consensus 4/23/13		The majority of NPCC's Balancing Authorities have indicated support for the standard, however NPCC as the Regional Entity has concerns based on results of the field trials that were conducted. These field trials have indicated the potential for an increased number of SOL violations as well as potential for increased ACE due to large inadvertent flows with the proposed BAAL limits based on frequency triggers. To be respectful of the positions of the NPCC BAs who will have to implement this new methodology and the support expressed, NPCC as the Regional Entity will cast an Abstention
389	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 42.75%	Oppose 4/23/13		There is a lack of technical justification for the 500 MW threshold within the standard-NPCC will submit suggested improvements

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
390	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 23.84%	Oppose 4/23/13		Losses of large blocks of load are typically caused by coincident transmission contingencies. Excessive and uninformed adjustments made to generation in order to bring the ACE to zero may well lead to further transmission issues. NPCC will submit suggested improvements
391	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
392	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
393	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
394	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Recirculation Ballot	4/18/2013	4/29/2013	Quorum: 80.70% Approval: 88.15%	No Consensus 3/22/13		
395	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Successive ballot	5/15/2013	5/24/2013	Quorum: 81.25% Approval: 69.23%	Support 5/23/13		The Regional Standard Committee has not expressed any concerns of significance that would warrant a ballot to reject, therefore the RSC recommends a yes vote, "Affirmative", to accept the standard
396	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Non-binding Poll	5/15/2013	5/24/2013	Quorum: 80.17% Approval: 61.11%			
397	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Successive Ballot	6/24/2013	7/3/2013	Quorum: 77.65% Approval: 52.71%			
398	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Non-binding Poll	6/24/2013	7/3/2013	Quorum: 77.12% Approval: 52.48%			
399	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Initial Ballot	7/3/2013	7/12/2013	Quorum: 85.53% Approval: 49.73%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
400	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Successive Ballot	7/10/2013	7/19/2013	Quorum: 76.32% Approval: 58.36%	No Consensus 7/19/13 [Due to the concerns expressed over the potential actions by the NERC BOT and FERC as well as the incremental improvement of the standard over the previous versions, NPCC as the Regional Entity will support the standard and submit comments.]		organizations support the standard as written however some members expressed concern that in order to measure compliance with R1 and R2, the standard will require all Reliability Directives to be investigated to determine if RC approved and documented communication protocols have been violated. Also it was identified that TO, BA communication protocols would have to approved by the RC potentially causing some legal issues if protocols aren't approved and casts question on the enforcement of those protocols. NPCC will be submitting some helpful comments should the standard pass and some non-substantive revision be performed prior to the "final" (previously named recirculation) ballot.
401	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 76.20% Approval: 55.37%			
402	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Successive Ballot	7/10/2013	7/19/2013	Quorum: 85.05% Approval: 72.43%	Support 7/19/13		
403	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 82.51% Approval: 64.59%			
404	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Final Ballot	7/16/2013	7/25/2013	Quorum: 92.31% Approval: 74.54%	No Consensus 7/22/13		The RSC has not reached a full consensus however the majority are in support. Issues outstanding for those not in support are concern over "hitting limits" more frequently and potential issues with BA's potentially "dragging" on the interconnection. NPCC will be voting affirmative on the standard.
405	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Initial Ballot	7/26/2013	8/5/2013	Quorum: 80.05% Approval: 93.00%	Support 8/5/13		
408	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025-1	Final Ballot	8/2/2013	8/12/2013	Quorum: 89.13% Approval: 76.52%	Support 8/12/13		
406	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Initial Ballot	8/2/2013	8/12/2013	Quorum: 76.32% Approval: 62.74%	Support 8/9/13		
407	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	8/2/2013	8/12/2013	Quorum: 75.89% Approval: 55.45%			
409	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Initial Ballot	8/14/2013	8/23/2013	Quorum: 78.33% Approval: 79.42%	Support 8/23/13		
410	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Non-binding Poll	8/14/2013	8/23/2013	Quorum: 77.45% Approval: 81.37%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
411	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Ballot	8/16/2013	8/26/2013	Quorum: 76.14% Approval: 51.10%	No Consensus 8/26/13		NPCC to support with comments
412	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Non-binding Poll	8/16/2013	8/26/2013	Quorum: 75.98% Approval: 53.29%			
413	Project 2010-01	Project 2010-01 - Training - PER-005-2	Ballot	8/23/2013	9/3/2013	Quorum: 75.25% Approval: 34.46%	No Consensus 8/31/13		NPCC to support with comments The most contentious issues raised by RSC members was surrounding the Control Center definition and the potential to vastly expand those needing training subject to the standard and compliance and that there was no need for a standard, rather, the FERC Directives should be addressed through other means.
414	Project 2010-01	Project 2010-01 - Training - PER-005-2	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 80.45% Approval: 34.24%			
415	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Ballot	8/23/2013	9/3/2013	Quorum: 81.89% Approval: 43.79%	Oppose 8/31/13		The standard, in the view of the group, has extensive issues including but not limited to, applicability issues, lacks clarity, missing measures, quality, and other substantive issues. NPCC will be submitting detailed comments to address these issues. The RSC does not believe it would be beneficial to support the standard at this point as the next step, if it fails the initial ballot, would still require an additional ballot prior to moving to recirculation due to the substantive changes that are needed for the next revision. NPCC will be submitting helpful comments to NERC and supporting the drafting team effort.
416	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 79.95% Approval: 44.23%			
417	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Ballot	8/26/2013	9/4/2013	Quorum: 82.29% Approval: 41.24%	Support 8/31/13		
418	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 79.66% Approval: 40.00%			
419	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Ballot	8/26/2013	9/4/2013	Quorum: 81.96% Approval: 55.76%	Support 8/31/13		
420	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 80.35% Approval: 58.97%			
421	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	8/26/2013	9/4/2013	Quorum: 78.68% Approval: 66.11%	Support 8/31/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
426	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Final Ballot	9/4/2013	9/13/2013	Quorum: 85.93% Approval: 90.83%	Support 8/5/13		
422	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Ballot	9/6/2013	9/16/2013	Quorum: 76.15% Approval: 58.23%	No Consensus 9/12/13		
423	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Non-binding Poll	9/6/2013	9/16/2013	Quorum: 75.69% Approval: 59.66%			
424	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Final Ballot	9/11/2013	9/20/2013	Quorum: 91.64% Approval: 98.61%	Support 3/14/13		
425	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Final Ballot	9/11/2013	9/20/2013	Quorum: 90.98% Approval: 98.92%	Support 3/14/13		
427	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Additional Ballot	10/9/2013	10/21/2013	Quorum: 77.58% Approval: 88.75%	Support 10/16/13		
428	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	10/9/2013	10/21/2013	Quorum: 75.89% Approval: 90.04%			
429	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing Phase 2 (Reclosing Relays) - PRC-005-3	Final Ballot	10/16/2013	10/25/2013	Quorum: 85.71% Approval: 85.38%			
430	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	10/18/2013	10/29/2013	Quorum: 75.83% Approval: 72.55%	Support 10/21/13		
431	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Final Ballot	10/25/2013	11/4/2013	Quorum: 86.90% Approval: 91.95%			
432	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	10/25/2013	11/7/2013	Quorum: 76.67% Approval: 58.24%	No Consensus 11/1/13		
433	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	11/1/2013	11/12/2013	Quorum: 76.23% Approval: 56.48%	Support 11/11/13		
434	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Initial Ballot	11/4/2013	11/13/2013	Quorum: 76.12% Approval: 67.35%	Support 11/5/13		
435	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-006-4	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 75.58%	Support 11/5/13		
436	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-009-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 68.40%	Support 11/5/13		
437	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 58.03%	Support 11/5/13		
438	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-011-1	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.52% Approval: 71.35%	Support 11/5/13		
439	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Initial Ballot	11/4/2013	11/15/2013	Quorum: 76.42% Approval: 77.82%	Support 11/5/13		
440	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Final Ballot	11/8/2013	11/18/2013	Quorum: 81.68% Approval: 74.34%	Support 10/21/13		
441	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Additional Ballot	11/8/2013	11/20/2013	Quorum: 81.69% Approval: 82.97%	No Consensus 8/26/13		
442	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.05% Approval: 73.46%	Support 8/31/13		
443	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.84% Approval: 69.42%	Support 8/31/13		
444	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	11/13/2013	11/22/2013	Quorum: 80.54% Approval: 57.59%	Support 8/31/13		
445	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Additional Ballot	11/15/2013	11/25/2013	Quorum: 80.81% Approval: 69.43%			
446	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	11/15/2013	11/25/2013	Quorum: 81.06% Approval: 66.09%			
447	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2	Additional Ballot	12/2/2013	12/12/2013	Quorum: 75.29% Approval: 64.24%	No Consensus 12/9/13	Affirmative	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
448	Project 2007-11	Project 2007-11 Disturbance Monitoring - PRC-002-2	Initial Ballot	12/6/2013	12/16/2013	Quorum: 82.25% Approval: 43.29%	No Consensus 12/15/13	Affirmative	Highlights of comments received expressed: • Agreement with the methodology to determine BES locations for which data had to be captured • Use of the term "locations" • DDR for Flowgates, IROLs • Clarification needed for some data that is to be captured • Editorial suggestions
449	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Final Ballot	12/6/2013	12/16/2013	Quorum: 87.53% Approval: 77.49%	Support 8/31/13	Affirmative	
450	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-006-4	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 80.77%	Support 11/5/13	Affirmative	
451	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-009-2	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 72.86%	Support 11/5/13	Affirmative	
452	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-011-1	Final Ballot	12/10/2013	12/20/2013	Quorum: 84.78% Approval: 72.91%	Support 11/5/13	Affirmative	
453	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Final Ballot	12/11/2013	12/20/2013	Quorum: 87.16% Approval: 86.40%	No Consensus 8/26/13	Affirmative	
454	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Final Ballot	12/13/2013	12/23/2013	Quorum: 84.34% Approval: 75.35%		Affirmative	
455	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-027-1	Additional Ballot	12/9/2013	12/31/2013	Quorum: 76.60% Approval: 65.71%	No Consensus 12/27/13	Affirmative	
456	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	1/10/2014	1/21/2014	Quorum: 76.92% Approval: 81.41%	Support 8/31/13	Affirmative	
457	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	1/8/2014	1/22/2014	Quorum: 7912% Approval: 74.63%	Support 11/11/13	Affirmative	
458	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 81.19%	Support 11/5/13	Affirmative	
459	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 90.23%	Support 11/5/13	Affirmative	
460	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Additional Ballot	1/16/2014	1/29/2014	Quorum: 76.12% Approval: 92.17%	Support 11/5/13	Affirmative	
461	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	1/22/2014	1/31/2014	Quorum: 76.03% Approval: 71.86%	No Consensus 11/1/13	Affirmative	Ballot Period Extended to 2/4/14
462	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.88% Approval: 83.44%	Support 11/5/13	Affirmative	
463	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.58% Approval: 91.51%	Support 11/5/13	Affirmative	
464	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Final Ballot	1/27/2014	2/5/2014	Quorum: 82.49% Approval: 82.45%	Support 8/31/13	Affirmative	
465	Project 2010-01	Project 2010-01 - Training - PER-005-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 84.02% Approval: 77.06%	Support 11/11/13	Affirmative	
466	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Final Ballot	1/31/2014	2/10/2014	Quorum: 81.79% Approval: 90.12%	Support 11/5/13	Affirmative	
467	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Additional Ballot	2/21/2014	3/3/2014	Quorum: 75.06% Approval: 62.63%	Support 9/5/12	Affirmative	Ballot Period Extended to 3/11/14
468	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Final Ballot	3/28/2014	4/7/2014	Quorum: 78.21% Approval: 77.62%	Support 3/28/14	Affirmative	
469	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	4/1/2014	4/10/2014	Quorum: 76.92% Approval: 83.40%	Support 8/31/13	Affirmative	
470	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	4/4/2014	4/14/2014	Quorum: 78.03% Approval: 82.40%		--	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments	
471	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	Initial Ballot	4/20/2014	4/24/2014	Quorum: 88.60% Approval: 82.07%	Support 4/23/14	Abstain		
472	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Final Ballot	4/25/2014	5/5/2014	Quorum: 80.37% Approval: 90.00%	Support--4/25/14	Affirmative		
473	Project 2013-04	Project 2013-04 - Voltage and Reactive Control - VAR-001-4, VAR-002-3	Final Ballot	4/23/2014	5/5/2014	Quorum: 83.84% Approval: 88.26%	Support--4/10/14	Affirmative		
474	Project 2014-04	Project 2014-04 - Physical Security - CIP-014-1	Final Ballot	5/1/2014	5/5/2014	Quorum: 92.53% Approval: 85.61%	Support--4/23/14	Abstain		
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Initial Ballot	5/6/2014	5/15/2014	Quorum: 85.79%/79.08% Approval: 86.28%/78.81%	No Consensus--5/15/14	Reject		
476	Project 2012-13	Project 2012-13 - NUC - Nuclear Plant Interface Coordination	Initial Ballot	5/13/2014	5/22/2014	Quorum: 80.60% Approval: 97.36%	Support--5/20/14	Affirmative		
477	Project 2007-17.3	Project 2007-17.3 - Protection System Maintenance and Testing Phase 3 (Sudden Pressure Relays) - PRC-005-X	Initial Ballot	5/23/2014	6/2/2014	Quorum: 85.42% Approval: 47.89%	Support	Affirmative		
478	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Initial Ballot	5/30/2014	6/9/2014	Quorum: 79.06% Approval: 17.02%	Does not Support--6/6/14	Negative		
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Final Ballot	6/12/2014	6/23/2014	Quorum: Approval: 89.03%/83.46%	Support	Affirmative		
479	Project 2007-11	Project 2007-11 - Disturbance Monitoring - PRC-002-2	Additional Ballot	6/13/2014	6/23/2014	Quorum: 77.69% Approval: 52.29%	Support	Affirmative	Extended to achieve a quorum.	
480	Project 2010-05.1	Project 2010-05.1 - Protection System: Phase 1 (Misoperations) - PRC-004	Additional Ballot	6/20/2014	7/9/2014	Quorum: 76.98% Approval: 74.53%	Support	Affirmative	Extended to achieve a quorum.	Last RSC Meeting
481	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	Ballot	6/23/2014	7/2/2014	Quorum: 82.32%/82.59%/82.59%/82.85%/82.85%/82.06%/82.59%/82.85%/82.85%/81.00%/80.74% Approval: 68.57%/36.94%/47.87%/60.26%/61.67%/57.94%/30.99%/62.18%/63.07%/62.64%/64.70%	No Consensus--6/24/14	Affirmative Negative Affirmative Affirmative Affirmative Affirmative Negative Affirmative Affirmative		
482	Project 2012-13	Project 2012-13 NUC - Nuclear Plant Interface Coordination	Final Ballot	6/24/2014	7/3/2014	Quorum: 88.63% Approval: 97.23%	Support--6/23/14	Affirmative		
483	Project 2014-02	Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions Rich HTML Content 1 http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx	Final Ballot	7/7/2014	7/16/2014	Quorum: 80.73%/80.49%/80.00%/80.24%/80.24%/80.49%/80.24%/78.29% Approval: 35.67%/80.76%/76.24%/78.41%/85.32%/49.42%/82.55%/78.58%	CIP-003 No CIP-004 Yes CIP-006 Yes CIP-007 Yes CIP-009 Yes CIP-010 Yes CIP-011 Yes Definitions Yes Support--7/14/14			
484	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)	Final Ballot	7/16/2014	7/25/2014	Quorum: 78.92% Approval: 58.88%	Support--7/23/14			
485	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	7/18/2014	7/28/2014	Quorum: 79.49%/80.15%/80.00%/80.83%/80.36% Approval: 91.38%/92.20%/89.51%/90.58%/87.09%	Support--7/24/14	Affirmative		
486	Project 2012-13	Project 2013-03 Geomagnetic Disturbance Mitigation	Final Ballot	7/21/2014	7/30/2014	Quorum: 82.67% Approval: 55.77%		Affirmative		
487	Project 2012-13	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Initial Ballot	7/29/2014	8/7/2014	Quorum: 76.37% Approval: 76.91%		Affirmative		
488	Project 2012-13	Project 2009-03 Emergency Operations	Initial Ballot	8/6/2014	8/15/2014	Quorum: 77.66%	Negative--8/14/14	Negative		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Approval: 42.27%	[illegible]	[illegible]	
489	Project 2014-01	Project 2010-05.1 - Protection System: Phase 1 (Misoperations) - PRC-004	Final Ballot	7/29/2014	8/7/2014	Quorum: 77.94% Approval: 79.75%	Support	Affirmative	
490	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	Final Ballot	8/27/2014	9/5/2014	Quorum: 85.32%/86.01% Approval: 95.35%/95.86%	Support	Affirmative	
491	Project 2007-17.3	Project 2007-17.3 - Protection System Maintenance and Testing	Additional Ballot	9/3/2014	9/12/2014	Quorum: 84.33% Approval: 76.03%	Support--9/4/14	Affirmative	
492	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	Additional Ballot	9/10/2014	9/19/2014	Quorum: 85.75%/84.96%/84.96%/85.22%/84.96%/85.22%/85.49%/85.22%/86.28%/83.11%/83.91% Approval: 76.12%/74.23%/75.67%/85.49%/75.96%/78.67%/48.73%/78.87%/87.03%/93.34%/90.13%	TOP-001-3: Negative TOP-002-4: Affirmative TOP-003-3: Affirmative IRO-001-4: No consensus however the majority indicated an Affirmative vote IRO-002-4: Negative IRO-008-2: No consensus, a majority indicated a Negative and the others indicated abstention IRO-010-2: Affirmative IRO-014-3: Negative IRO-017-1: Affirmative Implementation Plan and Definitions: Affirmative		
493	Project 2010-14.1	Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	Additional Ballot	9/23/2014	10/2/2014	Quorum: 79.94% Approval: 46.73%	Negative--10/1/14		
494	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Additional Ballot	9/26/2014	10/6/2014	Quorum: 79.01% Approval: 53.02%	Affirmative--10/1/14		
495	Project 2012-13	Project 2008-02 Undervoltage Load Shedding (UVLS) & Underfrequency Load Shedding (UFLS)	Additional Ballot	9/29/2014	10/8/2014	Quorum: 83.24%/84.82% Approval: 80.69%/84.05%	Affirmative--10/7/14	Affirmative	
496	Project 2012-13	Project 2013-03 Geomagnetic Disturbance Mitigation	Additional Ballot	10/1/2014	10/10/2014	Quorum: 82.93% Approval: 57.95%	Affirmative--10/7/14		
497	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)	Additional Ballot	10/3/2014	10/14/2014	Quorum: 80.54% Approval: 75.79% Approval:	Affirmative--10/7/14		

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
1.	N/A	Standards Project Prioritization Reference Document and Tool	Project Prioritization Tool		1/21/11	2/10/11	Yes 2/10/11
2.	Project 2007-23	Project 2007-23 - Violation Severity Levels	VSLs		1/20/11	2/18/11	Yes 2/18/11
3.	N/A	CAN-0015--Draft CAN-0015 Unavailability of NERC Tools	CAN-0015 Unavailability of NERC Tools		2/4/11	2/18/11	Yes 2/18/11
4	N/A	CAN-0016--Draft CAN-0016 CIP-001-1 R1 - Applicability to Non-BES	CAN-0016 CIP-001-1, R1		2/4/11	2/18/11	Yes 2/18/11
5.	N/A	CAN-0018--Draft CAN-0018 FAC-008 R.1.2.1 - Terminal Equipment	CAN-0018 FAC-008, R.1.2.1		2/4/11	2/18/11	Yes 2/18/11
6.	Regional Standard	Regional Reliability Standards - PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		1/10/11	2/24/11	
7.	Project 2007-07	Project 2007-07 - Vegetation Management - FAC-003	FAC-003-2		1/27/11	2/28/11	Yes 2/28/11
8.	N/A	CAN-0017--Draft CAN-0017 CIP-007 R5 System Access and Password Controls	CAN-0017 CIP-007, R5		2/11/11	3/4/11	Yes 3/4/11
9.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1		2/4/11	3/7/11	Yes 3/7/11
10.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	COM-001 COM-002 IRO-001 IRO-014		1/18/11	3/7/11	Yes 3/7/11
11.	NERC RoP	Proposed Changes to Rules of Procedure to Add Section 1700 - Challenges to Determinations	RoP Section 1700		2/14/11	3/7/11	Yes 3/7/11
12.	Project 2009-02	Project 2009-02 - Real-time Reliability Monitoring and Analysis Capabilities	Concept White Paper		2/16/11	4/4/11	Yes 4/4/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
13.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		3/4/11	4/4/11	Yes 4/4/11
14.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		3/9/11	4/8/11	Yes 4/8/11
15.	RFC RoP	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments			3/1/11	4/15/11	
16.	NERC RoP	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Appendices 3B and 3D		3/1/11	4/15/11	Yes 4/15/11
17.	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	CIP-005		3/29/11	4/28/11	Yes 4/27/11
18.	Project 2009-06	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	FAC-008-3		3/17/11	5/2/11	Yes 5/2/11
19.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		4/13/11	5/12/11	Yes 5/9/11
20.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		4/28/11	5/27/11	Yes 5/27/11
21.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	TPL-001-2		4/18/11	5/31/11	Yes 5/31/11
22.	Project 2007-03	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	TOP-001 through TOP-008 and PER-001		4/26/11	6/9/11	Yes 6/9/11
23.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		5/11/11	6/10/11	Yes 6/10/11
24.	NERC RoP	Rules of Procedure Development Team: BES Definition Exception Process	BES Definition Exception Process		5/11/11	6/10/11	Yes 6/10/11
25.	N/A	CAN-0024--Draft CAN-0024 CIP-002 through CIP-009 Routable Protocols and Data Diodes	CAN-0024 CIP-002 through CIP-009		5/20/11	6/10/11	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
26.	N/A	CAN-0029--Draft CAN-0029 PRC-004-1 R1, R2 and R3 Misoperations	CAN-0029 PRC-004-1 R1, R2 and R3		5/20/11	6/10/11	
27.	N/A	CAN-0030--Draft CAN-0030 Attestations	CAN-0030 Attestations		5/20/11	6/10/11	
28.	N/A	CAN-0039--Draft CAN-0039 DOE Form 407	CAN-0039 DOE Form 407		5/20/11	6/10/11	
29.	Project 2010-05.1	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)			6/10/11	7/11/11	
30.	Project 2007-09	Project 2007-09 – Generator Verification – MOD-025-2, MOD-027-1, PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		6/15/11	7/15/11	Yes 7/15/11
31.	Project 2010-07	Project 2010-07 – Generator Requirements at the Transmission Interface – Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards		6/17/11	7/17/11	Yes 7/15/11
32.	Project 2007-09	Project 2007-09 – Generator Verification – MOD-026-1 and PRC-024-1	MOD-026-1 and PRC-024-1		6/15/11	8/1/11	Yes 8/1/11
33.	NERC RoP	Proposed Changes to NERC Rules of Procedure and associated Appendices (Appendix 4B – Sanction Guidelines; and Appendix 4C – Compliance Monitoring and Enforcement Program)	Appendices 4B and 4C		6/30/11	8/15/11	
34.	N/A	Compliance Application Notice (CAN) Process	CAN Process		8/15/11	9/6/11	Yes 9/6/11
35..	N/A	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	CAN-0016 CIP-001, R1		8/15/11	9/6/11	Yes 9/6/11
36.	N/A	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004	CAN-0001 through 0004 Retirement		8/31/11	9/21/11	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
37.	NERC RSDP	NERC 2012-2014 Reliability Standards Development Plan	2012-2014 RSDP		9/12/11	9/26/11	Yes 9/26/11
38.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		8/15/11	9/28/11	Yes 9/28/11
39.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	BES Definition		8/26/11	10/10/11	Yes 10/10/11
40.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Technical Principles for Demonstrating BES Exceptions	Technical Principles for Demonstrating BES Exceptions		8/26/11	10/10/11	Yes 10/10/11
41.	N/A	New CAN Template, five DRAFT CANs for Industry review and CANs Status posted to NERC Compliance's Web site.	CANs		9/23/11	10/14/11	Yes 10/14/11
42.	RoP	Proposed Changes to NERC Rules of Procedure and All Appendices			9/2/11	10/17/11	
43.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests	RoP Section 509, Section 1703 and Appendix 5C		9/13/11	10/27/11	Yes 10/27/11
44.	N/A	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	CAN-0010 Definition of Annual		10/10/11	10/31/11	Yes 10/31/11
45.	N/A	CAN-0011--PRC-005-1 R2: New Equipment	CAN-0011 PRC-005-1 R2		10/10/11	10/31/11	Yes 10/31/11
46.	N/A	CAN-0012--Completion of Periodic Activity Requirements During Implementation Plan	CAN-0012 Completion of Periodic Activity Requirements		10/10/11	10/31/11	Yes 10/31/11
47	N/A	CAN-0013--PRC-023 R1 and R2 Effective Dates for Switch-on-to-Fault Schemes	CAN-0013 PRC-023 R1 and R2		10/10/11	10/31/11	
48.	N/A	CAN-0015--Unavailability of NERC Software Tools	CAN-0015 NERC Tools		10/10/11	10/31/11	Yes 10/31/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
49.	N/A	CAN-0022--VAR-002-1.1b R1 and R3 Generator Operation in Manual Mode	CAN-0022 VAR-002-1.1b R1 and R3		10/10/11	10/31/11	
50.	N/A	CAN-0024--CIP-002 R3 Routable Protocols and Data Diode Devices	CAN-0024 CIP-002, R3		10/10/11	10/31/11	Yes 10/31/11
51.	N/A	CAN-0026--TOP-006 R3 Protection Relays	CAN-0026 TOP-006, R3		10/10/11	10/31/11	Yes 10/31/11
52.	N/A	CAN-0028--TOP-006-1 R1.2 Reporting Responsibilities	CAN-0028 TOP-006-1, R1.2		10/10/11	10/31/11	
53.	N/A	CAN-0020--TPL-002, TPL-003, TPL-004 and TOP-002 Equipment Maintenance Outages	CAN-0020 TPL-002, TPL-003, TPL-004 and TOP-002		10/19/11	11/9/11	
54.	N/A	CAN-0030--Attestations	CAN-0030		10/19/11	11/9/11	
55.	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	MOD-028, R3.1		10/3/11	11/16/11	Yes 11/16/11
56.	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Interpretation of COM-002-2, R2		10/4/11	11/18/11	Yes 11/18/11
57.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		10/5/11	11/18/11	Yes 11/18/11
58.	N/A	Draft Directive Regarding Generator Transmission Leads	Draft Directive #2011 CAG-001		10/17/11	11/18/11	Yes 11/18/11
59.	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 R1.1 by Progress Energy	Interpretation of CIP-006-1, R1.1		10/12/11	11/21/11	Yes 11/21/11
60.	N/A	CAN-0040 - BAL-003 Frequency Bias Calculation			11/2/11	11/23/11	
61.	N/A	CAN-0043 - PRC-005 Protection System Maintenance and Testing Evidence	PRC-005 Evidence		11/2/11	11/23/11	Yes 11/22/11
62.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1			12/8/11	Yes 12/8/11
63.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2			12/12/11	Yes 12/12/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
64.	N/A	Draft CAN-0027: TOP-003 R2 Coordination of Scheduled Outages	CAN-0027 TOP-003, R2		11/22/11	12/14/11	
65.	NERC RoP	Proposed Changes to the NERC Rules of Procedure and Associated Appendices			11/7/11	12/22/11	
66.	NERC RoP	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			11/22/11	12/22/11	
67.	Regional Standard	Regional Reliability Standard PRC-006-NPCC-1 — Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		11/22/11	12/22/11	
68.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 (Version 5 CIP Standards)	Version 5 CIP Standards		11/7/11	1/6/12	Yes 1/6/12
69.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations - TOP-001-2, TOP-002-3 and TOP-003-2	TOP-001-2 TOP-002-3 TOP-003-2		12/14/11	1/12/12	Yes 1/12/12
70.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition, Phase 2		1/4/12	2/3/12	Yes 2/3/12
71.	N/A	Order 754 - Request for Data or Information	Data Request		12/22/11	2/6/12	Yes 2/6/12
72.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001 COM-002 IRO-001-3		1/9/12	2/9/12	Yes 2/8/12
73.	WECC Regional Standard	Regional Reliability Standard BAL-004-WECC-02 - Automatic Time Error Correction	BAL-004-WECC-02		1/23/12	3/9/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
74.	WECC Regional Standard	Regional Reliability Standard BAL-001-0.1a - Real Power Balancing Control Performance - WECC Variance	BAL-001-0.1a		1/23/12	3/9/12	
75.	N/A	NERC Functional Model Demand Response Functions and Entities	NERC Functional Model		2/13/12	3/14/12	
76.	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 for WECC	Interpretation of CIP-004-1		2/8/12	3/23/12	Yes 3/23/12
77.	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Interpretation of CIP-002-1, R3		2/8/12	3/23/12	Yes 3/23/12
78.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		2/8/12	3/23/12	Yes 3/23/12
79.	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing - PRC-005	PRC-005-2		2/28/12	3/28/12	Yes 3/28/12
80.	Project 2007-09	Project 2007-09 Generator Verification - MOD-026-1 and PRC-024-1	MOD-026-1 and PRC-024-1		2/29/12	3/29/12	Yes 3/29/12
81.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - FAC-003-X, FAC-003-3	FAC-003-X FAC-003-3		3/9/12	4/9/12	Yes 4/9/12
82.	Project 2007-09	Project 2007-09 Generator Verification - MOD-025-2, MOD-027-1, and PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		2/29/12	4/16/12	Yes 4/16/12
83.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - PRC-005-1.1a	PRC-005-1.1a		3/2/12	4/16/12	Yes 4/16/12
84.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations	TOP-001 through TOP-008 and PER-001		3/22/12	4/20/12	Yes 4/20/12
85.	Project 2012-INT-02	Request for Interpretation - Project 2012-INT-02 TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		4/24/12	5/4/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
86.	Project 2008-06	Project 2008-06 - Cyber Security Order 706 Version 5 CIP	CIP-002 and CIP-003 - Comment Form A		4/12/12	5/21/12	Yes 5/20/12
			CIP-004 thru CIP-007 - Comment Form B		4/12/12	5/21/12	Yes 5/20/12
			CIP-008 thru CIP-011 - Comment Form C		4/12/12	5/21/12	Yes 5/20/12
			Definitions and Implementation Plan - Comment Form D		4/12/12	5/21/12	Yes 5/20/12
87.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		4/25/12	5/24/12	Yes 5/24/12
88.	Project 2007-12	Project 2007-12 Frequency Response Technical Conferences			5/30/12	6/15/12	
89.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003		5/7/12	6/20/12	Yes 6/20/12
90.	N/A	Adequate Level of Reliability Revised Definition and Associated Documents	Adequate Level of Reliability (ALR)		4/25/12	6/25/12	Yes 6/25/12
91.	N/A	Order 754 - Request for Data or Information	Data Request		5/11/12	6/25/12	Yes 6/25/12
92.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR - 002 for Constellation	Interpretation of VAR -002		5/22/12	6/27/12	Yes 6/27/12
93.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		5/29/12	6/27/12	Yes 6/27/12
94.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserve	BAL-001-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-002-2		6/4/12	7/3/12	Yes 7/3/12
			BAL-012-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-013-1		6/4/12	7/3/12	Yes 7/3/12
95.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		5/21/12	7/5/12	Yes 7/5/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
96.	N/A	Cost Effective Analysis Process (CEAP) for NERC ERO Standards	CEAP		5/7/12	7/6/12	Yes 7/6/12
97.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001, COM-002 and IRO-001-3		6/7/12	7/6/12	Yes 7/6/12
98.	Project 2006-02	Project 2006-02 – Assess Transmission Future Needs and Develop Transmission Plans	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		6/19/12	7/9/12	Yes 7/9/12
99.	N/A	Standard Processes Manual Revisions to Implement SPIG Recommendations	SPIG Reco		6/20/12	7/19/12	Yes 7/19/12
100.	Project 2012-INT-02	Project 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for System Protection and Control Subcommittee	- Interpretation of TPL-003-0a and TPL-004-0		6/20/12	7/20/12	Yes 7/19/12
101.	Project 2012-INT-05	Interpretation of 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		6/27/12	7/27/12	Yes 7/27/12
102.	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision to Address Interpretation of VAR-002 for Constellation	Rapid Revision to VAR-002		7/18/12	7/27/12	Yes 7/26/12
103.	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Rapid Revision of TOP-006		6/14/12	7/30/12	Yes 7/27/12
104.	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Glossary of Terms		6/19/12	8/2/12	Yes 8/2/12
105.	N/A	Reliability Guideline: System Operator Verbal Communications – Current Industry Practices	System Operator Verbal Communications		6/26/12	8/10/12	Yes 8/9/12
106.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		7/27/12	8/27/12	Yes 8/27/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
107.	Project 2010-11	Project 2010-11 - TPL Table 1 Order TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		7/31/12	8/29/12	Yes 8/29/12
108.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs			7/31/12	8/30/12	
109.	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group			7/25/12	9/4/12	
110.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		8/3/12	9/4/12	Yes 9/4/12
111.	Project 2010-05.1	Project 2010-05.1 - Protection Systems: Phase 1 (Misoperations)			7/25/12	9/7/12	Yes 9/7/12
112.	N/A	Definition of Adequate Level of Reliability	Adequate Level of Reliability (ALR)		8/15/12	9/13/12	Yes 9/13/12
113.	N/A	2013-2015 Reliability Standards Development Plan	2013-2015 RSDP		8/17/12	9/18/12	Yes 9/18/12
114.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols	COM-003-1		8/22/12	9/20/12	Yes 9/20/12
115.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		8/29/12	9/27/12	
116.	SPP Regional Standard	Regional Reliability Standard PRC-006-SPP-01 Automatic Underfrequency Load Shedding	PRC-006-SPP-01		8/15/12	9/28/12	
117.	Project 2008-06 Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		9/11/12	10/10/12	Yes 10/10/12
			RSAW		9/11/12	10/10/12	Yes 10/10/12
118.	MRO SPM	Regional Reliability Standards - MRO Standards Process Manual			8/28/12	10/11/12	
119.	N/A	Standard Process Manual Revisions to Implement SPIG Recommendations	SPIG Reco		8/29/12	10/12/12	Yes 10/10/12
120.		Revisions to Outstanding VRFs and VSLs			9/5/12	10/19/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
121.	Project 2013-01	Project 2013-01 - Cold Weather Preparedness			9/25/12	10/24/12	
122.	Project 2007-09	Project 2007-09 - Generator Verification			9/28/12	10/29/12	
123.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System			10/4/12	11/5/12	
124.	2007-12	Project 2007-12 - Frequency Response			10/5/12	11/7/12	
125.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		10/26/12	11/7/12	
126.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025		10/5/12	11/7/12	
127.	N/A	IRO-006-WECC-2			10/3/12	11/16/12	
128.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B			10/5/12	11/19/12	
129.	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		10/22/12	12/5/12	Yes 12/5/12
130.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		10/25/12	12/10/12	Yes 12/10/12
131.	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	- Interpretation of CIP-003-3		11/9/12	12/10/12	Yes 12/10/12
132.	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	- Interpretation of CIP-007-3		11/9/12	12/10/12	Yes 12/10/12
133.	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols - RSAW	COM-003-1		11/14/12	12/13/12	Yes 12/13/12
			COM-003-1 RSAW		11/14/12	12/13/12	Yes 12/13/12
134.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		11/16/12	12/17/12	Yes 12/17/12
135.	Project 2012-INT-05	Project 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		11/6/12	12/20/12	Yes 12/20/12
136.	N/A	Standard Processes Manual to Implement SPIG Revisions	SPIG Reco		11/21/12	12/20/12	Yes 12/20/12
137.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		12/10/12	1/11/13	Yes 1/11/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
138.	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	PRC-024-1		12/12/12	1/11/13	Yes 1/11/13
139.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-012-1	BAL-012-1		11/30/12	1/14/13	Yes 1/14/13
140.	N/A	Reliability Guideline--Draft Generating Unit Winter Weather Readiness - Current Industry Practices			12/20/12	2/4/13	Yes 2/4/13
141.	Project 2010-05-1	Project 2010-05-1 Protection System Misoperations					Yes 2/20/13
142.	Project 2007-09	Project 2007-09 Generator Verification - PRC-024-1	PRC-024-1	Formal	1/25/13	2/25/13	Yes 2/25/13
143.	N/A	Rapid Revision Procedure		Informal	2/25/13	3/6/13	Yes 3/6/13
144.	Project 2010-13-2	Project 2010-13-2 - Phase 2 of Relay Loadability - Generation - PRC-025-1	PRC-025-1	Formal	1/25/13	3/11/13	Yes 3/11/13
			Supplemental SAR	Informal	1/25/13	3/11/13	Yes 3/11/13
			Cost Effectiveness	CEAP Pilot	1/25/13	3/11/13	Yes 3/11/13
			RSAW	Feedback	1/25/13	3/11/13	Yes 3/11/13
145.	Project 2012-INT-04	Interpretation 2012-INT-04 - Interpretation of CIP-007 for ITC	Interpretation of CIP-007	Formal	2/6/13	3/22/13	Yes 3/22/13
146.	Project 2012-INT-06	Interpretation 2012-INT-06 - Interpretation of CIP-003 for Consumers Energy	Interpretation of CIP-003	Formal	2/6/13	3/22/13	Yes 3/22/13
147.	Project 2012-08-1	Project 2012-08-1 - Phase 1 of Glossary Updates--Statutory Definitions	Glossary of Terms	Formal	2/21/13	3/22/13	Yes 3/22/13
148.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003-1	COM-003-1	Formal	3/7/13	4/5/13	Yes 4/5/13
			RSAW	Feedback	3/7/13	4/5/13	Yes 4/5/13
149.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-001-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-002-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-013-1	Formal	3/12/13	4/25/13	Yes 4/25/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
150.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays)	Draft SAR	Informal	4/5/13	5/6/13	Yes 5/6/13
			PRC-005-3	Formal	4/5/13	5/6/13	Yes 5/613
151.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation	PRC-023-3 PRC-025-1	Formal	4/25/13	5/24/13	Yes 5/24/13
152.	Project 2007-11	Project 2007-11 - Disturbance Monitoring — PRC-002 and PRC-018	SAR	Informal	5/03/13	6/03/13	Yes 6/3/13
153.	Project 2007-11	Project 2007-11 - Disturbance Monitoring PRC-002 and PRC-018	Request for Information	Informal	6/05/13	7/05/13	
154.	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	PRC-001 and PRC-027		6/04/13	7/03/13	Yes 7/03/13
155.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition		5/29/13	7/12/13	Yes 7/12/13
156.	TRE Regional Standard	Regional Reliability Standard - BAL-001-TRE-01	BAL-001-TRE-01		5/31/13	7/15/13	
157.	N/A	NPCC Regional Standards Process Manual	NPCC RSPM		6/06/13	7/22/13	
158.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003-1		6/20/13	7/19/13	Yes 7/19/13
159.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025-1		6/20/13	7/19/13	Yes 7/19/13
160.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023	PRC-023-3	Formal	6/20/13	8/05/13	Yes 8/5/13
161.	N/A	SPP RE Regional Standards Process Manual	SPP RSPM		6/26/13	8/09/13	
162.	Project 2013-03	Project 2013-03 - Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	6/27/13	8/12/13	Yes 8/12/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
163.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005	PRC-005-3	Formal	7/10/13	8/23/13	Yes 8/23/13
164.	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards	INT-004-3 INT-006-4 INT-009-2 INT-010-2 INT-011-1	Informal	7/25/13	8/23/13	Yes 8/23/13
165.	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	MOD-001-2	Formal	7/11/13	8/26/13	Yes 8/26/13
166.	Project 2010-01	Project 2010-01 - Training - PER-005-2	PER-005-2	Formal	7/19/13	9/03/13	Yes 9/3/13
167.	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-001-4 VAR-002-3	Formal	7/19/13	9/03/13	Yes 9/3/13
168	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	MOD-032-1 MOD-033-1	Formal	7/22/13	9/04/13	Yes 9/4/13
169.	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	7/22/13	9/04/13	Yes 9/4/13
170	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System – Phase 2	BES Definition Phase 2	Formal	8/6/13	9/4/13	Yes 9/4/13
171	Project 2012-13	Project 2012-13 - NUC Five-Year Review	NUC-001-2	5-year review	7/26/13	9/9/13	Yes 9/9/13
172	2014-2016 RSDP	2014-2016 Reliability Standards Development Plan	Reliability Standards Development Plan	Annual Review	8/30/13	9/13/13	Yes 9/13/13
173	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-001-1 FAC-002-1	5-year review	8/1/13	9/16/13	Yes 9/16/13
174	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-003-3 FAC-008-3 FAC-010-2.1 FAC-011-2 FAC-013-2 FAC-014-2	5-year review	8/1/13	9/16/13	Yes 9/16/13
175	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	BAL-002-2	Formal	8/2/13	9/16/13	Yes 9/16/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
176	Project 2009-03	Project 2009-03 — Five-Year Review of Emergency Operations EOP-001, EOP-002, EOP-003, and IRO-001	EOP-001-2.1b EOP-002-3.1 EOP-003-2	5-year review	8/6/13	9/19/13	Yes 9/19/13
177	Project 2012-09	Project 2012-09 IRO Five-Year Review	IRO-003-2 IRO-004-2 IRO-005-4 IRO-006-5 IRO-006-East IRO-008-1 IRO-009-1 IRO-010-1a	5-year review	8/7/13	9/20/13	Yes 9/20/13
178	Project 2008-02	Project 2008-02 Undervoltage Load Shedding	Revised SAR	Informal	9/10/13	10/9/13	Yes 10/9/13
179	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	9/4/13	10/18/13	Yes 10/18/13
180	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition	Formal	9/27/13	10/28/13	Yes 10/28/13
181	Project 2007-02	Project 2007-02 Operating Personnel Communications Protocols	COM-002-4	Formal	10/21/13	11/7/13	Yes 11/4/13
182	Project 2010-01	Project 2010-01 Training	PER-005-2	Formal	9/27/13	11/12/13	Yes 11/12/13
183	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	Various INT Standards	Formal	9/30/13	11/13/13	Yes 11/13/13
184	Project 2012-05	Project 2012-05 ATC Revisions (MOD A)	MOD-001-2	Formal	10/4/13	11/20/13	Yes 11/18/13
185	Project 2010-03	Project 2010-03 Modeling Data (MOD B)	MOD-032-1, MOD-033-1	Formal	10/07/13	11/20/13	
186	Project 2010-04	Project 2010-04 Demand Data (MOD C)	MOD-031-1	Formal	10/09/13	11/22/13	Yes 11/22/13
187	Project 2013-04	Project 2013-04 Voltage and Reactive Control	VAR-001-4, VAR-002-3	Formal	10/11/13	11/25/13	Yes 11/25/13
188	Project 2009-03	Project 2009-03 Emergency Operations	SAR	Informal	11/06/13	12/05/13	Yes 12/5/13
189	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-002-2	Formal	10/28/13	12/11/13	Yes 12/11/13
190	Project 2007-11	Project 2007-11 - Disturbance Monitoring	PRC-002-2	Formal	11/01/13	12/16/13	Yes 12/16/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
191	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-027	Formal	11/04/13	12/18/13	Yes 12/18/13
192	Project 2014-01	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	SAR	Formal	11/20/13	12/19/13	Yes 12/19/13
193	Project 2010-01	Project 2010-01 Training - PER-005-2	PER-005-2	Formal	12/4/13	1/22/14	Yes 1/17/14
194	Project 2010-03	Project 2010-03 Modeling Date - MOD B	MOD-033-1	Formal	12/6/13	1/22/14	Yes 1/21/14
195	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	INT-004-3 INT-010-2	Formal	1/10/14	1/24/14	Yes 1/22/14
196	Project 2007-02	Project 2007-02 Operating Personnel	COM-002-4	Formal	1/22/14	1/31/14	Yes 1/31/14
197	Project 2014-02	Project 2014-02 Standard Authorization Request – Cyber Security Standards	CIP SAR	Informal	1/17/14	2/18/14	Yes 2/18/14
198	2014 Work Plan	2014 Work Plan for NERC Reliability Standards Development	2014 Work plan			2/21/13	Yes 2/21/14
199	Project 2010-17	Project 2010-17 Definition of Bulk Electric System - Phase 2	BES	Informal	1/29/14	2/27/14	Yes 2/27/14
200	Project 2010-05.1	Project 2010-05.1 Protection System: Phase 1 (Misoperations) - PRC-004-3	PRC-004-3	Formal	1/17/14	3/11/14	Yes 3/2/14
201	Project 2012-13	Project 2012-13 NUC-Nuclear Plant Interface Coordination Standard Authorization Request	NUC-001-2.1 SAR	Informal	2/12/14	3/13/14	Yes 3/13/14
202	Project 2010-05.2	Project 2010-05.2 Special Protection Systems (Phase 2 of Protection Systems) - SAR	SAR	Informal	2/18/14	3/19/14	Yes 3/19/14
203	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	SAR	Formal	02/21/14	03/24/14	Yes 3/24/14
204	Project 2014-03	Technical Conferences on Revisions to TOP/IRO Reliability Standards	Technical Conference Topics	Informal	03/11/14	03/24/14	
205	Project 2014-04	Project 2014-04 - Physical Security	SAR	Informal	03/21/14	03/28/14	Yes 3/28/14

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
206	Project 2010-14.2	Project 2010-14.2 - Periodic Review of BAL Standards	Reco to Revise BAL-005 and BAL-006	Formal	02/21/14	04/07/14	
207	2010-05.2	Project 2010-05.2 - Phase 2 of Protection Systems - Revised Definition of Special Protection System	SPS Definition	Informal	03/11/14	04/09/14	Yes 4/9/14
208	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	02/25/14	04/10/14	Yes 4/10/14
209	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-002-3	Formal	02/27/14	04/14/14	Yes 4/14/14
210	Project 2008-02	Project 2008-02 - Undervoltage Load Shedding - PRC-010, PRC-020, PRC-021 and PRC-022	PRC-010-1	Informal	03/17/14	04/16/14	Yes 4/16/14
211	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	CIP-014-1	Formal	04/10/14	04/24/14	Yes 4/24/14
212	Project 2009-03	Project 2009-03 Emergency Operations – EOP-011-1	EOP-011-1	Informal	03/28/14	04/28/14	Yes 4/28/14
213	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-005-2(X) PRC-005-3(X) PRC-005-X(X) VAR-002-2b(X) VAR-002-4	Formal	04/17/14	05/05/14	Yes 5/5/14
214	Project 2010-02	Project 2010-02 – Connecting New Facilities to the Grid	FAC-001-1 FAC-002-1	Formal	04/01/14	05/15/14	Yes 5/15/14
215	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	TPL-007-1	Informal	04/22/14	05/21/14	Yes 5/21/14
216	Project 2012-13	Project 2012-13 Nuclear Plant Interface Coordination	NUC-001-3	Formal	04/08/14	05/22/14	Yes 5/22/14
217	Project 2007-17.3	Project 2007-17.3 Protection System Maintenance and Testing – Phase 3 (Sudden Pressure Relays)	PRC-005-X	Formal	04/17/14	06/03/14	Yes 6/3/14
218	Project 2010-13.3	Project 2010-13.3 Relay Loadability: Stable Power Swings	PRC-026-1	Formal	04/25/14	06/09/14	Yes 6/9/14
219	Project 2007-11	Project 2007-11 Disturbance Monitoring	PRC-002-2	Formal	05/09/14	06/25/14	Yes 6/25/14

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
221	Project 2008-02	Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding	PRC-010 PRC-020 PRC-021 PRC-022	Informal	05/23/14	06/23/14	Yes 6/23/14
222	Project 2010-05-1	Project 2010-05-1 Protection System – Phase 1 – Misoperations	PRC-004	Formal	05/16/14	07/09/14	Yes 7/9/14
223	Project 2014-03	Project 2014-03 Revisions to TOP-IRO Reliability Standards	TOP-001-3 TOP-002-4 TOP-003-3 IRO-001-4 IRO-002-4 IRO-008-2 IRO-010-2 IRO-014-3 IRO-017-1	Formal	05/19/14	07/02/14	Yes 7/2/14
224	Project 2014-02	Project 2014-02 CIP Version 5 Revisions – Cyber Security Standards	CIP-002 to CIP-011	Formal	06/02/14	07/17/14	Yes 7/16/14
225	Project 2015-2017	Project 2015-2017 Reliability Standard Development Plan		Informal		7/21/14	Yes 7/21/14
226	2010-05.2	Project 2010-05.2 - Phase 2 of Protection Systems - Revised Definition of Special Protection System	SPS Definition	Formal	7/16/14	7/25/14	Yes 7/25/14
227	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-005-2(X) PRC-005-3(X) PRC-005-X(X) VAR-002-2b(X) VAR-002-4	Formal	06/12/14	7/29/14	Yes 7/29/14
228	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	TPL-007-1	Formal	06/13/14	07/30/14	Yes 7/30/14
229	Project 2008-02	Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding	PRC-010 PRC-020 PRC-021 PRC-022	Formal	06/23/14	08/8/14	Yes 8/6/14
230	Project 2010-14-2	Project 2010-14-2 Balancing Authority Reliability-based Control Standard Authorization Request	BAL-005 BAL-006	Informal	07/16/14	08/14/14	Yes 8/12/14

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
		for BAL-005 and BAL-006					
231	Project 2009-03	Project 2009-03 Emergency Operations – EOP-011-1	EOP-011-1	Formal	07/2/14	08/15/14	Yes 8/13/14
232	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	PRC-004-2.1a(X) PRC-004-3(X)	Formal	07/10/14	08/26/14	Yes 8/25/14
233	Project 2007-17.3	Project 2007-17.3 Protection System Maintenance and Testing – Phase 3 (Sudden Pressure Relays) – PRC-005-X	PRC-005-X	Formal	07/30/14	09/12/14	Yes 9/12/14
234	Project 2014-03	Project 2014-03 Revisions to TOP-IRO Reliability Standards	TOP-001-3 TOP-002-4 TOP-003-3 IRO-001-4 IRO-002-4 IRO-008-2 IRO-010-2 IRO-014-3 IRO-017-1	Formal	08/6/14	09/19/14	Yes 9/22/14
235	Project 2010-14.1	Project 2010-14.1 Balancing Authority Reliability-based Control	BAL-002-2	Formal	08/19/14	10/03/14	Yes 10/2/14
236	Project 2010-13.3	Project 2010-13.3 – Relay Loadability: Stable Power Swings	PRC-026-1	Formal	09/26/14	10/06/14	Yes 10/6/14
237	Project 2008-02	Project 2008-02: Underfrequency Load Shedding (UFLS)	PRC-006-2	Formal	08/21/14	10/08/14	Yes 10/7/14
238	Project 2013-03	Project 2013-03: Geomagnetic Disturbance Mitigation	TPL-007-1	Formal	08/27/14	10/10/14	Yes 10/10/14
239	NERC Rules of Procedure	NERC Rules of Procedure	NERC Rules of Procedure	Formal	08/26/14	10/10/14	Yes 10/14/14
240	Project 2010-05.2	Project 2010-05.2 – Special Protection Systems Phase 2 of Protection Systems	RAS Definition	Formal	08/29/14	10/14/14	Yes 10/14/14
241	Project 2014-01	Project 2014-01 Standards Applicability for Dispersed Generation Resources	VAR-002-2b(X) VAR-002-4	Formal	08/27/14	10/16/14	Yes 10/16/14
242	Project 2014-02	Project 2014-02 CIP Version 5 Revisions – Cyber Security Standards	CIP-003-6 CIP-010-2 CIP-003-X CIP-004-X	Formal	09/03/14	10/17/14	Yes 10/17/14

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
			CIP-007-X CIP-010-X CIP-011-X				
243	Project 2009-03	Project 2009-03 Emergency Operations	EOP-011-1	Formal	09/05/14	10/20/14	Yes 10/20/14
244	Project 2007-06	Project 2007-06 System Protection Coordination PRC-027-1 (Preliminary Draft 5)	PRC-027-1	Informal	10/01/14	10/21/14	Yes 10/21/14
245	Project 2007-11	Project 2007-11 Disturbance Monitoring	PRC-002-2	Formal	09/05/14	10/21/14	Yes 10/21/14
246	Project 2014-01	Project 2014-01 Applicability for Dispersed Generation	PRC-004-2.1a(X) PRC-004-4	Formal	09/05/14	10/22/14	Yes 10/22/14
247	Project 2014-03	Project 2014-03 Revisions to TOP/IRO Reliability Standards TOP-001-3	TOP-001-3	Formal	10/10/14	11/10/14	Yes 11/10/14
248	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation TPL-007-1	TPL-007-1	Formal	10/28/14	11/21/14	Yes 11/24/14
249	Project 2010-13.3	Project 2010-13.3 – Relay Loadability: Stable Power Swings	PRC-026-1	Formal	11/04/14	11/24/14	Yes 11/25/14
250							
251							
252							
253							
254							
255							
256							

Note: RSC past comment forms are posted on the NPCC Website under "Standards - Regional Standards Comments."

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC Regional Standards Process Manager, NPCCstandard@npcc.org . The NPCC Regional Standards Process Manager shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:
Request Date:

RSAR Requester Information

Name:	**RSAR Type (Check box for one of these selections.)**	
Company:	☐	New Standard
Telephone:	☐	Revision to Existing Standard
Fax:	☐	Withdrawal of Existing Standard
Email:	☐	Urgent Action

Purpose (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.**)**
Industry Need (Provide a detailed statement justifying the need for the proposed standard, along with any supporting documentation**.)**
Brief Description (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.**)**

Reliability Functions

The Standard will Apply to the Following Functions (Check all applicable boxes.)		
☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission	The entity responsible for the reliability of its "local" transmission system,

	Operator	and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.
☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected bulk power 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 power 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 power 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 power 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 power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

☐	7. The security of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
Recognizing that reliability is an Common Attribute of a robust North American economy:
1. A reliability standard shall not give any market participant an unfair competitive advantage.Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability 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 a standard based on this description.)

Related Standards

Standard No.	**Explanation**

Related SARs or RSARs

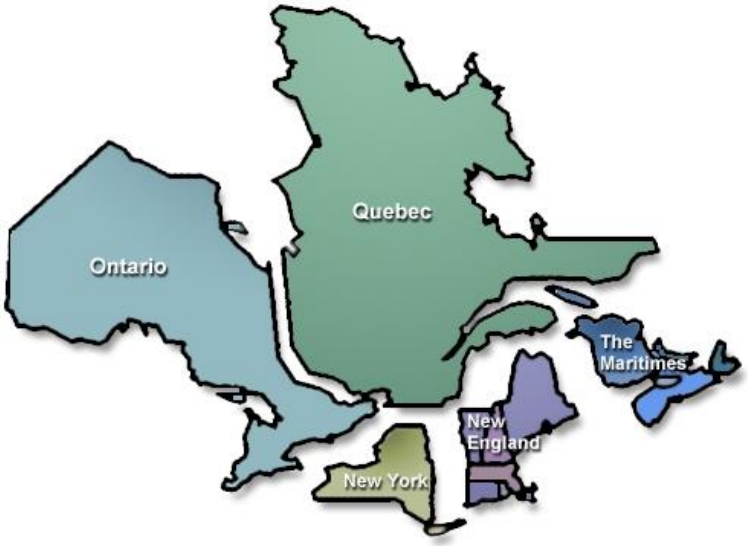
SAR ID	**Explanation**

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Northeast Power Coordinating Council, Inc.

Regional Reliability Standards Development Procedure



Approved by NPCC Board of Directors
September 19, 2007
Approved by NERC BOT October 23, 2007
Adopted by FERC March 21, 2008

NPCC

REGIONAL RELIABILITY STANDARDS DEVELOPMENT PROCEDURE

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. REGIONAL RELIABILITY STANDARD DEVELOPMENT PROCEDURE

1. CHARACTERISTIC ATTRIBUTES 2
2. ELEMENTS OF A REGIONAL STANDARD 5
3. TERMS AND FUNCTIONS 8
4. PROCEDURE DESCRIPTION 10
5. FLOWCHART 15
6. ERO AND REGULATORY APPROVALS 16
7. APPEALS 16

III. APPENDIX

A) RSAR FORM 19

I. EXECUTIVE SUMMARY

The purpose of the Northeast Power Coordinating Council, Inc. ("NPCC"), is to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of more stringent and specific regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards pursuant to the execution and implementation of a Regional Delegation Agreement with the Electric Reliability Organization ("ERO") and applicable Canadian Memoranda of Understanding that are backstopped by the Federal Energy Regulatory Commission ("FERC") and Canadian Provincial authorities. In the development and enforcement of Regional Reliability Standards, NPCC, to the extent possible, facilitates attainment of fair, effective, efficient, and competitive electric markets.

General Membership in NPCC is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the ERO that has an interest in the reliable operation of the Northeastern North American bulk power system.

The NPCC Regional Reliability Standards Development Procedure describes the procedures, policies and practices implemented to ensure an "open, fair, and inclusive" process for the transparent initiation, development, implementation and revision of NPCC Regional Reliability Standards necessary for the reliable operation of the international and interconnected bulk power system in Northeast North America. These Standards will, in all cases, not be inconsistent with or less stringent than any requirements of the North American Electric Reliability Council/Electric Reliability Organization (NERC/ERO) Reliability Standards. The procedure will not unnecessarily delay the development of the proposed reliability standards. Each regional reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of pertinent reliability principles and criteria, thereby ensuring that no standard undermines reliability through an unintended consequence.

II. REGIONAL RELIABILITY STANDARD DEVELOPMENT PROCEDURE

1. CHARACTERISTIC ATTRIBUTES

The NPCC Regional Reliability Standards Development Procedure is:

- **Open** — The NPCC Regional Reliability Standards Development Procedure provides any person the ability to participate in the development of a standard. Any entity that is directly and materially affected by the reliability of the NPCC's bulk power system has the ability to participate in the development and approval of reliability standards. There are no undue financial barriers to participation. Participation in the open comment process is not conditional upon membership in the ERO, NPCC or any organization, and participation is not unreasonably restricted on the basis of technical qualifications or other such requirements. NPCC utilizes a website to accomplish this. Online posting and review of standards and the real time sharing of comments uploaded to the website allow complete transparency.

- **Inclusive** — The NPCC Regional Reliability Standards Development Procedure provides any person with a direct and material interest the right to participate by expressing an opinion and its basis, have that position considered, and appealed through an established appeals process if adversely affected.

- **Balanced** — The NPCC Regional Reliability Standards Development Procedure has a balance of interests and all those entities that are directly and materially affected by the reliability of the NPCC's bulk power system are welcome to participate and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter. This will be accomplished through the NPCC Bylaws defining eight sectors (categories) for voting.

- **Fair Due Process** — The NPCC Regional Reliability Standards Development Procedure provides for reasonable notice and opportunity for public comment. The procedure includes public notice of the intent to develop a standard, a 45 calendar day public comment period on the proposed standard request, or standard with due consideration of those public comments, and responses to those comments will be posted on the NPCC website. A final draft will be posted for a 30 calendar day pre-balloting period, and then a ballot of NPCC Members will be conducted. Upon approval by the NPCC Members, the NPCC Board then votes to approve submittal of the Regional Standard to NERC.

- **Transparent** — All actions material to the development of Regional Reliability Standards are transparent and information regarding the progress is posted on the NPCC website as well as through extensive email lists.

In as much as NPCC is one of several regional entities within the Eastern Interconnection of North America, there will be **no** *presumption of validity* by the ERO for any NPCC Regional Reliability Standard. In order to receive the approval of the ERO, the NPCC Reliability Standards Development Process must also achieve the following objectives:

- **No Adverse Impact on Reliability of the Interconnection** —An NPCC Regional Reliability Standard provides a level of bulk power system reliability that is necessary and adequate to protect public health, safety, welfare, and North American security and will not have an adverse impact on the reliability of the Interconnection or other Regions within the Interconnection.

- **Justifiable Difference** — An NPCC Regional Reliability Standard is based on justifiable differences between Regions, such as different electrical systems or facilities, sensitivity of load to disruptions, sensitivity of generation to disruptions, frequency and voltage sensitivity, system operating limit development and facilities ratings process, electrical system interactions, etc.

- **Uniformity**- NPCC Regional Reliability Standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk

power system of the North American continent. A NPCC Reliability Standard shall be more stringent than a continent-wide reliability standard, may include a regional variation that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the northeast's bulk power system, where the interpretation of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

- **No Undue Adverse Impact on Commerce** — An NPCC Regional Reliability Standard will not cause any undue adverse impact on business activities that are not necessary for reliability of the Region and its interconnected Regions. All regional reliability standards shall be consistent with NERC's market principles.

Other Attributes of the NPCC Regional Reliability Standards Development Procedure include;

- **Maintenance of Regional Reliability Standards-**NPCC Regional Standards will be reviewed for possible revision at least every three years and follow the same process as a new standard. The old standard will remain in place until such time as the revised version has passed through the entire process, at which point the old standard will be retired in accordance with any applicable new implementation plan associated with the approved revised standard. The review process shall be conducted by soliciting comments from the stakeholders and through open posting on the NPCC website. If no changes are warranted, Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or withdraw a standard, a regional standard authorization request shall be prepared by the RSC and submitted in accordance with the standards development process contained in this procedure.

- **Maintenance of Regional Reliability Standards Development Procedure-** This NPCC Regional Reliability Standards Development Procedure will be reviewed for possible revision at least once every five years or more frequently if needed and subject to the same procedure as that of the development of a standard. All such revisions shall be subject to approval by the NPCC Board, NERC, FERC, and could be subject to approval, if required, by applicable authorities in Canada. The NPCC RSC has the authority to make non-substantive changes to this procedure and subsequently notify the NPCC Board for their concurrence at their next scheduled meeting.

- **Interpretation of Standards-** All persons who are directly and materially affected by the NPCC's bulk power system reliability shall be permitted to request an interpretation of a standard. The person requesting an interpretation will send an email request to the Regional Standards Process Manager (RSPM), as noted on the NPCC website, explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material

impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard. The RSPM along with guidance from the RSC will forward the request to the originating Task Force which acted as the drafting team for that regional reliability standard. The Task Force will address, through a written response, the request for clarification as soon as practical, but not more than 45 business days from its receipt by the Task Force. This written interpretation will be posted along with the final approved and adopted standard and will stand until such time as the standard is revised through the normal RSAR process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.

2. ELEMENTS OF A RELIABILITY STANDARD

- **Elements of a Regional Reliability Standard**
  To ensure uniformity of regional reliability standards, a regional reliability standard shall consist of the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of standards. This discipline is necessary to achieving standards that are measurable, enforceable, and consistent.

  All mandatory requirements of a regional reliability standard shall be within the standard document. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself.

  The most current version of the approved NERC Reliability Standard template and its associated elements as or if applicable, will be used at the time of the development of the NPCC Regional Reliability Standard to ensure all essential elements are contained therein to achieve consistency and uniformity and meet all statutory requirements. A sample of the elements contained in the standard appears in Table 1 below, however the latest ERO Board approved Standard template, that may be found on the NERC website, will supersede the list below at the time the regional standard is developed.

Table 1- Elements of a Regional Reliability Standard

Identification Number	A unique identification number assigned in accordance with an administrative classification system to facilitate tracking and reference. (i.e. "NPCC- BAL-002-0-Date" which refers to NPCC Regional Standard, referencing NERC BAL-002 Version 0, with NPCC Effective Date-final adoption by all Regional Authorities)
Title	A brief, descriptive phrase identifying the topic of the standard.
Applicability	Clear identification of the functional classes of entities responsible for complying with the standard, noting any specific additions or exceptions. The standard will be applicable to the Bulk Power System unless otherwise noted.
Effective Date	The effective date of the standard or, prior to approval of the

and Status	standard, the proposed effective date.
Purpose	The purpose of the standard. The purpose shall explicitly state what outcome will be achieved or is expected by this standard.
Requirement(s)	Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Each statement in the requirements section shall be a statement for which compliance is mandatory.
Risk Factor(s)	The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below: A High Risk Factor requirement (a) is one that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, 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, or could hinder restoration to a normal condition. A Medium Risk Factor requirement (a) is a requirement that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk power system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. A Lower Risk Factor 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.

Measure(s)	Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.

Table 2 — Compliance Elements of a Regional Reliability Standard

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible for providing the data or information for measuring performance or outcomes. • The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating data or information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Measurement data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Supporting Information Elements

Interpretation	Any interpretation of regional reliability standard that is developed and approved in accordance with the "Interpretation of Standards" section of Appendix A of this procedure, to expound on the application of the standard for unusual or unique situations or to provide clarifications.
Implementation Plan	Each regional reliability standard shall have an associated implementation plan describing the effective date of the standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the standard in the compliance program and other considerations in the initial use of the standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and is approved as part of the ballot of the standard.

Supporting References	This section references related documents that support reasons for, or otherwise provide additional information related to the regional reliability standard. Examples include, but are not limited to: • Glossary of terms • Developmental history of the standard and prior versions • Notes pertaining to implementation or compliance • Standard references • Standard supplements • Procedures • Practices • Training references • Technical references • White papers • Internet links to related information

3. TERMS AND FUNCTIONS

- **Regional Standards Committee (RSC)**—An NPCC committee charged with management of the NPCC Standards Procedure under a sector based voting structure as described in the NPCC Bylaws. The NPCC RSC will consider requests for new or revised standards and be available for advisement to the NPCC Board on the standards.

  The RSC may not itself modify the standard without issuing a new notice to stakeholders regarding a vote of the modified standard. Any RSC action will only be activated in the event of a minor correction of a standard such as errata.

  The RSC is an open and balanced stakeholder committee inclusive of all stakeholder interests that provide for or are materially impacted by the reliability of the bulk power system.

  The RSC disposition regarding the regional standard authorization request, which will in all cases be within 60 calendar days of receipt of a completed standard request, shall include:

  - Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The RSC may, at its discretion, expand or narrow the scope of the standard request under consideration. The RSC shall prioritize the development of standards in relation to other proposed standards, as may be required based on the volume of requests and resources.

- Reject the standard request. If the RSC rejects a standard request, a written explanation for rejection will be delivered to the requester within 30 calendar days of the decision.
- Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the RSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the RSC.

The NPCC Standard Process responsibilities of the RSC will include:

- Review of NPCC Draft Standards for such factors as completeness, sufficient detail, rational result, and compatibility with existing standards; clarifying standard development issues not specified in this procedure. Under no circumstance will the RSC change the substance of a draft standard.
- Due consideration to the work of the drafting team as well as the comments of stakeholders and minority objections, in approving a proposed regional reliability standard to go to ballot.
- Approve standards for pre-ballot posting under a sector based voting structure as described later in the NPCC ~~Inc.~~ Bylaws or
- Remand the standard back to the Task Force acting as the drafting team for further work or recommend a change in those participating in the drafting team (i.e. a new drafting team).

- **Regional Standards Process Manager (RSPM) -** The Regional Reliability Standards Procedure shall be administered by a NPCC staff Regional Standards Process Manager. The RSPM is responsible for ensuring that the development and revision of standards is in accordance with this manual. The RSPM works to ensure the integrity of the process, format, consistency of quality, and completeness of the reliability standards. The RSPM facilitates all steps in the process.

- **Reliability Coordinating Committee (RCC)** —The RCC, will support the standards development process through the assignment of NPCC Task Forces. They will also provide a technical advisory role in the Regional Reliability Standards development procedure through recommendations.

- **Requester**— A Requester is any individual or an entity (organization, company, government authority, etc.) that submits a complete request for development, revision, or withdrawal of a standard. Any person or an entity that is directly and materially affected by an existing standard or the need for a new standard may submit a request for a new standard or revision to a standard. The Requester is assisted by the RSAR drafting team (if one is appointed by the RSC) to respond to comments and to decide if and when the RSAR is forwarded to the RSC with a request to draft a standard. The Requester is responsible for the RSAR, assisted by the RSAR drafting team and Regional Standards Process Manager, until such time the RSC authorizes

development of the standard. The Requester has the option at any time to allow the RSAR drafting team to assume full responsibility for the RSAR. The Requester may chose to participate in subsequent standard drafting efforts related to the RSAR.

- **Task Forces and Working Groups,**—The committees, task forces and working groups within NPCC , serve an active role in the standards process:
  - Identify the need for new or modified regional standards.
  - Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs).
  - Develop comments (views and objections) to standards actions.
  - Participate in NPCC Standard drafting.
  - Provide technical oversight in response to changing industry conditions and ERO Requirements.
  - Conduct Field Tests as required

4. PROCEDURE DESCRIPTION

STEPS 1 AND 2: REQUEST TO DEVELOP A NEW REGIONAL STANDARD

Requests to develop a new Regional Reliability Standard shall be submitted to the RSPM by completing a **Regional Standard Authorization Request** (RSAR) ***(see Appendix A)***. The RSAR is a description of the new or revised standard in sufficient detail to clearly define the scope, purpose, and importance of the Regional Standard, impacted parties or other relevant information. A "needs" statement will provide the justification for the development of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard. The RSPM shall maintain the RSAR form and make it available electronically on the NPCC website.

Any person or entity ("Requester") directly or materially affected by an existing standard or the need for a new or revised standard may initiate a RSAR.

The Requester will submit the RSAR to the RSPM electronically and the RSPM will acknowledge receipt of the RSAR immediately, through electronic receipt. The RSAR, as a minimum, needs to contain the following information in order to be qualified for consideration. The NPCC RSPM will assist the Requester to ensure all the following information is submitted (on the RSAR) in a form appearing in Appendix A:

1. Proposed Title and Date of New RSAR
2. Requester's Name and Contact Information
3. Purpose of the Regional Standard
4. Description of Industry Need
5. Provide a Brief Description of the Standard
6. Identification of the Entities in the Functional Model as being responsible to adhere to the standard.
7. Necessary information to assist the drafting the team, to the extent feasible, to allow them to draft the standard.
8. A cross references to existing NPCC or NERC documents

The RSPM shall forward all properly completed RSARs to the RSC. The RSC shall meet at established intervals to review all pending RSARs. The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for RSC action more than 60 calendar days from the date of receipt. The RSC may take one of the following actions:

- Remand the RSAR back to the RSPM for additional work. In this case, the RSPM may request additional information or clarification for the RSAR from the Requester.
- Accept the RSAR as a candidate for a new or revised standard. In this case, the RSC will forward the RSAR to the RCC to assign a NPCC Task Force to provide technical support and analysis of comments for that RSAR, and assist the Requester and the RSPM in the remaining steps of the process. The RSPM shall post notification of intent to develop a standard on both NPCC and ERO websites within 30 calendar days of acceptance.
- Reject the RSAR. In this case, the RSC will provide a written explanation for rejection to the Requester within 30 calendar days of the rejection decision.

STEPS 3, 4, AND 5: RSC ACCEPTS RSAR AND RCC ASSIGNS TF TO DRAFT NEW OR REVISED STANDARD

A RSAR that is accepted by the RSC will be submitted to the RCC. Within 60 calendar days the RCC shall assign the development of the standard to a Task Force Drafting Team. The RSPM shall solicit and recommend a list of additional candidates for appointment to the team and shall submit the list to the RSC. This list shall include the Requester. The RSC may select other individuals to serve, with the Task Force to draft the Standard. This team shall consist of a small group of people who collectively have the necessary technical expertise and work process skills.

The RSPM shall assign NPCC staff personnel to assist in the drafting of the standard including compliance measure, process and elements. The drafting of measures and compliance administration aspects of the standard will be coordinated with the Compliance Program.

STEP 6: SOLICIT PUBLIC COMMENTS ON DRAFT STANDARD

Once a draft standard has been verified by the RSC to be within the scope and purpose of the RSAR, the RSPM will post the draft standard for the purpose of soliciting public comments. The posting of the draft standard will be linked to the RSAR for reference. In addition to the standard, an implementation plan shall be posted to provide additional details to the public and aid in their commenting and decision process. Comments on the draft standard will be accepted for a 45 calendar day period from the public notice of posting. Comments will be accepted on-line using the NPCC Open Process web-based application.

Final draft standards will be concurrently posted on the ERO website for comments.

STEPS 7, 8, AND 9: OPEN PROCESS POSTING AND ANALYSIS OF THE COMMENTS

The RSPM will assemble the comments on the new draft standard and distribute those comments to the Task Force acting as the standard drafting team. The Task Force shall give prompt consideration to the written views and comments of all participants. An effort to address all expressed comments shall be made, and each commenter shall be advised of the disposition of the comment and the reasons therefore, in addition to public posting of the responses.

The Task Force acting as the Standard Drafting Team shall take one of the following actions:

- Submit the draft standard for RCC endorsement as it stands, along with the comments received and responses to the comments. Based on the comments received, the Task Force acting as the standard drafting team may include revisions that are not substantive. A substantive change is one that directly and materially affects the application of the standard, including, for example: changing "shall" to "should," changing "should" to "shall"; adding, deleting, or revising requirements; or adding, deleting, or revising measures for which compliance is mandatory.
- Make substantive revisions to the draft standard and reposts it for further open review and comment.
- Task Force recommends Field Test if necessary to RSC.

Requester also may withdraw the request for a standard.

RCC submits proposed RRS to the RSC along with its recommendation based on comments, Task Force statements and any field test results.

STEPS 10 AND 11: RSC APPROVES OF THE NEW OR REVISED STANDARD FOR POSTING

If the RSC, acting with consideration of any recommendations by the RCC and utilizing the composite sector voting structure, as outlined in the NPCC, votes to post the draft standard for approval, the draft standard, all comments received, and the responses to those comments shall be posted electronically for the NPCC Members, by the RSPM and made public through the NPCC Website (www.npcc.org) for a 30 calendar day "pre-ballot review" and request for balloting. If the RSC decides more work is needed, the draft standard will be remanded back to the drafting Task Force. All actions of the RCC, Task Forces acting as drafting teams and the Regional Standards Committee will be recorded in regular minutes of the group(s) and posted on the NPCC website. Once the notice for a ballot has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued

STEPS 12, 13 AND 14: BALLOT OF STANDARD

Upon notification of a ballot, the Members of NPCC's registered ballot body will cast their vote consistent with the NPCC Bylaws. This ballot shall commence no sooner than 15 calendar days and no later than 30 calendar days following the notification of ballot. All members of the NPCC are eligible to participate in the voting on proposed, standard revisions or deletions of regional standards. The ballot period will typically begin immediately following the 30 calendar day pre-ballot posting and will last at least 10 business days.

The NPCC registered ballot body comprises all entities or individuals that qualify for one of the eight NPCC stakeholder sectors and are registered with NPCC as potential

ballot participants in the voting on standards. Each member of the NPCC registered ballot body is eligible to vote on standards.

In order for a NPCC Regional Standard to be approved;

- A quorum must be established by at least 50% of the NPCC Members of at least 60% of the Voting Sectors on the roster of Members maintained by NPCC.
- A two-thirds majority of the total weighted sector votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions, and non-responses. Weighted sector vote will be calculated as follows;
  - Affirmative votes cast in each sector will be divided by the sum of affirmative and negative votes cast, in that same sector, to determine the fractional affirmative vote for each sector. Abstentions and non-responses will not be counted for the purposes of determining the fractional affirmative vote for a sector.
  - The sum of the fractional affirmative votes from all sectors divided by the number of sectors voting will be used to determine if a two-thirds majority has been achieved. (A sector will be considered as "voting" if any member of the sector in the ballot pool casts either an affirmative or a negative vote.)
  - A standard will be approved if the sum of fractional affirmative votes from all sectors divided by the number of voting sectors is at least 2/3.

Ballots will be cast electronically and alternatives are as follows;

- Affirmative
- Affirmative with Comments
- Negative
- Negative with Comments
- Abstain

The RSPM shall post the final outcome of the ballot process. If the standard is rejected, it may be withdrawn by either the RCC or the original Requester, or the standard may be remanded by the RSC back to the Task Force acting as the drafting team to address the issues. All comments submitted during the process will be posted and archived for consideration when redrafting the standard upon review.

The standard, once approved by ballot, and a recommendation will be forwarded to the NPCC Board for final Regional approval. The Board may not make substantive modifications to the standard. If the Board does not approve the standard for transmittal to NERC it will be remanded back to the RSC.

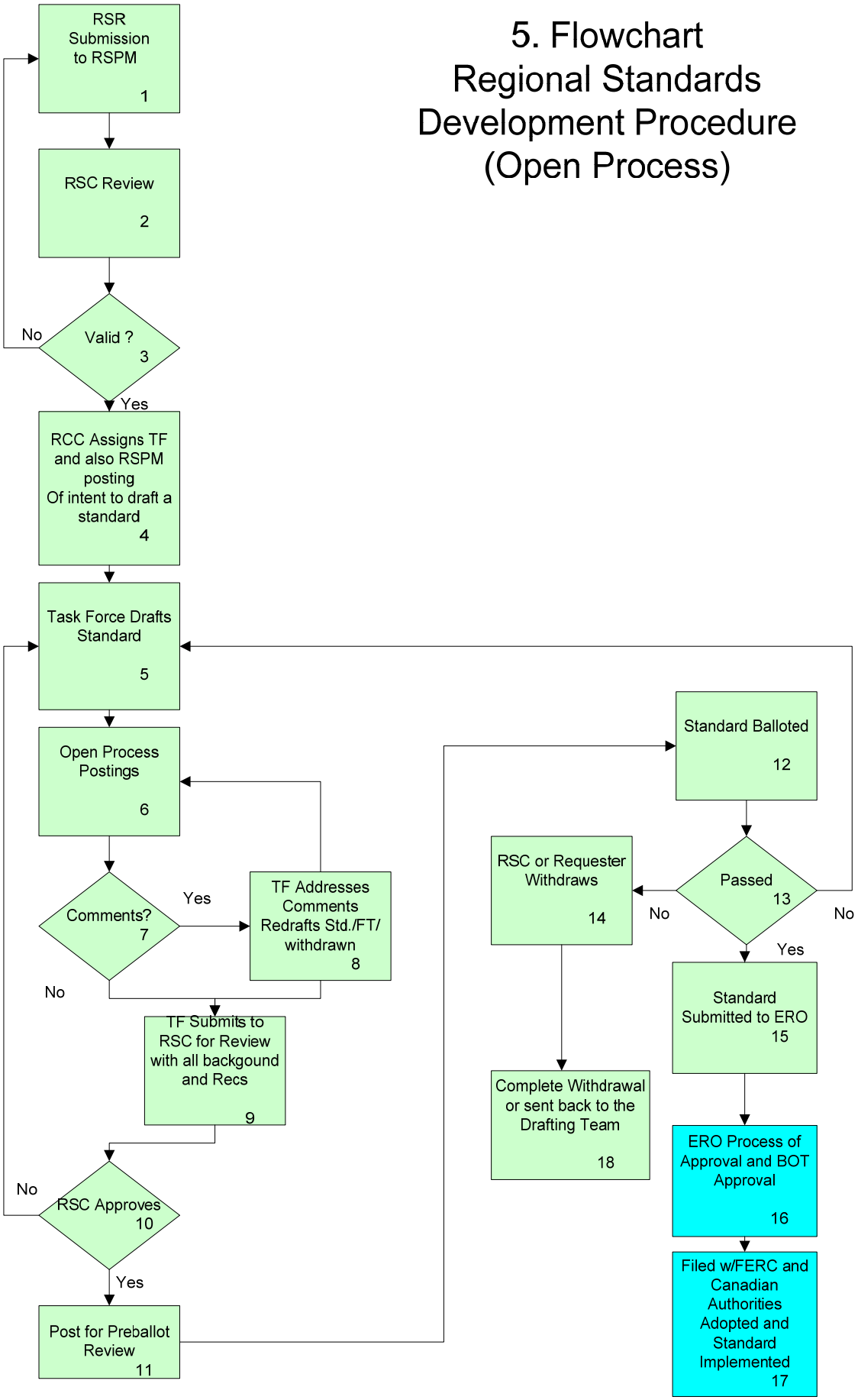
If the standard is approved, the standard will be submitted to the NERC/ERO Board of Trustees for approval.

STEPS 15, 16 AND 17: IMPLEMENTATION OF THE NPCC REGIONAL STANDARD
Upon approval within the NPCC , the standard will be submitted to the NERC/ERO for approval(s) and filing with FERC and applicable Canadian Governmental and/or Regulatory Authorities for adoption.

Once a reliability standard is adopted and made effective, all users, owners, planners, and operators of the Bulk Power System in the NPCC geographic area of the Northeast are required to comply with the standard. The NERC/ERO Board of Trustees has established a separate compliance program, also administered in the Northeast by NPCC , to measure compliance with the standards and administer sanctions as appropriate. After adoption of a NPCC Regional Standard, the standard will be forwarded to the compliance program for compliance monitoring and enforcement.

STEP 18: WITHDRAWAL OF STANDARD
Upon rejection of a proposed standard, the RCC or the requester may withdraw the standard completely or remand it back to the Task Force acting as the standard drafting team for further work.

5. Flowchart Regional Standards Development Procedure (Open Process)



6. ERO and Regulatory Process and Approvals

- **NERC/ERO Comment Period** —NERC/ERO shall publicly notice and request comment on the NPCC Regional Reliability Standard, allowing a minimum of 45 calendar days for comment on NERC's website and actively notify all adjoining Regions. Concurrent with this regional posting, final drafts will be forwarded to NERC for posting on the NERC website to ensure full industry awareness of the standard and expedite and coordinate all commenting. All comments will be responded to electronically through a posted response on the NPCC website or a link on the NERC website. NPCC shall have an opportunity to resolve any objections identified in the comments and may choose to withdraw the request, revise the NPCC Regional Reliability Standard and request another posting for comment, or submit the NPCC Regional Reliability Standard along with a response to any objections received, for approval by NERC.

- **NERC/ERO Approval of NPCC Regional Reliability Standards** — Proposed regional reliability standards shall be subject to approval by the NERC/ERO who shall have a process to evaluate and recommend whether a proposed non-Interconnection-wide NPCC Regional Reliability Standard has been developed in accordance with all applicable procedural requirements and whether NPCC has considered and addressed stakeholder objections. NPCC Board, having been notified of the results of the regional ballot concerning a NPCC Regional Reliability Standard, shall vote to submit the Standard to the NERC/ERO Board for approval as a NERC Reliability Standard. The NERC/ERO Board shall consider NPCC's request, the scope and implications of the Standard, the recommendation for action on the Standard, any unresolved stakeholder comments, and NPCC's consideration of comments and unresolved issues if any, in determining whether to approve the NPCC Regional Reliability Standard as a NERC Reliability Standard.

- **Regulatory Authority Approval** — An NPCC Regional Reliability Standard that has been approved by the NERC/ERO board shall be filed with FERC and applicable Canadian Governmental and/or Regulatory Authorities for approval and shall become effective and enforceable within the U.S., per Section 215 of the Federal Power Act, only when adopted by FERC, and within Canada, only when adopted by applicable Canadian Governmental and/or Regulatory Authorities. The regional reliability standard, once adopted will be made part of the body of NERC reliability standards and shall be mandatory and enforceable on all applicable bulk power system owners, operators, and users within the NPCC Region, regardless of membership status.

7. Appeals

- Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the development, approval, revision, reaffirmation, or withdrawal of a regional reliability standard shall have the right to appeal.

This appeals process applies only to the standards process as defined in this procedure.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within 30 calendar days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

- Level 1 Appeal

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the RSPM that describes the substantive or procedural action or inaction associated with a reliability standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary staff and committee resources, the RSPM shall prepare a written response addressed to the appellant as soon as practical, but not more than 45 calendar days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response will be made a part of the public record associated with the standard and posted with the standard.

- Level 2 Appeal

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the regional standards process manager, the RSPM shall convene a Level 2 Appeals Panel. This panel shall consist of five members total appointed by the NPCC's board.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The RSPM shall post the complaint and other relevant materials and provide at least 30 calendar days notice of the meeting of the Level 2 Appeals Panel. In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC with a statement of the issues and facts in regard to which fair and equitable action was not taken. The panel may find against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise,

approve, disapprove, or adopt a reliability standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the NPCC Board for consideration at the time the board decides whether to adopt a particular reliability standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than 30 calendar days after the announcement of the vote on the standard in question.

APPENDIX A

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC Regional Standards Process Manager, NPCCstandard@npcc.org . The NPCC Regional Standards Process Manager shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:
Request Date:

RSAR Requester Information

Name:	**RSAR Type (Check box for one of these selections.)**
Company:	☐ New Standard
Telephone:	☐ Revision to Existing Standard
Fax:	☐ Withdrawal of Existing Standard
Email:	☐ Urgent Action
Purpose (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability**.)**	
Industry Need (Provide a detailed statement justifying the need for the proposed standard, along with any supporting documentation**.)**	
Brief Description (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others**.)**	

Reliability Functions

The Standard will Apply to the Following Functions (Check all applicable boxes.)

☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission Operator	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.
☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected bulk power 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 power 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 power 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 power 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 power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
Recognizing that reliability is an Common Attribute of a robust North American economy:	
1. A reliability standard shall not give any market participant an unfair competitive advantage.Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	
4. A reliability 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 a standard based on this description.)

Related Standards

Standard No.	**Explanation**

-t

Related SARs or RSARs

SAR ID	**Explanation**

REGIONAL STANDARDS COMMITTEE

Chairman:

Guy V. Zito
Assistant Vice President - Standards
Northeast Power Coordinating Council, Inc.
Tel. (212) 840-1070
Email: gzito@npcc.org

Co-Vice Chairman:

Gregory A. Campoli
Supervisor, Reliability Compliance & Assessment
New York Independent System Operator
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

Co-Vice Chairman:

Bruce Metruck
NERC Compliance Program Manager II
New York Power Authority
F.R. Clark Energy Center
6520 Glass Factory Road
Marcy, NY 13403
Tel. (315) 792-8213
Email: bruce.metruck@nypa.gov

Sector 1 - Transmission Owners

Hydro One Networks, Inc.

Primary
Ayesha Sabouba, P. Eng., MBA
Manager - Policy and Reliability Standards Compliance
Tel. (416) 345-5267
Email: asabouba@HydroOne.com

Alternate
Muhammed Ali
Network Management Engineer – Reliability Standards and Compliance Department
Tel. (416) 345-5856
Email: muhammed.ali@hydroone.com

Consolidated Edison Company of New York, Inc.

Primary
Kelly Dash
Engineer – Standards and Compliance
Room 1300 NW 4 Irving Place NY, NY 10003
Tel. (212) 460-4155
Email: dashk@coned.com

Alternate
David Balban
Engineer – Standards and Compliance
Room 1300 NW 4 Irving Place NY, NY 10003
Tel. (212) 460-1078
Email: balband@coned.com

National Grid

Primary
Brian Shanahan
Tel. (315) 460-2346
Email: brian.shanahan@nationalgrid.com

Alternate
Michael Jones
Lead Analyst – FERC Compliance
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

New Brunswick Power Corporation

Primary
Alan MacNaughton, P.Eng.
Senior Compliance Engineer
Tel. (506) 443-6577
Email: amacnaughton@nbpower.com

Alternate

The United Illuminating Company

Primary
Robert J. Pellegrini
ES Asset Management
Manager Protection &Control/ SCADA
180 Marsh Hill Road
Orange, Connecticut 06477
Tel. (203) 499-2413
Email: Robert.pellegrini@uinet.com

Alternate

Hydro-Quebec TransÉnergie

Primary
Sylvain Clermont
Manager Transmission Services
Tel. (514) 879-4648
Email: clermont.sylvain@hydro.qc.ca

Alternate
Si Truc Phan
2 Complexe Desjardins, 19th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 879-4100 Ext. 3610
Email: phan.si_truc@hydro.qc.ca

Orange & Rockland Utilities, Inc.

Primary
Ben Wu
Transmission & Substation Engineering
Tel. (845) 577-3713
Email: WUB@oru.com

Alternate

Northeast Utilities

Primary
Mark J. Kenny
Program Manager - Reliability Compliance
Tel. (781) 441-8179
Email: Mark.Kenny@nu.com

Alternate

Sector (2) - Reliability Coordinators

New York Independent System Operator

Primary
Gregory A. Campoli
Supervisor, Reliability Compliance & Assessment
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

Alternate
James (Jim) Grant
Reliability Senior Engineer
Tel. (518) 356-6128
Email: jgrant@nyiso.com

ISO New England, Inc.

Primary
Kathleen M. Goodman
Senior Operations Compliance Coordinator
Tel. (413) 535-4111
Email: kgoodman@iso-ne.com

Alternate
Matthew Goldberg
Director of Reliability & Operations Compliance
Tel. (413) 535-4029
Email: mgoldberg@iso-ne.com

Independent Electricity System Operator

Primary
Helen Lainis
Senior Engineer/Technical Officer
Tel. (905) 855-4106
Email: helen.lainis@ieso.ca

Alternate
Scott Berry
Senior Engineer/Technical Officer
Tel. (905) 403-6912
Email: scott.berry@ieso.ca

Hydro-Quebec TransÉnergie

Primary
Si Truc Phan
2 Complexe Desjardins, 19th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 879-4100 Ext. 3610
Email: phan.si_truc@hydro.qc.ca

Alternate
Chantal Mazza
Direction Contrôle des Mouvements d'énergie
C.P. 10000, succ. pl Desjardins
Complexe Desjardins 19th floor
Montréal, QC H5B 1H7
Tel. (514) 879-4100 Ext. 5499
Email: mazza.chantal@hydro.qc.ca

Sector (3) - Transmission Dependent Utilities ("TDUs"); Distribution Companies and Load-Serving Entities ("LSEs")

Consolidated Edison Company of New York, Inc.

Primary
Peter Yost
Manager, Standards & Compliance
Tel. (212) 460-2889
Fax (212) 529-1130
Email: yostp@coned.com

Alternate
Christopher L. de Graffenried
Senior Engineer Transmission Planning
Room 1300, 13th Floor - Northwest
Tel. (212) 460-2925
Email: degraffenriedc@coned.com

National Grid

Primary
Michael Jones
Lead Analyst – FERC Compliance
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Alternate
Brian Shanahan
Tel. (315) 460-2346
Email: brian.shanahan@nationalgrid.com

Orange & Rockland Utilities, Inc.

Primary	Alternate
David Burke	Thomas Neglia
Senior Specialist - Compliance	Senior Specialist – Compliance
Tel. (845) 577-2841	Tel. (845)-577-2839
Fax (845) 577-2840	Email: NegliaT@oru.com
Email: burkeda@oru.com	

Sector (4) - Generator Owners

New York Power Authority

Primary	Alternate
Wayne Sipperly	Shivaz Chopra
NERC Compliance Program Manager II	RSC Engineer II, Technical Compliance
Tel. (914) 287-3753	Tel. (914) 681-6828
Email: wayne.sipperly@nypa.gov	Email: shivaz.chopra@nypa.gov

Dominion Resources Services, Inc.

Primary	Alternate
Connie Lowe	Lou Oberski
NERC Compliance Policy Manager	Managing Director NERC Compliance Policy
Dominion Resources Services, Inc.	Dominion Resources Services, Inc.
Tel. (804) 819-2917	Tel. (804) 819-2837
Email: connie.lowe@dom.com	Email: lou.oberski@dom.com

Ontario Power Generation, Inc.

Primary	Alternate
David Ramkalawan, P.Eng.	
Senior Manager - Reliability Compliance	
Tel. (416) 592-6089	
Email: david.ramkalawan@opg.com	

NextEra Energy, LLC

Primary	Alternate
Silvia Parada Mitchell	
Director Reliability Standards & Compliance	
Tel. (561) 694-4414	
Email: silvia.parada.mitchell@fpl.com	

Sector (5) - Marketers, Brokers and Aggregators

New York Power Authority

Primary
Bruce Metruck
NERC Compliance Program Manager II
F.R. Clark Energy Center
6520 Glass Factory Road
Marcy, NY 13403
Tel. (315) 792-8213
Email: bruce.metruck@nypa.gov

Alternate
Daniella Piper
Reliability Standards & Compliance Engineer
Tel. (914) 681-6595
Email: daniella.piper@nypa.gov

Alternate
Salvatore Spagnolo
Senior Reliability Standards & Compliance Engineer I
Tel. (914) 390-8224
Mob. (347) 992-7015
Email: Salvatore.Spagnolo@nypa.gov

Utility Services, Inc.

Primary
Brian Robinson
Compliance Analyst
Tel. (802) 552-4022
Email: brian.robinson@utilitysvcs.com

Alternate
Brian Evans-Mongeon
President/CEO
Tel. (802) 552-4022
Email: brian.evans-mongeon@utilitysvcs.com

Sector (6) – State and Provincial Regulatory and/or Governmental Authorities

New York State Department of Public Service

Primary
Vijay Puran
Utility Engineer 3
Tel. (518) 486-5948
Email: vijay.puran@dps.ny.gov

Alternate
Diane J. Barney
Chief, Bulk Electric Systems
Tel. (518) 486-2943
Email: diane.barney@dps.ny.gov

Sector 7 – Sub-Regional Reliability Councils, Customers and Other Regional Entities and Interested Entities

New York State Reliability Council, LLC

Primary
Alan Adamson
Independent Consultant
2104 Braxton Street
Clermont, FL 34711
Tel. (352) 989-4653
Email: aadamson@nycap.rr.com

Alternate

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 28, 2014

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. RR14-6-000
Request for Acceptance of 2015 Business Plans and budgets of NERC and Regional Entities and for Approval of Proposed Assessments to Fund Budgets-
Update on CRISP Implementation

Dear Secretary Bose,

The purpose of this letter is to provide the staff of the Federal Energy Regulatory Commission (the Commission) with a brief update regarding the status of CRISP Program implementation which was included in the NERC's 2015 business plan and budget.

Significant progress has been made since the filing of NERC's 2015 business plan and budget in August, 2014. NERC and 15 utilities have executed the Master Agreement (Master Agreement) and related Statements of Work. NERC has also executed the related agreement with Battelle Memorial Institute, the operator of the Pacific Northwest National Laboratory (PNNL). Implementation of the CRISP Program is now underway, and NERC will continue to seek additional industry participation in the CRISP program.

Funding by utility participants is in process. 2015 funding will be in two installments, with the first installment due in early January, 2015. The second installment will be due within 30 days after NERC provides a reconciliation of 2014 actual to budgeted costs, which is anticipated to be on or about March 15, 2015. A separate bank account has been established to segregate CRISP program funds and track funding by utility participants

Budget Recap

The 2014 budget is sufficient to fund 100% of the 2014 CRISP program costs, inclusive of PNNL costs. An overall not to exceed budget, as well as a not to exceed budget by participating utility, has been agreed to with PNNL and each participating utility. Consistent with the NERC board's resolution authorizing the program, 2014 utility funding amounts have been established in a sufficient amount to avoid the use of existing NERC reserves.

The 2015 CRISP program budget reflects final cost reduction negotiations with PNNL from those assumed in the 2015 business plan and budget, as well as the allocation of direct funding of program startup costs

by participating utility in 2014 that were assumed to be incurred in 2015 in the 2015 business plan and budget. As a result, the final 2015 CRISP program budget, inclusive of PNNL costs, has been reduced from the approximately $9.3M included in the 2015 business plan and budget to approximately $5.9M. This is in large part due to the 2014 allocation of funding of startup expenses as noted above. The 2014 CRISP program budget, covering the period from October 1, 2014 thru December 31, 2014, is approximately $4.9M, entirely funded by the utility participants. The total direct utility funding for 2014 and 2015 will be approximately $10.8M. The final total 2014 and 2015 CRISP budgets are set forth in Attachment A. NERC's internal 2015 ES-ISAC department budget, which is exclusive of PNNL subcontract costs and other costs funded directly by utility participants, is consistent with the internal ES-ISAC budget included in NERC's 2015 business plan and budget and which was utilized for purposes of determining the proposed 2015 CRISP program funding from assessments.

Please do not hesitate to contact me should Commission staff have any questions or require further information.

Sincerely,



Michael A. Walker
Senior Vice President
Chief Financial and Administrative Officer

CC: Gerald Cauley
Charles Berardesco
Susan Turpen
Tim Roxey
Matthew Light
Meredith Jolivert

Attachment A
2014 and 2015 NERC CRISP Budget in Statement of Activities Format
(Includes both NERC and PNNL costs)

Statement of Activities and Fixed Assets Expenditures 2014 and 2015 NERC Budget CRISP	NERC 2014 Budget	NERC 2015 Budget
Funding		
ERO Funding		
NERC Assessments*	-	$ 860,938
Penalty Sanctions	-	16,554
Total NERC Funding	**$ -**	**$ 877,492**
Third-Party Funding (CRISP)	4,894,545	5,038,269
Interest	-	42
Total Funding (A) (Equals Total Budget plus Change in Working Capital)	**$ 4,894,545**	**$ 5,915,803**
Expenses		
Personnel Expenses		
Salaries	$ 90,839	363,357
Payroll Taxes	5,248	20,990
Benefits	8,488	33,953
Retirement Costs	10,238	40,951
Total Personnel Expenses	**$ 114,813**	**459,251**
Meeting Expenses		
Meetings	$ 3,750	15,000
Travel	7,500	30,000
Conference Calls	1,250	5,000
Total Meeting Expenses	**$ 12,500**	**50,000**
Operating Expenses		
Consultants & Contracts - PNNL Initial Start-Up	$ 1,902,385	$ -
Consultants & Contracts - PNNL Operations	1,380,893	4,275,735
Consultants & Contracts - NERC	135,000	135,000
Office Rent	-	-
Office Costs	76,250	305,000
Professional Services	250,000	50,000
Cyber/E&O Insurance Premiums	325,000	150,000
Depreciation	-	-
Total Operating Expenses	**$ 4,069,528**	**$ 4,915,735**
Total Direct Expenses	**$ 4,196,841**	**$ 5,424,986**
Indirect Expenses	**$ 92,201**	**$ 368,803**
Other Non-Operating Expenses	**$ -**	**-**
Total Expenses (B)	**$ 4,289,041**	**$ 5,793,788**
Fixed Assets		
Computer & Software CapEx	$ 100,000	100,000
Allocation of Fixed Assets	5,504	22,014
Inc(Dec) in Fixed Assets (C)	**$ 105,504**	**$ 122,014**
TOTAL BUDGET (=B + C)	**$ 4,394,545**	**$ 5,915,803**
INSURANCE DEFENSE FUND (=A-B-C)	**$ 500,000**	**$ -**

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Assurance Initiative	**)**	**Docket No. RR15-__-000**

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC")[1] hereby submits to the Federal Energy Regulatory Commission ("FERC" or "Commission"), for informational purposes, a description of the various processes and programs developed and deployed through the ERO Enterprise's[2] Reliability Assurance Initiative ("RAI"). The initiative was developed to implement across the ERO Enterprise a risk-based compliance monitoring and enforcement program ("CMEP")[3] that provides reasonable assurance of reliability through compliance monitoring, appropriate deterrence through enforcement, and a feedback loop to improve Reliability Standards.

The processes and programs described herein are fully consistent with existing NERC Rules of Procedure and authority and the Commission's rules, orders, and regulations.

[1] NERC is the Commission-certified electric reliability organization ("ERO") responsible for the development and enforcement of mandatory Reliability Standards. *See North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 342 (D.C. Cir. 2009).

[2] The term "ERO Enterprise" refers to NERC and the eight Regional Entities. The eight Regional Entities are Florida Reliability Coordinating Council ("FRCC"), Midwest Reliability Organization ("MRO"), Northeast Power Coordinating Council ("NPCC"), ReliabilityFirst ("RF"), SERC Reliability Corporation ("SERC"), Southwest Power Pool Regional Entity ("SPP RE"), Texas Reliability Entity ("Texas RE"), and Western Electricity Coordinating Council ("WECC").

[3] As the context requires, "CMEP" refers to the compliance monitoring and enforcement program or the document found at Appendix 4C of the NERC Rules of Procedure, which contains the rules associated with such program.

Therefore, NERC and the Regional Entities are not requesting Commission action on this informational filing.

Section II of this filing describes the context for the development of the initiative. It discusses in summary form, the process of developing the risk-based approach to compliance monitoring and enforcement. Finally, the section describes the oversight and training programs established by the ERO Enterprise to ensure appropriate and consistent application of the processes discussed herein.

Section III of this filing describes the enhancement of a feedback loop between compliance monitoring and enforcement and other activities, including the development of Reliability Standards.

Section IV of the filing describes compliance monitoring processes, as well as the regulatory framework that allows implementation of these processes. This section discusses the identification and prioritization of risk elements, the inherent risk assessment ("IRA"), and internal controls evaluation ("ICE") processes, and the development of compliance oversight plans for registered entities including the planning and execution of Compliance Audits.

Section V of the filing discusses the processes associated with a greater exercise of enforcement discretion by the ERO Enterprise, specifically the use of compliance exceptions and self-logging of minimal risk issues.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 5

II. DEVELOPMENT OF THE RELIABILITY ASSURANCE INITIATIVE 6

A. COMPLIANCE PILOT PROGRAM 7
B. ENFORCEMENT ACTIVITIES 9
C. FROM DESIGN TO IMPLEMENTATION 13
1. Increased Outreach and Communication 13
2. Oversight by NERC 15
3. Continuous Training 17
4. Increased Coordination 18

III. FEEDBACK LOOP FOR THE IMPROVEMENT OF RELIABILITY STANDARDS 19

IV. RISK-BASED COMPLIANCE MONITORING 20

A. REGULATORY STRUCTURE 20
B. RISK-BASED OVERSIGHT PLAN FRAMEWORK 23
1. Risk Elements 24
2. Inherent Risk Assessment 26
3. Internal Controls Evaluation 30
4. CMEP Tools 34
C. PLANNING AND EXECUTION OF COMPLIANCE AUDITS 35

V. RISK-BASED ENFORCEMENT 38

A. FFT AS THE PLATFORM FOR THE EVOLUTION OF A RISK-BASED ENFORCEMENT PROGRAM 38
B. REGULATORY STRUCTURE AND IDENTIFICATION OF THE RISK POSED BY NONCOMPLIANCE 40
C. COMPLIANCE EXCEPTIONS 43
1. Instances of Noncompliance that Qualify for Recording as Compliance Exceptions 45
2. Applicability throughout ERO Enterprise 46
3. Processing and Recording of Compliance Exceptions 47
4. Experience Gained during Pilot Phase 50
5. Visibility and Accountability 50
6. Oversight by NERC 54
D. SELF-LOGGING PROGRAM 55
1. Eligibility to Participate in the Program 56
2. Processing and Recording of Self-Logged Noncompliance 57
3. Experience Gained during Pilot Phase 59
4. Visibility and Accountability 61
5. Benefits of Self-logging 62

6. Oversight by NERC 63
VI. CONCLUSION 65
VII. NOTICES AND COMMUNICATION 66

I. EXECUTIVE SUMMARY

RAI was a collaborative effort among NERC, the Regional Entities, and industry to identify and implement changes to enhance the effectiveness of compliance monitoring and enforcement. Essentially, the initiative resulted in the adoption of a risk-based approach to compliance monitoring and enforcement. This approach benefits reliability by focusing resources applied to compliance monitoring and enforcement based on risk, thereby allowing the ERO Enterprise and registered entities to focus appropriate time and effort on higher-risk issues. As the reliable operation of the bulk power system ("BPS") is in the public interest, the focusing, by the ERO Enterprise on matters that pose greater risk to that reliable operation is also in the public interest. This approach does not equate to ignoring lesser-risk issues, which, as explained in this filing, continue to be identified, corrected, and tracked.

A risk-based approach is fully consistent with NERC's existing rules and authority, as demonstrated below. Further, this approach focuses on how the ERO Enterprise performs oversight and obtains assurance regarding compliance with Reliability Standards and does not create new or additional requirements (beyond those established in Reliability Standards) for registered entities operating the grid. However, this approach has the benefit of allowing the ERO Enterprise to leverage certain management practices in use at registered entities in focusing its own oversight activities. This ability to leverage management practices also has the effect of disseminating and enhancing such practices throughout industry.

The ERO Enterprise is prepared to implement the new processes described in this filing fully in January 2015. By the end of 2015, the ERO Enterprise expects to measure the success of

this initiative in a number of ways, including through measures related to staff competencies, robustness of outreach, program transparency, and sharing of best practices.

As the ERO, NERC has the oversight authority, responsibility, and obligation to monitor Regional Entities' adherence to the NERC Rules of Procedure, specifically the CMEP, and performance of their delegated responsibilities on behalf of NERC. NERC will continue its oversight activities to ensure consistency throughout the ERO Enterprise in identification of risks and evaluation of processes, procedures, and internal controls, as well as the assessment of risks associated with noncompliance and mitigation. NERC oversight of all components of the risk-based CMEP will be essential to the proper application of the program over the long-term.

Through implementation of the risk-based approach described in this filing, the ERO Enterprise also will strengthen the trust of the Commission and other applicable governmental authorities in the ERO Enterprise's risk-based compliance and enforcement. An appropriate level of transparency will be in place for various facets of risk-based compliance monitoring and enforcement, balancing efficiency and the confidentiality needs of a registered entity with the needs of industry as a whole to learn from others.

II. DEVELOPMENT OF THE RELIABILITY ASSURANCE INITIATIVE

In 2012, the ERO Enterprise initiated a multi-year effort to identify and implement changes that enhance the effectiveness of the CMEP. The experience of the past several years demonstrates that a one-size-fits-all and zero tolerance approach to compliance monitoring and enforcement does not properly allocate time, attention and resources for serious and lesser risk noncompliance, does not demonstrably equate to more reliable operations of the BPS, and is not sustainable. In fact, the risk-based approach outlined herein is more likely to ensure the reliable

operation of the BPS. The case for a risk-based approach to compliance monitoring and enforcement has been previously outlined in a NERC white paper, *Incorporating Risk Concepts into the Implementation of Compliance and Enforcement*.[4]

Over this time, the ERO Enterprise tested, through various pilot programs, a number of concepts, processes, and programs to develop a risk-based compliance monitoring framework and a risk-based enforcement program. This experience is described below.

A. Compliance Pilot Program

The ERO Enterprise compliance pilot program focused on the development and implementation of approaches to risk assessments and testing of internal controls. The purpose of the compliance pilot program was to develop a single, common ERO Enterprise approach to compliance monitoring, focusing on risk-based assessments, scoping, internal controls review concepts, and tests of controls. Specific outcomes from the pilot program included proposed processes and methods for conducting inherent risk assessments of a registered entity and evaluating internal controls.

NERC and the Regional Entities initiated phase one of the pilot program during 2013. This phase explored different approaches to applying risk-based auditing concepts. In phase one, five Regional Entities designed pilots that included various approaches to audit scoping, inherent risk assessments, and testing of internal controls related to Reliability Standards. Regional Entities worked with registered entities to identify entity-specific risks and related internal controls to scope an audit and assess compliance with the Reliability Standards in scope. Both

[4] *See* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/White%20Paper%20–%20The%20Need%20for%20Change%20(paper%201).pdf.

Regional Entity and registered entity representatives involved in the pilots provided feedback on the pilot approaches.

The second phase of the pilot program evaluated the pilot results. Representatives from each of the eight Regional Entities reviewed pilot results and identified specific approaches or processes that the ERO Enterprise should use for its single, common method for compliance monitoring. Converging the various approaches into a single design began in January 2014 and included a detailed review of each pilot and presentation of each individual Regional Entity pilot design to an evaluation team during February 2014. The evaluation team consisted of an independent audit consultant and senior NERC, Regional, and industry representatives. To assist the evaluation team in determining the best approach, NERC and the Regional Entities invited a group of industry professionals to help develop criteria to evaluate the various approaches. The established criteria included transparency, design effectiveness, alignment to Reliability Standards, implementation requirements, and registered entity impact.

The third and final stage of the pilot program, beginning in June 2014, was finalizing the single, common approach to inherent risk assessments and internal controls evaluations. During the final stage, two smaller teams of NERC and Regional Entity staff designed guidance documents to provide an overall framework for how Regional Entities would conduct inherent risk assessments and internals control evaluations. The teams used the pilot results and evaluation criteria to finalize guidance documents. The two design teams coordinated with industry representatives to obtain input into the development and content of the guidance documents. Additionally, the NERC Board of Trustees requested policy input from industry on the draft inherent risk assessment guidance, which the final guidance documents incorporated.

As explained below, the new processes developed through RAI associated with the compliance monitoring program have resulted in the development of a common framework for oversight of registered entities based on the identification of risk elements, assessment of an entity's inherent risk, and evaluation of its internal controls. Each of these components allows the Compliance Enforcement Authority ("CEA")[5] to select the appropriate monitoring tools on the basis of risk. The framework is based on the use of risk-based compliance monitoring practices similar to those utilized in other industries. The focus, method, and frequency of monitoring engagements are based on a common ERO Enterprise approach to assessing a registered entity's risk to the reliability of the BPS and may be further refined based on the strength of the registered entity's management controls related to compliance with Reliability Standards.

B. Enforcement Activities

Recognizing the opportunity for risk-based enforcement improvements, in parallel with the risk-based compliance activities referenced above, the ERO Enterprise began to transition away from a process-driven enforcement strategy to a proactive, risk-based strategy that defines, communicates, and promotes desired entity behavior in an effort to improve the reliability of the BPS. Specifically, this approach allows the ERO Enterprise to focus on the higher risks to the reliability of the BPS, providing clear signals to registered entities about identified areas of concern and risk prioritization, while maintaining the ERO Enterprise's existing visibility into potential noncompliance issues regardless of the level of risk they posed. This approach also

[5] "Compliance Enforcement Authorities" or "CEAs" refer to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

encourages the self-identification of noncompliance and enhancement of internal controls by registered entities. NERC and the Regional Entities worked together to develop a series of activities designed to further align enforcement processes with risk and to increase the transparency regarding the ERO Enterprise's assessment of the risk to the BPS posed by specific instances of noncompliance.

The ability of CEAs to arrive at a final determination with respect to all noncompliance in an efficient manner is in part dependent on the quality of the information they have about the noncompliance and related mitigation. With that in mind, NERC and Regional Entity staff prepared self-report[6] and mitigation plan[7] user guides. These user guides build on guidance previously available from NERC and the Regional Entities and explain, among other things, the type and quality of information that should be submitted with a self-report and mitigation plan in order to allow for a prompt evaluation and, as appropriate, prompt disposition of noncompliance (in particular, of noncompliance that posed a minimal risk to the reliability of the BPS).

The ERO Enterprise also addressed concerns regarding timeliness of resolution of minimal risk issues and communication through the adoption of a triage process. As of January 1, 2014, all Regional Entities implemented a triage process. On average, within 60 days of discovery, regardless of discovery method, the CEA reviews noncompliance and determines whether: (i) there is enough information to support treating the noncompliance as a compliance

[6] *ERO Self-Report User Guide* (April 2014), *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf.
[7] *ERO Mitigation Plan Guide* (April 2014), *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Mitigation%20Plan%20Guide%20(April%202014).pdf.

exception; (ii) more information is required prior to determining the disposition; or (iii) the noncompliance needs to be enforced.

Finally, the ERO Enterprise developed additional processes to allow the continued streamlining of the resolution of minimal risk noncompliance, in particular that which is self-identified.

The Find, Fix, Track and Report ("FFT") program was the first step in implementing a risk-based strategy that recognizes that not all instances of noncompliance require the same type of enforcement process. The natural evolution of the FFT program includes the ability to exercise greater discretion, including by declining to initiate an enforcement action to resolve an instance of noncompliance that did not pose a serious or substantial risk to the reliability of the BPS. The ERO Enterprise developed two new processes to achieve this goal: the self-logging program and the use of compliance exceptions. Both are discussed in greater detail below.

The ERO Enterprise's risk-based approach generally reserves enforcement actions under section 5.0 of the CMEP for those issues that pose a higher risk to the reliability of the BPS. As to issues posing a lesser risk, NERC and the Regional Entities may exercise appropriate discretion whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes. This approach allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability. In this context, efficiency does not necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. In addition, this approach allows the ERO Enterprise to continue to provide clear signals to registered entities about identified areas of concern and risk prioritization, while

maintaining existing visibility into potential noncompliance and emerging areas of risk. Finally, this approach improves reliability by acknowledging and encouraging the enhancement of internal controls and self-identification and mitigation of noncompliance by registered entities. Visibility and accountability is maintained because noncompliance that is not enforced is nevertheless mitigated, tracked for analytical purposes, and subject to oversight by NERC as discussed herein.

This approach is not new. Many enforcement agencies in the United States, including FERC, exercise discretion in addressing noncompliance with the regulations they administer and establish priorities for the allocation of their resources. Such enforcement agencies also acknowledge and reward management practices associated with the self-identification and mitigation of noncompliance by regulated entities.[8] The processes described herein build on the

[8] *See* John C. Moot, *Compliance Programs, Penalty Mitigation and the FERC*, 29 Energy Law Journal 547, 562-563 (2008) discussing a Securities and Exchange Commission ("SEC") action forgoing enforcement because "the company had quickly identified the violations, promptly reported them, remedied them internally through disciplinary actions, and taken prospective corrective action to avoid future violations." *See also id.* at 564-65 *citing, Environmental Protection Agency, Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations*, 65 Fed. Reg. 19,618 (2000), which discusses the EPA's policy on *Incentives for Self-Policing, Discovery, Disclosure, Correction and Prevention of Violations*, which provides "[t]he revised Policy … is designed to encourage greater compliance with Federal laws and regulations that protect human health and the environment. It promotes a higher standard of self-policing by waiving gravity-based penalties for violations that are promptly disclosed and corrected, and which were discovered systematically-that is, through voluntary audits or compliance management systems." *See also* Orly Lobel, *Interlocking Regulatory and Industrial Relations: The Governance of Workplace Safety*, 57 ADMIN. L. REV. 1071, 1105-08 (2005) for a discussion of the Occupational Safety and Health Administration ("OSHA") "star" status program, under which OSHA can exempt employers from routine inspections and allow them to claim "star" status in exchange for maintaining exemplary safety records and satisfying other program certification requirements. The pursuit of "star" status improves employee safety and health, decreases regulatory costs, and enhances an entity's reputation.

success of the FFT program, the ERO Enterprise's well-established process for differentiating the resolution of noncompliance based on the risk posed to the reliability of the BPS.

C. From Design to Implementation

The basic framework design for all of these processes was concluded with the posting of program documents and guides on the RAI page of the NERC website in September and October 2014.[9] As discussed below, the ERO Enterprise is continuing to develop tools and templates, and is continuing to perform oversight, in order to obtain assurance that CEAs are implementing the new processes appropriately and consistently. The ERO Enterprise also has strengthened the communication and outreach regarding the processes and program and developed a robust training program.

With the completion of the design, reflected in the various published guides discussed below, and the baseline training provided to ERO Enterprise staff, the program is ready to be implemented in 2015. Over time, and through NERC's oversight of the program, areas that require additional guidance and training will be identified and addressed (either in the form of revised guides or through other means). In identifying such areas, NERC will consider the feedback from Commission staff, Regional Entities, registered entities, and other stakeholders. This iterative review cycle provides the most effective means of quickly adapting to specific implementation challenges.

1. Increased Outreach and Communication

Communication and education also are essential to the successful implementation of the risk-based compliance monitoring and enforcement approach. In recognition of this fact, the

[9] The RAI page is available at: http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

ERO Enterprise has significantly increased its stakeholder outreach efforts in the second half of 2014. Outreach efforts have taken a number of forms, including workshops, webinars, newsletters, and other communications.

A significant milestone associated with the outreach and communication efforts was the formation, in September 2014, of an advisory group composed of stakeholders representing diverse Standing Committee, Regional, and regulatory perspectives. The advisory group was based on the successful experience of other ERO Enterprise initiatives and provided input and advisory guidance to NERC and Regional Entity staff as it finalized the design of the various components of the risk-based approach to compliance monitoring and enforcement. Currently the advisory group provides assistance on RAI-related outreach and training to the industry, including the format and agenda for the workshops described below.

In November, the ERO Enterprise is hosting two industry outreach workshops (on November 6, 2014 in Atlanta, GA and November 20, 2014 in Phoenix, AZ). The topics and agenda will be the same for each event. At each workshop, a panel of participants from Regional Entities and stakeholder companies will discuss their experiences and expectations about the components of risk-based approach to compliance monitoring and enforcement. Discussion on the panels will also include the application of the risk-based concepts to version 5 of the CIP Reliability Standards. The workshops are designed to foster practical conversations on how risk-based compliance monitoring and enforcement will look and feel to registered entities as the ERO Enterprise implements this approach in 2015.

NERC also conducted webinars to help disseminate information on the new processes.[10] In particular, an "RAI 101" webinar was held on October 3, with over 150 attendees, and presenters from NERC and several Regional Entities. The presentation and recording are also available on the NERC RAI page under "RAI Workshops and Webinars."

In the second half of 2014, NERC also increased its communication efforts associated with the initiative through individual announcements of relevant milestones, and spotlights of recent developments regarding RAI in its weekly and monthly publications. These materials have been distributed to broad distribution lists by email and are also posted on the NERC RAI page under "Program News."

2. Oversight by NERC

Oversight is essential to the long-term success of the compliance monitoring and enforcement program. Oversight ensures consistency in identification of risks and evaluation of processes, procedures, and internal controls, as well as the assessment of risks associated with noncompliance and mitigation. The, ERO Enterprise is currently developing measures of success to evaluate the risk-based approach to compliance monitoring and enforcement.

As part of its oversight role, NERC uses a combination of review processes to ensure that CEAs are implementing the CMEP effectively, to provide constructive feedback where appropriate, to identify trends, and to drive the implementation of best practices. In developing a comprehensive oversight plan, NERC has built, and will continue to build, on its experience overseeing CEAs on matters that involve the exercise of professional judgment. NERC's

[10] A schedule of stakeholder outreach opportunities is available at: http://www.nerc.com/pa/comp/Documents/RAI%20Schedule.pdf.

oversight of and involvement with the Regional Entities' compliance monitoring and enforcement activities are not limited to an after-the-fact determination of the quality of a Regional Entity's performance relative to a given process. NERC will regularly report on the results of its oversight, including performance as measured by certain key metrics, at its board meetings.

Regarding the compliance monitoring activities, NERC will conduct Regional Entity reviews during the first quarter of 2015 with the intent of supporting conceptual consistency in the application of the ERO Enterprise's risk-based approach. Throughout 2015, NERC's oversight will begin to evolve into a more traditional evaluation to assess areas supporting consistency in implementation of the guidance documents and providing feedback on opportunities for greater consistency. During 2015, NERC will focus on samples of Regional Entity IRAs, ICEs, and other aspects of the Framework that utilized the new risk-based approaches.

Regarding the enforcement activities, NERC will continue to perform oversight on an ongoing basis through three main categories of activities: analysis of data and metrics, annual spot checks of various programs, and dissemination of guidance and training. NERC oversight focuses on identifying areas for improvement in the future, rather than reopening closed matters. NERC prepares analyses and reports to assist with monitoring of CMEP processes for consistency and reasonable assurance of reliability, and to help identify trends that may affect BPS reliability. As an example, NERC analyzes repeat violations as well as new violations reported. Analysis of new violations helps identify significant violations that may adversely affect BPS reliability. Performance indices are also computed on a regular basis to quantify the

performance of the Regional Entities and NERC in processing violations and mitigation and to provide insight in determining the effectiveness of regional programs and adequacy of regional and NERC resources. Additional detail regarding NERC oversight of the self-logging and compliance exceptions programs is included below.

NERC also collaborates closely with FERC staff on oversight. A current example of such collaboration is the joint review of the FFT program through a combined annual spot check.

NERC oversight of all components of the risk-based compliance monitoring and enforcement program will be essential to the proper application of the program over the long term.

3. Continuous Training

As the design of RAI is completed, dissemination of guidance and training continues to be an integral component of ongoing CMEP implementation and in support of progressive consistency across the ERO Enterprise. To consistently implement the risk-based compliance oversight framework ("Framework") and its components in 2015, NERC is collaborating with a group of Regional Entity leaders to develop multiregional training covering all of the ERO Enterprise staff.

A NERC and Regional Entity core group of presenters has provided training to ERO Enterprise staff in a number of different venues. First, the group presented to auditors, enforcement and risk staff at the ERO Auditor Workshop in September. The presentations covered all aspects of the risk-based approach to compliance monitoring and enforcement, based on the near final versions of the various program documents available at the time.

This group is also implementing a phased program to provide more focused training to the staff performing IRAs and ICEs. Phase one of the training will address the implementation of the IRA and ICE guides, focusing first on regional staff that will actually perform IRAs and ICEs. Specifically, NERC and the Regional Entity leaders are holding three two-day sessions with Regional Entity staff in November and December. As noted above, to ensure consistency in training and approach, there is a core group of NERC-led presenters and trainers composed of both NERC and Regional Entity staff. The majority of the ERO Enterprise staff performing IRAs and ICEs has committed to attending the in-person training sessions and all staff will be trained. The training will include the discussion of hypotheticals and case studies developed based on the existing guides. This training is expected to be complete in December 2014.

Phase two will occur through the second quarter of 2015, and involves a reevaluation of guidance documents, development of lessons learned, and reevaluation of training needs. NERC and the Regional Entities will continue to assess training needs throughout 2015 and revise existing and ongoing training to incorporate Framework concepts.

Additional information on training is provided below, in connection with the discussions of Compliance Audits and enforcement processes. Training opportunities for industry, beyond those discussed in the context of outreach, above, are also in development.

4. Increased Coordination

Parallel to the adoption of a risk-based approach to compliance monitoring and enforcement, the ERO Enterprise is examining its practices associated with monitoring and enforcement for entities located in more than one Regional Entity footprint. There is an ongoing effort to enhance the coordination among Regional Entities for the execution of the compliance

monitoring and enforcement processes defined in CMEP. These efforts include a more defined structure and transparency for such coordination. Initial results are expected to be available in 2015.

III. FEEDBACK LOOP FOR THE IMPROVEMENT OF RELIABILITY STANDARDS

The ERO Enterprise will factor the knowledge and information gained through the implementation of these new policies into future revisions of existing NERC Reliability Standards to improve their content and clarity. NERC will also use that knowledge and information in the evaluation of patterns that may indicate potential reliability gaps or risks. The ERO Enterprise will use these trends in determining appropriate approaches to address reliability risks, developing training and guidelines, completing reliability assessments, and performing other data-based analysis. This feedback will benefit both the ERO Enterprise and registered entities. In particular, the opportunities to analyze trends to identify and educate entities on reliability risks will facilitate the improved application of resources to minimize reliability risks to the BPS.

In addition to the Standards drafting process, NERC will also ensure appropriate information flows from compliance monitoring and enforcement to other NERC programs, including Reliability Assessment and Performance Analysis, Registration and Certification, and Event Analysis.

IV. RISK-BASED COMPLIANCE MONITORING

A. Regulatory Structure

Risk-based compliance monitoring is fully consistent with NERC's existing rules and authority and does not require a change in the fundamental tenets of the Rules of Procedure (including its Appendix 4C, the CMEP). The ERO Enterprise is implementing risk-based compliance monitoring in accordance with existing rules, regulations, and orders; the framework aligns the ERO Enterprise monitoring with specific requirements set out through the Generally Accepted Government Auditing Standards ("GAGAS") and Institute of Internal Auditors ("IIA")—standard monitoring practices used in various industries. In addition to the CMEP, referenced above, NERC's program for monitoring and enforcing compliance with Commission-approved Reliability Standards is implemented through the Sanction Guidelines (Appendix 4B to the Rules of Procedure) and delegation agreements with the eight Regional Entities.

As specified in section 4.1 of the NERC CMEP, NERC develops and posts an annual Compliance Monitoring and Enforcement Program Implementation Plan ("ERO CMEP IP") each year. The ERO CMEP IP is the annual operating plan for compliance monitoring and enforcement activities to ensure that NERC and the Regional Entities fulfill their responsibilities under applicable legislation.

Beginning with the 2015 CMEP IP and beyond, NERC replaced the approach used to develop the ERO CMEP IP and the Actively Monitored List ("AML") with processes that identify and prioritize continent-wide risks to the reliability of the BPS, as well as related

Reliability Standards and registration functional categories.[11] Specifically, the ERO determines risk elements, taking into account compliance findings and event analysis experiences, data analysis provided in several NERC publications and reports, and expert judgment of ERO Enterprise staff, committees and subcommittees. Examples of such data and reports include the State of Reliability Report, the Long-Term Reliability Assessment, publications from the Reliability Issues Steering Committee, special assessments or reports, the ERO Enterprise Strategic Plan, ERO Event Analysis Process insights, significant occurrences noted by NERC and Regional Entity Situation Awareness staffs, and other relevant documents pertaining to risks to the reliability of the BPS. This revised approach continues to identify a subset of NERC Reliability Standards and Requirements for monitoring purposes, but it provides input to the development of a more individualized compliance oversight plan for registered entities. Therefore, the transformation to focus on identifying and prioritizing risks replaces a static, one-size-fits-all list of Reliability Standards and prioritizes functions and Reliability Standards based on risk to determine the appropriate oversight method.

Regional Entities use the risk elements and other information identified in the annual ERO CMEP IP in developing their own individual annual Regional Entity implementation plans ("Regional Entity IPs"). Regional Entity IPs are based on a common template, developed by the ERO Enterprise, and include: (i) details on Regional Risk Assessment processes and results; (ii) Reliability Standards and Requirements associated with Regional Risk Assessment results; (iii) Regional compliance oversight plan, which includes its annual audit plan; and (iv) other key

[11] These processes are described in the Risk Elements Guide for the Development of the 2015 CMEP IP, *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

activities and processes used for CMEP implementation. As of the time of this filing, NERC is evaluating the 2015 Regional Entity IPs that incorporate the risk elements outlined within the ERO CMEP IP for approval in accordance with section 4.2 of the CMEP.

The Rules of Procedure provide for seven compliance-monitoring processes, which are also referred to in this filing as CMEP tools (i.e., the main tools by which the monitoring program is executed). These methods include: (i) Compliance Audits; (ii) Self-Certifications; (iii) Spot Checks; (iv) Compliance Investigations; (v) Self-Reports; (vi) Periodic Data Submittals; and (vii) investigation of complaints.[12] The Rules of Procedure set forth steps for these methods, including requirements for the Regional Entity to report the results of the processes to NERC, which will then report to the Commission. The Rules of Procedure also specify the process steps after identifying registered entity noncompliance with a Reliability Standard.[13] These processes are unchanged. As discussed more fully below, all instances of noncompliance will continue to be reported and tracked at the Regional Entity, NERC, and Commission levels.

As explained below, the Regional Entity will determine the type and frequency of the compliance monitoring processes, or CMEP tools (e.g., off-site or on-site audits, spot checks or self-certifications), that are warranted for a particular registered entity based on reliability risks. The determination of the appropriate CMEP tools will be adjusted, as needed.

In selecting CMEP tools, more resource-intensive compliance monitoring activities, particularly Compliance Audits, may be used for these and other functions or entities within a

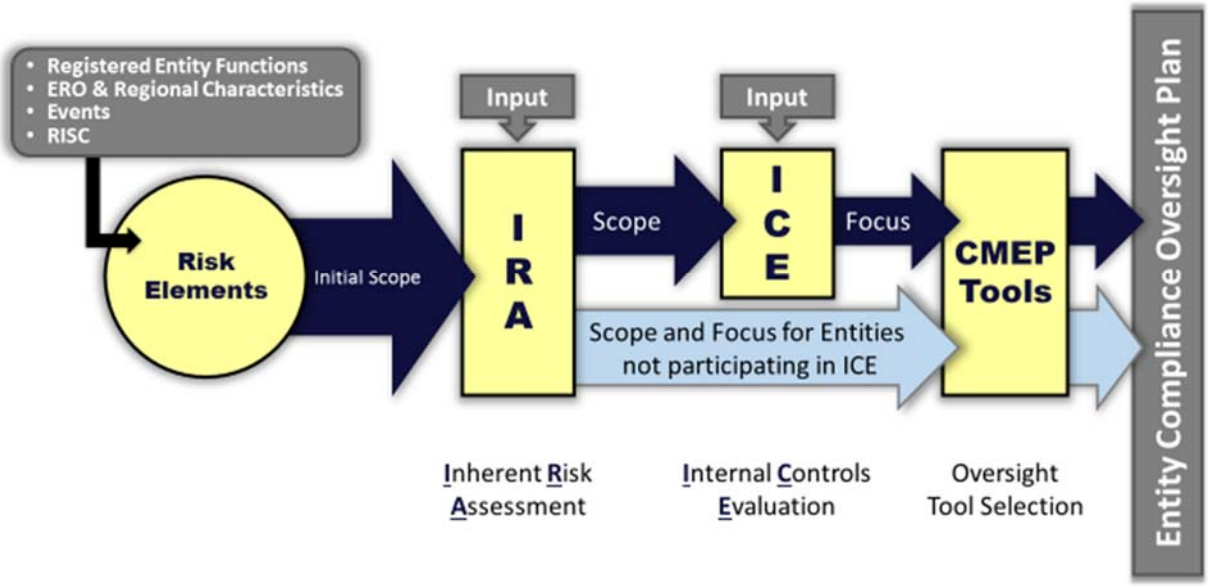
[12] CMEP §3.0 (Appendix 4C to the Rules of Procedure).
[13] *Id.* § 3.8.

specific Regional Entity that can have the most significant impact on reliability of the BPS. Functional roles or entities that have a lesser impact on reliability to the BPS may have compliance monitoring approaches tailored accordingly, for example, the use of spot checks or self-certifications, instead of Compliance Audits, may be appropriate tools in such instances. Registered entities required to be audited at a minimum three-year interval per the NERC Rules of Procedure will continue to be audited at least once every three years,[14] although the actual frequency and scope will be determined based on the Framework.

B. Risk-Based Oversight Plan Framework

RAI resulted in the development of the Framework depicted below. The Framework illustrates a number of steps including the review of system-wide risk elements, the assessment of a registered entity's inherent risk, and, as applicable, the evaluation of a registered entity's internal controls. These steps allow each CEA to establish a monitoring plan that is tailored to the risk to the BPS posed by a particular entity or group of entities. As a result, the Framework allows the ERO Enterprise to focus its resources, as well as those of registered entities, on those areas that pose the highest risk and have the greatest potential to affect reliability. Each step of the Framework is more fully discussed below.

[14] NERC Rules of Procedure, § 403.11.1.



1. Risk Elements

The first step of the Framework consists of the identification and prioritization of ERO Enterprise-wide risks. Risks are identified and prioritized based on significance, likelihood, vulnerability, and potential impact to the reliability of the BPS through a process outlined in the Risk Elements Guide for the Development of the 2015 CMEP IP ("Risk Elements Guide").[15] Risks may be categorized as operational risks and planning risks, as well as threats to cyber systems or physical security. While risk identification occurs on an annual basis, risks are dynamic. Accordingly, periodic reviews and updates may be necessary and appropriate to address increased and emerging risks or in the alternative, to reflect mitigated risks.

[15] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

Through the review of the ERO Enterprise-wide risks, the ERO develops an annual compilation of risk elements reflected in the ERO CMEP IP.[16] The ERO CMEP IP serves as guidance to Regional Entities in the preparation of their Regional Entity IP. Any needed updates will be reflected in the ERO CMEP IP on a dynamic basis. The Regional Entity IPs are subject to review and approval by NERC as required in the Rules of Procedure.[17]

Reliability Standards are in place to help ensure the reliable operation of the BPS. Through the identification of risk elements, the ERO Enterprise maps a preliminary list of applicable Reliability Standards and responsible registration functional categories to the top reliability risks identified as areas of focus for monitoring purposes. This preliminary list is reflected in the ERO CMEP IP. As discussed above, this list and the processes used to identify and prioritize continent-wide risks to reliability of the BPS, as well as related Reliability Standards and registration functional categories, replaces the AML used in prior years.

The risks and associated Reliability Standards identified through the ERO CMEP IP and Regional Entity IP processes do not reflect the entirety of the risks that may affect the reliability of the BPS. As noted in the Risk Elements Guide, issues being addressed through other mechanisms are not included as areas of focus for compliance monitoring activities.

In order to focus on a complete picture of reliability risks when determining the appropriate compliance tool, Regional Entities then consider local risks and specific circumstances associated with individual registered entities within their footprints in developing

[16] *Available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V7_090814.pdf.
[17] NERC Rules of Procedure, § 402.1.1.

their entity-specific compliance oversight plans. As a result, the scope of monitoring of a particular registered entity may include more, fewer, or different Reliability Standards than those outlined in the ERO and Regional Entity CMEP IPs.

2. Inherent Risk Assessment

After the ERO CMEP IP and Regional Entity IPs identify and prioritize risk elements, the IRA enables the CEAs to determine areas of focus and scoping of oversight for specific registered entities. As a result, the IRA identifies the Reliability Standards and Requirements that should be monitored.

The ERO Enterprise Inherent Risk Assessment Guide ("IRA Guide")[18] describes the process used to assess inherent risk of registered entities and serves as a guide for implementing and performing an IRA. As noted above, the ERO Enterprise is currently training to support the implementation and consistent application of the IRA process. In short, an IRA is a review of potential risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition. In considering such factors, a Regional Entity is not limited by the risk elements identified in the ERO CMEP IP. Rather, the IRA considers multiple factors to focus oversight to entity-specific risk. These factors may include the functional role and responsibilities of a registered entity. Risks may differ based on an entity's size, types of facilities, location, or the entity's assets, as applicable. An entity's system geography, population, and seasonal/ambient conditions may affect potential risk to reliability, as will BPS

[18] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Inherent_Risk_Assessment_Guide_20141010.pdf.

exposure (transmission, generation, and operating limitations), and interconnection points and critical paths. The existence or nonexistence of certain systems like Special Protection Systems, Undervoltage Load Shedding, Underfrequency Load Shedding, Supervisory Control and Data Acquisition ("SCADA"), and Energy Management Systems may reduce or increase exposure of the BPS to entity-specific risks. In addition to the physical systems and assets of an entity, an entity's past operational performance and compliance and enforcement history informs the IRA's selection of appropriate oversight tools.

While the IRA Guide provides guidance on risk factors and associate criteria/thresholds for Regional Entity consideration, it is important to note that certain risk factors and the associated criteria/thresholds may vary by region, by entity size, or by function. Depending on the unique characteristics of the entity, the conclusion may be that some of the listed risk factors may be more applicable or contributory than others, some may not be applicable at all, or there may be additional risk factors not listed that would be appropriate to consider. For example, while certain characteristics of a registered entity may result in a higher assignment of risk relative to that specific factor, the registered entity's size or function may mean that the risk factor itself does not merit significant consideration in determining an entity's unique inherent risks to the reliability of the BPS. This also reflects the notion that some risk factors that might contribute towards determining overall inherent risk for a larger entity may contribute differently to the evaluation of a smaller entity.

Communication between the Regional Entity and registered entity may provide critical information for a risk determination. As needed, CEAs work with the registered entity to ensure the CEA has appropriate and sufficient information to conduct the IRA and reach accurate

conclusions. After the CEA finalizes IRA results, it communicates a summary of the results to the registered entity (including risk areas and impact on the scope of monitoring).

Below are some hypotheticals and one practical example of the application of the IRA process.

In a June 2014 presentation, MRO explained how the IRA process applies to registered entities.[19] First, a Regional Entity identifies risks at the regional level and categorizes risks into reliability themes. The Regional Entity identifies how susceptible a registered entity is to well-known risk themes such as events, and includes entity-specific data, regional factors affecting reliability, compliance history, and legal or regulatory factors affecting reliability. In addition, the Regional Entity assesses each registered entity by analyzing other specific factors important to its function, such as peak load capacity, BPS exposure, interconnection points, and other resources and trends. MRO illustrated potential results for three similarly situated registered entities.

Specifically, MRO illustrated what the results would be for risk assessments of three wind plants with similar registrations, Generator Owner and Generator Operator. Before conducting the IRAs, MRO would have identified 131 applicable Requirements for each wind plant. The individual risk assessments captured unique aspects of each registered entity and allowed for a tailored monitoring scope for each. Wind Farm #1's IRA resulted in an audit scope of 20 Requirements. Wind Farm #2 was responsible for interconnection of a nuclear facility and therefore had 25 Requirements in its audit scope. Finally, Wind Farm #3, which did not own a

[19] *Reliability Assurance Initiative Update*, June 19, 2014, *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

collector bus, had two Requirements in scope. Rather than conducting a Compliance Audit, MRO could determine to use another compliance monitoring tool, such as a guided Self-Certification.

In another example, SERC conducted an IRA of Georgia Transmission Corporation ("GTC") in preparation of a Compliance Audit.[20] SERC collected and reviewed data regarding GTC's potential risks to the BPS through a pre-audit survey, reviewed GTC's compliance history, and used SERC's understanding of GTC from previous audit engagements. Based on its review of communication and coordination of operators, and GTC's related arrangements with other entities for the performance of registered functions, SERC adjusted the audit scope. Specifically, SERC increased the scope of the audit by eight Requirements.

SERC and GTC both agreed that the processes resulted in an improved focus on inherent risk when compared with the 2008 audit of GTC. SERC and GTC also learned that additional communication should occur during the development of the IRA. SERC has adjusted its communication with registered entities while conducting an IRA based on its experience with GTC.

The Regional Entity will perform IRAs on a periodic basis. The frequency may vary based on occurrence of significant changes to existing reliability risks or emergence of new reliability risks. At a minimum, a Regional Entity will be expected to consider whether IRAs should be updated when NERC identifies risk elements through the annual ERO CMEP IP. After consideration of the facts and circumstances, the Regional Entity will determine whether

[20] This experience was the subject of a presentation to the NERC Board of Trustees Compliance Committee on August 13, 2014. The presentation is available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/BOTCC%20-%20Presentation.pdf.

changes are required from year-to-year or sooner. As NERC performs oversight and observes what factors tend to trigger revisions to IRAs, NERC will consider providing additional guidance on this issue. For monitoring activities performed in 2015, Regional Entities are in various stages of conducting IRAs for registered entities within their footprints. During 2015 and beyond, Regional Entities will continue to expand the IRA process to entities in their footprints based on risk and compliance monitoring schedules.

3. Internal Controls Evaluation

An Internal Controls Evaluation ("ICE") enables a further refinement of the compliance oversight plan for individual registered entities. The ERO Enterprise Internal Compliance Evaluation Guide ("ICE Guide")[21] was developed by NERC in partnership with Regional Entities, registered entities, and various other stakeholders to assist CEAs in identifying and more effectively considering existing internal controls around CMEP objectives - compliance with Reliability Standards.[22]

[21] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf.

[22] The most generally accepted definition of the term "internal controls" comes from the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), "…a process, effected by an entity's board of directors, management and other personnel, designed to provide 'reasonable assurance' regarding the achievement of objectives…" in this case, compliance with NERC Reliability Standards. *Internal Control – Integrated Framework*, 1992, *available at:* http://www.coso.org/documents/internal%20control-integrated%20framework.pdf. In addition, GAGAS defines internal controls in a similar manner under Section 6.15 c.: "Internal control, sometimes referred to as management control, in the broadest sense includes the plan, policies, methods, and procedures adopted by management to meet its missions, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance with provisions of laws, regulations, contracts or grant agreements; or

Considering internal controls in the scope of audits is required under GAGAS.[23] The ICE is NERC and the Regional Entities' effort to formalize and standardize internal controls evaluation in a broader manner to complement risk-based monitoring of compliance through the IRA and using the breadth of CMEP monitoring tools more effectively. ICE refines the focus on those controls related to the entity-specific risks identified through the IRA and germane to the applicable Reliability Standards and allows CEA staff to leverage the entire breadth of CMEP tools more effectively, including to determine whether a Compliance Audit is necessary. During an ICE, Regional Entities may use existing information from past work with the Registered Entity, such as past audits, mitigation plans, previous Internal Compliance Program reviews conducted through enforcement. Registered entities have an opportunity to provide, on a voluntary basis, additional information related to the ICE including details that demonstrates the effectiveness of detective, corrective, and compensating controls. Because of the ICE, the Regional Entity may further focus the compliance assurance activities for a given entity. The depth and breadth of any particular area of review may decrease based on the Regional Entity's conclusions on its ability to rely on the internal controls of the registered entity. For example, if a registered entity demonstrates effective internal controls for a given Reliability Standard, the Regional Entity may determine that it does not need to audit the registered entity's compliance with that Reliability Standard as frequently or select a different monitoring tool. Conversely, if a registered entity does not demonstrate effective internal controls for a given Reliability Standard during the ICE, the scope will not change from the IRA.

abuse." Government Auditing Standards: 2011 Revision (Reissued on Jan. 20, 2012) p. 131, *available at:* http://gao.gov/assets/590/587281.pdf.

[23] See GAGAS Section 6.16.

Because the controls to be evaluated pursuant to the ICE process are those related to the inherent risk posed by a particular registered entity, the extent of an evaluation will naturally vary in accordance with that inherent risk.

Below are some examples of the application of the ICE process.

In the June 2014 presentation mentioned above, MRO provided examples regarding the evaluation of internal controls.[24] The first example involved a review of American Transmission Company's ("ATC") internal controls related to Reliability Standard COM-002. In this example, ATC's preventive control involved a random review of operator communications, followed by feedback and corrective actions. The review showed that ATC used three-part communication for routine exchanges. In addition, ATC's detective control involved a complete review of any situation in which a directive may be issued. MRO concluded that ATC would identify and address issues on a timely basis. Therefore, MRO determined that it did not need to directly test compliance with Reliability Standard COM-002.

The second example related to the Protection and Control ("PRC") family of NERC Reliability Standards. ATC had implemented preventative controls that tracked activities and alerted any upcoming or missing tests. ATC also had detective controls that involved random monthly management review of 10% of maintenance and testing records. MRO concluded that ATC had internal controls for all of the requirements related to maintenance and testing intervals. Thus, the result allowed for reduced sampling for the related PRC Reliability Standards.

[24] *Reliability Assurance Initiative Update*, June 19, 2014, *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

In another example, in preparation for a Compliance Audit, SERC evaluated GTC's internal controls. As part of its evaluation, SERC reviewed GTC's independent audit reports, and accepted the independent audit report findings for 18 of the 38 Requirements in scope. Therefore, SERC did little to no additional testing in these areas. In reaching its conclusions, SERC determined that the independent audit reports: (i) adequately addressed the applicable Reliability Standards and Requirements; (ii) were relevant to the audit period; and (iii) reflected an appropriate level of rigor for SERC staff to draw the same conclusions.

The CEA is ultimately responsible for evaluating internal controls to determine proper oversight scope (i.e. the extent of reliance on internal controls for applicable Reliability Standards). The CEA makes this determination by understanding the BPS risks to which the registered entity is susceptible and gaining an understanding of how the registered entity controls or mitigates those risks in a meaningful manner. When the CEA has reasonable assurance that internal controls are functioning to protect reliability in accord with Reliability Standards, the CEA may rely on those internal controls and therefore, extensive testing may not be necessary.

Depending on regional flexibility and available resources, a CEA may conduct an ICE outside of normal compliance monitoring processes. However, the ERO Enterprise anticipates that during 2015, Regional Entities will generally only conduct an ICE in preparation for a scheduled compliance monitoring activity, e.g., a Compliance Audit.

The complexity of internal controls and the CEA evaluation of such internal controls will be scaled in accordance with the size of the registered entity, as described in the ICE Guide. However, it is possible that after the IRA, few applicable standards may remain as part of the monitoring scope for an entity posing a small inherent risk. In that case, it is possible that an

ICE may not result in a significant further tailoring of monitoring activities. Nevertheless, the ICE provides, even for those entities, an opportunity for continuous improvements in controls that could increase reliability and mitigate risks.

4. CMEP Tools

Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (i.e., off-site or on-site audits, spot checks or self-certifications)[25] that are warranted for a particular registered entity based on reliability risks. The determination of the appropriate CMEP tools will be adjusted, as needed, within a given implementation year. Regional Entities' IPs may indicate CMEP tools being used during the implementation year (e.g., audit schedules, self-certifications, or periodic data submittals), but the Regional Entity will continue to identify appropriate CMEP tools to use based on results from regional risk assessments, IRAs, and ICEs.

NERC is currently reviewing the 2015 Regional Entity IPs for approval as provided in the Rules of Procedure. These region-specific plans provide the inputs and considerations that impact the development of compliance oversight plans for registered entities. Regional Entity IPs identify how the Regional Entities will use various compliance monitoring tools, such as on- and off-site audits. For example, prior to 2015, Regional Entities conducted audits for all entities on a three- and six-year audit cycle. Using a risk-informed approach, Regional Entities will continue to conduct three-year audits per the Rules of Procedure. However, a registered entity's IRA, and ICE if used, will determine the frequency and Compliance Audit scope rather than a standardized approach based solely on the registered function and the applicability of

[25] CMEP §3.0 (Appendix 4C to the Rules of Procedure).

Requirements contained in an actively monitored list. In their 2015 Regional Entity IPs, the Regional Entities identified registered entities scheduled for Compliance Audits in 2015. However, all registered entities are subject to oversight, and additional registered entities, at the discretion of the Regional Entity, may also be subject to compliance monitoring in 2015.

C. Planning and Execution of Compliance Audits

Compliance Audits remain a relevant part of the ERO Enterprise's risk-based approach to compliance monitoring. Pursuant to the NERC Rules of Procedure, each Regional Entity must maintain and implement a program of proactive Compliance Audits of BPS owners, operators, and users responsible for complying with Reliability Standards.[26] Further, a Compliance Audit of an entity registered as a Balancing Authority, Reliability Coordinator, or Transmission Operator must occur at least once every three years.[27] However, the time since the last audit is no longer the main driver for the audit planning process. Instead, as explained above, NERC and the Regional Entities will look to other key criteria to measure risk to the BPS, including entity processes, controls, and compliance history in determining the appropriate compliance monitoring tool for a particular registered entity. In 2015, some Regional Entity IPs may include Compliance Audits that were scheduled prior to full implementation of risk-based compliance monitoring. Beginning in 2016, however, the decision to conduct a Compliance Audit or select a different monitoring tool should be made in accordance with the risk-based processes outlined herein.

[26] NERC Rules of Procedure, § 403.11.
[27] *Id.* § 403.11.1.

Risk-based audit principles and risk-based auditing are fully consistent with practices of other agencies, including for example, the Division of Audits and Accounting ("DAA") within FERC's Office of Enforcement. As DAA explained in the 2013 Staff Report on Enforcement, "Risk assessment continues to be an important aspect of DAA's audit program because a significant majority of audits are initiated without any allegation of wrongdoing. Audited entities are typically selected using risk-based criteria[.]"[28]

Moving from a strictly time-based audit cycle to a risk-based audit cycle will improve oversight of the reliability of the BPS. If a registered entity now on a minimum three-year audit schedule poses substantial risk to the reliability of the BPS, its CEA may schedule audits more frequently than every three years. Similarly, for registered entities not subject to the three-year cycle, CEAs will monitor these entities, and base compliance monitoring activities' frequency, depth, and breadth on that entity's specific risk to BPS reliability. The ERO Enterprise will also continue to use other compliance monitoring tools such as self-certifications and spot checks. Again, the use and application of compliance monitoring tools will vary based on the risk-based processes outlined above to create the best method for effective oversight of compliance with Reliability Standards.

As the ERO Enterprise implements a risk-based approach to monitoring compliance with Reliability Standards, NERC and the Regional Entities recognize the need for continued CEA

[28] *2013 Report on Enforcement*, Docket No. AD07-13-006, p. 29 (Nov. 21, 2013), *available at:* http://www.ferc.gov/legal/staff-reports/2013/11-21-13-enforcement.pdf.

staff training and additional tools, in addition to and in support of NERC oversight. For example, the ERO Enterprise Compliance Auditor Manual ("Manual"),[29] which includes the Compliance Auditor Handbook, is a recent tool developed to assist CEA staff.

NERC and the Regional Entities jointly developed the Manual to help improve consistency and quality of compliance monitoring across the ERO Enterprise. The Manual, which the Regional Entities adopted and began using in April 2014, contains common tools, techniques, and approaches for compliance auditors. The Manual Drafting Team completed the first draft of the Manual in December 2013 and provided it to the NERC and Regional Entity executive management for review and comment. The Manual is a living document, and revisions will occur as NERC and the Regional Entities improve, develop, and implement compliance monitoring processes. Currently, the Manual includes sections on: an Introduction to Compliance Auditing, the Compliance Auditor Handbook, and the Compliance Auditor Capabilities and Competency Guide. Additional sections continue to be developed for the Manual, including: Ethics and Standards, sampling methodology, supporting diagrams and flow charts, common forms and templates, and other content as needed.

Following the completion of the Manual, NERC and the Regional Entities supported the formal roll-out with training initiatives, information sessions, and workshops. NERC began roll-out and initial training to regional auditors on use of the Manual during the first quarter of 2014, with full implementation in the second half of 2014 and use for all audits scheduled in 2015. NERC and the eight Regional Entities also jointly developed communication and training

[29] *ERO Enterprise Compliance Auditor Manual, available at*: http://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/ERO_Enterprise_Compliance_Auditor_Manual_version_1.pdf.

activities. Training modules consisted of a series of presentations, exercises and, on-line and instructor-led training. As tools and processes evolve, they will be added to the Manual, with the development and administering of training to follow. NERC and the Regional Entities continue to incorporate the Manual as part of periodic training for compliance auditors, such as Auditor Team Lead training. In addition, NERC and the Regional Entities have established a process for Manual additions, enhancements, and updates. In addition to training, mid- and long-range revision management and maintenance are being developed to ensure the long-term sustainability of the document. Additionally, in 2015, NERC will perform oversight activities of the Regional Entities to support implementation and process improvements related to the use of the Manual.

V. RISK-BASED ENFORCEMENT

A. FFT as the Platform for the Evolution of a Risk-based Enforcement Program

Over the past several years, the ERO Enterprise has been enhancing its risk-based approach for assessing and processing noncompliance. The ERO Enterprise continues to expect identification and mitigation of all instances of noncompliance, regardless of the level of risk they posed to the reliability of the BPS. However, not all instances of noncompliance require the same level of documentation and processing. The overwhelming majority of the caseload processed by the ERO Enterprise over the years has posed a minimal or moderate risk to the

reliability of the BPS.[30] As a result, it is appropriate to use a variety of means to resolve noncompliance, including the exercise of discretion not to initiate a formal enforcement action.

Since 2011, the ERO Enterprise has used the FFT process to resolve over 2,000 instances of noncompliance with the Reliability Standards, most of which posed a minimal risk to the reliability of the BPS. Since June 2013, the FFT process has been used to resolve noncompliance posing a moderate risk to the BPS.[31] Building on the success of the FFT process, the ERO Enterprise identified and implemented additional processes that enhance its effectiveness while promoting and supporting reliability.

The processes discussed below further streamline the resolution of lesser-risk noncompliance with NERC Reliability Standards. This continued evolution is necessary to allow the ERO Enterprise, as well as industry, to allocate resources to address the issues posing a higher level of risk to reliability. In addition, this approach leverages registered entity existing internal practices relating to self-monitoring and assessment of compliance with Reliability Standards. By appropriately recognizing such efforts, the ERO Enterprise encourages the

[30] In 2012 and 2013, respectively, the ERO Enterprise handled 74% and 72% of the violations and issues posted or filed at FERC as FFTs or in Spreadsheet Notice of Penalty filings. Both of these disposition methods are used for only minimal or moderate risk noncompliance. *NERC Compliance Violation Statistics—Fourth Quarter 2013*, at 10, *available at:* http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx. In addition, in 2013 and 2014, respectively, 72% and 70% of instances of noncompliance posed a minimal risk to the reliability of the BPS and 27% (in both years) posed a moderate risk. From 2012 through October 1, 2014, only 2% of violations posed a serious or substantial risk to the reliability of the BPS.

[31] *North American Electric Reliability Corp.*, 138 FERC ¶ 61,193 ("2012 FFT Order"), *order on reh'g*, 139 FERC ¶ 61,168 (2012) (approving FFT program); *North American Electric Reliability Corp.*, 143 FERC ¶ 61,253 (2013) (approving expansion of program to include moderate risk issues and issues that will be mitigated within 90 days of posting, as well as proposal to publicly post FFT issues in lieu of submitting an informational filing); and *North American Electric Reliability Corp.*, 148 FERC ¶ 61,214 (2014) (approving continued inclusion of moderate risk issues as well as expansion of program to include issues that will be mitigated within one year of posting, subject to conditions).

enhancement of internal controls and self-identification of noncompliance throughout the industry.

Based on the experience with a streamlined process and a reduced record for resolution of minimal risk noncompliance, since 2013, NERC and the Regional Entities have exercised discretion when deciding whether to initiate a formal enforcement action regarding certain instances of noncompliance posing a minimal risk to the reliability of the BPS. Noncompliance that is not pursued through a formal enforcement action by the ERO Enterprise is referred to as a "compliance exception." As of September 30, 2014, a total 54 instances of noncompliance have received compliance exception treatment.

Beginning in October 2013, NERC and the Regional Entities began to allow select registered entities with demonstrated effective management practices to self-identify, assess, and mitigate instances of noncompliance to self-log minimal risk noncompliance that would otherwise be individually self-reported. Properly logged items are entitled to the presumption of being resolved as compliance exceptions unless there are additional risk factors involved. Logged items will be periodically filed with the Regional Entity. The Regional Entity will validate the logs. This is consistent with the notion that noncompliance that is self-identified through internal controls, corrected through a strong compliance culture, and documented by the entity, should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the BPS.

B. Regulatory Structure and Identification of the Risk Posed by Noncompliance

Section 3.8 of the CMEP, which describes what each CEA must do once it identifies a potential noncompliance with a Reliability Standard Requirement, provides, in part that:

> 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, unless an alternative enforcement process is used. (emphasis added)

Section 5.0 of the CMEP, which describes the processes associated with Enforcement Actions, further provides that:

> The following enforcement process is undertaken by the Compliance Enforcement Authority following identification of a Possible Violation of 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. The Registered Entity shall be entitled to object to the use of any such other approach. (emphasis added)

These provisions allow the ERO Enterprise to use alternative processes that are appropriate, efficient, or desirable means to achieve the overall objectives of the CMEP. The resolution of noncompliance as compliance exceptions through the process described herein is such an alternative approach for the resolution of lesser-risk noncompliance that is fully consistent with the overall objectives of the CMEP.

The Commission has expressed support for NERC and the Regional Entities to use risk-based compliance and enforcement processes, including using appropriate discretion when determining how to treat low-risk instances of noncompliance. For example, in its order approving Version 5 of the Critical Infrastructure Protection Reliability Standards, the Commission stated:

> We understand that NERC has inserted the "identify, assess, and correct" language into the CIP Reliability Standard requirements to move its

> compliance processes towards a more risk-based model. With this objective in mind, we believe that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards.[32]

A common understanding of how the ERO Enterprise determines the various levels of risk of instances of noncompliance is fundamental to the continued evolution of the risk-based enforcement program. The ERO Enterprise uses three different levels to identify the risk posed by any instance of noncompliance: "serious and substantial," "moderate," and "minimal." The analysis that is performed is based on prior Commission orders and is discussed in the ERO Enterprise Self-Report User Guide.[33]

In the Commission's 2012 FFT Order, the Commission agreed that examples of serious and substantial issues are those involving or resulting in (i) extended forced outages; (ii) loss of load; (iii) cascading blackouts; (iv) certain vegetation contacts; (v) systemic or significant performance failures; (vi) intentional or willful acts or omissions; (vii) gross negligence; and (viii) other misconduct.[34] The ERO Enterprise concentrates its efforts on such serious and substantial issues when they infrequently arise. NERC files serious and substantial matters with the Commission in Full Notices of Penalty.

---

[32] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160, P 75 (2013).

[33] *See ERO Self-Report User Guide*, pp. 11-13 (April 2014), *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf (describing the guidelines to help Registered Entities assess the risk to the reliability of the BPS posed by noncompliance with a Reliability Standard). *See also* the 2012 FFT Order, 138 FERC ¶ 61,193, at PP44-45 (FERC discussion of risk assessments including a review of actual versus potential risk).

[34] *Id.* P49.

Issues are determined to pose a minimal risk to BPS reliability based on the combination of the subject Reliability Standard requirement and the attendant facts and circumstances. If nothing serious could have occurred and there were complete or significant protections in place to reduce the risk, as a general matter, then the risk would likely be minimal.

The lack of harm is not sufficient justification, by itself, for a minimal or moderate risk assessment. The facts and circumstances leading to a moderate risk determination are necessarily different. If something serious could have occurred during a noncompliance and there were only some protections in place to reduce the risk, then the risk assessment would likely be moderate.[35] If the noncompliance is related to a serious event, then the risk would likely be serious and substantial. Examples of serious harm generally include loss of customer load, cascading outages, and malicious actions that affect Critical Assets.

The determination of the level of risk posed by instances of noncompliance resolved through an enforcement action is clearly identified in the Notice of Penalty or FFT spreadsheet. Numerous examples of these determinations are available on the Enforcement and Mitigation page of the NERC website.[36]

C. Compliance Exceptions

Consistent with the above, beginning in November 2013, the ERO Enterprise implemented, on a pilot basis, a method to expand the exercise of enforcement discretion by identifying minimal risk instances of noncompliance that do not warrant a penalty and which

[35] *See ERO Self-Report User Guide*, 11-13 (April 2014), *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf (describing the guidelines to help Registered Entities assess the risk to the reliability of the BPS posed by noncompliance with a Reliability Standard). *See also* 2012 FFT Order at PP44-45 (2012) (FERC discussion of risk assessments including a review of actual versus potential risk).
[36] *Available at:* http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

would be recorded and mitigated as a "compliance exception" without triggering a formal enforcement action under section 5.0 of the CMEP.

As noted above, the process of identifying and recording compliance exception builds on the FFT program. The exercise of discretion by the ERO Enterprise is informed by the facts and circumstances of the noncompliance, the risk posed by the noncompliance to the reliability of the BPS, and the deterrent effect of an enforcement action or penalty, among other things. These considerations are very similar to the considerations that have been used since 2011 to determine whether noncompliance should be processed as an FFT.[37]

Compliance exception is an alternative disposition method and is not a dismissal, FFT, or Notice of Penalty. It is essentially the exercise of enforcement discretion with respect to a noncompliance regardless of its method of discovery (self-report, self-certification, audit finding, etc.).

When an instance of noncompliance is disposed of as a compliance exception, NERC does not publicly post it as in the case of an FFT or file it with the Commission as in the case of a Notice of Penalty. Rather, the Regional Entity retains the record for the compliance exception and provides NERC, through non-public means, a summary of the record. NERC then submits the compliance exceptions to FERC through non-public means.

A compliance exception is part of a registered entity's compliance history only to the extent it serves to inform the Regional Entity and NERC of the minimal risk issues that are detected and corrected by the registered entity, and may inform the Regional Entity's decision on how to treat future noncompliance with the same or similar facts. It should be noted that repeat

[37] *See, e.g.*, 2012 FFT Order at PP17-21.

compliance exceptions may not always be indicative of poor performance; they may in fact be evidence of robust controls in place to detect and correct instances of noncompliance as they occur. A registered entity may object to resolution of any issue as a compliance exception by providing written notification to the Regional Entity within seven days of the communication by the Regional Entity. In the event a registered entity objects to resolution as a compliance exception, the noncompliance will be resolved through one of the other enforcement processes established in the CMEP at the discretion of the Regional Entity.[38]

1. Instances of Noncompliance that Qualify for Recording as Compliance Exceptions

Minimal risk instances of noncompliance are eligible for processing as compliance exceptions regardless of the discovery method. Regardless of the discovery method, however, the noncompliance is recorded and tracked and reviewed by the Regional entity. As noted above, all compliance exceptions are also provided to NERC and FERC.

The Regional Entity determination of whether an instance of noncompliance is eligible for compliance exception treatment is essentially the same as the process it has been using, since 2011, to make a determination of eligibility for FFTs posing a minimal risk to the reliability of the BPS.[39] Regional Entities focus on the underlying facts and circumstances of the noncompliance, including what happened, why, where, and when. Another factor Regional Entities use to determine whether a noncompliance should be eligible for compliance exception treatment is the potential and actual level of risk to reliability, including mitigating factors during the pendency of the noncompliance. Regional Entities consider the registered entity's internal

[38] CMEP (Appendix 4C to the Rules of Procedure) § 5.0 Enforcement Actions.
[39] *See, e.g.*, 2012 FFT Order at PP17-21.

compliance program ("ICP"), including preventative and corrective processes and procedures, management practices, and culture of compliance as factors to help determine whether a noncompliance should receive compliance exception treatment. A robust ICP with strong management practices around Reliability Standards that led to timely discovery and swift mitigation of noncompliance creates a strong argument in favor of compliance exception treatment. Regional Entities also consider the presence and applicability of aggravating factors, such as repeat or repetitive noncompliance. An instance of noncompliance may be eligible for compliance exception treatment even if a registered entity has negative compliance history with a same or similar standard. This ensures that NERC and the Regional Entities do not discourage registered entities from robustly self-reporting noncompliance. However, repeat noncompliance should lead to a deeper look into root causes of mitigation failure and an examination of the connection between the registered entity's ICP, applicable organizational and management practices, and its day-to-day adherence to Reliability Standards in operations.

At this time, only noncompliance posing a minimal risk to the reliability of the BPS is eligible for compliance exception treatment. NERC's annual review of the program will consider the inclusion of moderate risk issues in the future.

2. Applicability throughout ERO Enterprise

Throughout the ERO Enterprise, a noncompliance can qualify for compliance exception treatment in two ways. The first way that noncompliance can qualify for compliance exception treatment is on a case-by-case basis; an individual issue is deemed to have posed a minimal risk to the reliability of the BPS and does not warrant a penalty, as discussed above. Beginning in 2015, this discretionary treatment will be available for any qualified minimal risk

noncompliance, regardless of the registered entity or discovery method, or version of the Reliability Standard and Requirement. The resolution of the noncompliance, including whether it may be resolved as a compliance exception, is based, as noted above, on a review of specific facts and circumstances.

The second way in which noncompliance posing a minimal risk to the reliability of the BPS can be resolved as a compliance exception is through the self-logging program. As explained below, noncompliance that is self-logged is presumed to be appropriate for disposition as a compliance exception. This approach, however, is limited to registered entities designated by the Regional Entity as eligible for self-logging.

As Regional Entities increase use of the compliance exception process for minimal risk issues in 2015 and beyond, the FFT process will remain available for processing of any minimal or moderate risk issue. However, it is likely that the FFT process would be used primarily to process those moderate risk issues that qualify, and minimal risk issues, when appropriate, would be disposed of as compliance exceptions. The FFT process will remain an available processing method for issues that do not qualify for compliance exception treatment when the facts and circumstances, mitigation, internal controls, and other factors, such as the registered entity's compliance history, make a monetary penalty and resolution through a Notice of Penalty filing inappropriate.

3. Processing and Recording of Compliance Exceptions

All noncompliance, including that which is eligible for compliance exception processing, is entered into the Regional Entity system, given a tracking ID, and undergoes the triage process. Upon determination that an item will be disposed of as a compliance exception, the Regional

Entity provides information regarding said item to NERC through nonpublic means. The information provided to NERC includes the relevant Reliability Standard and Requirement, a brief description of the noncompliance, an assessment of the risk to the BPS posed by the issue, and a description of the actions taken (or to be taken) to mitigate the issue and prevent recurrence.

Compliance exceptions must be mitigated within twelve months of the time of the communication to the registered entity resolving the matter without an enforcement action.[40] The timing of completing mitigating activities is not always associated with the risk posed by the noncompliance.[41] Consistent with the Commission's direction in its recent FFT order,[42] in the event Regional Entities dispose of a matter that has yet to be mitigate as a compliance exception, the record must clearly indicate (i) the expected completion date, (ii) the justification for the length of time required, and (iii) a description of all compensating measures in place during the period of noncompliance which reduce the risk to reliability while mitigation is ongoing. NERC will in turn provide this information to Commission staff. In addition, NERC will notify FERC staff when the mitigation is completed for each compliance exception with an extended mitigation period.

[40] Some issues, despite their posing a lower risk, require mitigating steps that may require extra time to complete. Therefore, with the understanding that setting an abbreviated timeframe for mitigation completion as a condition of compliance exception processing does not always accurately reflect the risk posed by the noncompliance, the ERO Enterprise set a twelve-month mitigation completion timeframe for compliance exceptions. *See North American Electric Reliability Corp. Compliance Filing and Report on the Find, Fix, Track and Report Program*, Docket No. RC11-6-004 at pp. 47-49 (June 20, 2014).
[41] *Id.*
[42] *North American Electric Reliability Corp.*, 148 FERC ¶ 61,214 at P 37 (2014).

This mitigation completion period is not intended to allow every issue receiving compliance exception treatment to be unmitigated by the time of the determination. Rather, it is intended to allow flexibility for the Regional Entities to provide appropriate treatment, even for those instances of noncompliance that require additional time for mitigation.[43] The ERO Enterprise goal for the allowance of extended completion periods is to provide appropriate flexibility to ensure full mitigation, not to encourage the delay of mitigation activity. In fact, despite the fact that the ERO Enterprise may exercise discretion over noncompliance that is capable of being mitigated within twelve months, not all minimal risk matters with open mitigating activities may be appropriate for compliance exception treatment. Indeed, where NERC and the Regional Entities determine such mitigating activities are not prompt or are otherwise unnecessarily delayed, NERC and the Regional Entities will evaluate the totality of the facts and circumstances when assessing an appropriate disposition method.

Registered entities will notify the Regional Entity of completion of mitigation through an authorized representative of the registered entity (including through electronic means). The Regional Entity will track mitigation completion and will notify NERC of that completion. Failure to complete mitigation in the established timeframe, or any material misrepresentation of information provided in connection with this program, will result in rescission of the eligibility for compliance exception treatment.

A compliance exception notice indicates to a registered entity that the Regional Entity has completed its review of the matter.

[43] *North American Electric Reliability Corp. Compliance Filing and Report on the Compliance Enforcement Initiative and Proposed Enhancements to the Find, Fix, Track and Report (FFT) Program*, Docket No. RC11-6-004 at pp. 40-41 (March 15, 2013).

4. Experience Gained during Pilot Phase

From November 2013 to the present, Regional Entities have been selecting compliance exception candidates from minimal risk noncompliance. This approach allowed the ERO Enterprise to implement the program gradually and refine the program requirements and processes. As of September 30, 2014, a total of fifty-four instances of noncompliance have been treated as compliance exceptions. Twenty-two compliance exceptions (41%) were low-risk CIP noncompliance; the remaining thirty-two compliance exceptions (59%) were non-CIP noncompliance. Fifty percent of the compliance exceptions were discovered in 2014. Twenty-five (46%) compliance exceptions were externally identified by Regional Entities (Compliance Audits, Spot Checks, or Investigations) and twenty-nine (54%) were internally identified by registered entities. NERC has included in its regular presentations to its Board of Trustees Compliance Committee information on compliance exceptions including levels of utilization, representative examples, and other data.

5. Visibility and Accountability

While the Regional Entity reports all instances of noncompliance to NERC, unlike an enforcement action, compliance exceptions are not filed or publicly posted.

There are, however, various ways for communicating to the public useful information regarding the overall rationale for decisions not to pursue certain matters as well as regarding the use of compliance exceptions throughout the ERO Enterprise. For example, NERC has published a Compliance Exceptions Overview document on its website.[44] This document

[44] Compliance Exceptions Overview, *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf.

describes the aspects of the compliance exceptions, including eligibility requirements, mitigation requirements, finality, and how visibility and accountability will be maintained as the program is implemented and expanded across the ERO Enterprise. In addition, to ensure that the public can derive the maximum value of information regarding compliance exceptions without altering the message that these issues are generally not ones worthy of significant attention, NERC will make an annual informational filing to FERC reviewing the progress of the program and considering any enhancements or expansions that may be necessary. The annual report will include observed trends by standard, region or other categories. The report will also include examples of matters treated as compliance exceptions. Similar information will also be reported on a regular basis to the NERC Board of Trustees Compliance Committee.[45]

Non-public enforcement discretion is consistent with other regulatory regimes, including the Commission's. In FERC investigations closed without any action, the existence of the investigation remains non-public in all but rare circumstances.[46] In fact, in the Revised Policy Statement on Enforcement issued May 15, 2008, FERC noted that between 2005 and 2007, "Enforcement staff closed approximately 75 percent of its investigations without any sanctions being imposed, even though Enforcement staff found a violation in about half of those closed investigations. … Additionally, more than half of the self-reports submitted to FERC

[45] An example of the information submitted publicly to the Board of Trustees Compliance Committee is available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/November%2012%20Compliance%20Committee%20Agenda%20Package.pdf.
[46] *See* 18 C.F.R. Part 1b (2014).

Enforcement staff were closed with no action."[47] From 2007 through 2013, FERC Office of Enforcement, Division of Investigations staff closed approximately 50 percent of its investigations without imposing sanctions—many with findings of violation.[48] The rare circumstances in which FERC does publish both the existence and the results of its investigations underscore their importance and allow FERC to communicate the importance of such matters to the regulated community.

Indeed, an enforcement agency should not, as a general matter, provide precise indications of where the bar is for its exercise of discretion. The Freedom of Information Act acknowledges this rationale in permitting a U.S. agency to withhold law enforcement records that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law[.]" 5 U.S.C. § 552(b)(7)(E).

There is also a privacy issue for those registered entities involved where no formal determination regarding a violation has been made. An entity's reputation could be adversely impacted if disclosed, even though there was no formal determination regarding a violation. In the context of investigations, the Commission has acknowledged that "premature disclosure could adversely affect the reputation of the subject. Public disclosure at the outset of an

[47] *Revised Policy Statement on Enforcement*, 123 FERC ¶ 61,156, P 9 (2008) (2008 Revised Policy Statement).
[48] *2013 Staff Report on Enforcement*, Docket No. AD07-13-006 pp. 22-25 (November 21, 2013) *available at:* http://www.ferc.gov/legal/staff-reports/2013/11-21-13-enforcement.pdf.

investigation would risk exposing the subject to undue public suspicion without staff having conducted sufficient discovery to reach a preliminary finding that the subject may have violated a Commission requirement."[49] In the instance of a compliance exception, the CEA does not reach a determination regarding a violation. Therefore, public disclosure could "expose the subject to undue public suspicion."[50]

The nonpublic nature of compliance exceptions also reinforces the need for registered entities to shift focus and attention to higher-risk noncompliance, which is made public. The continuation of publicly posting the resolution of minimal risk noncompliance would dilute the message that is sent through the public disposition of higher-risk matters. As indicated above, trends and analysis associated with such minimal risk noncompliance may be educational or otherwise helpful, and will be provided to the public regularly. However, posting of individual accounts of trivial instances of noncompliance does not provide a benefit and diverts resources from the ERO Enterprise that should be allocated elsewhere. To illustrate this point, the following are examples of minimal risk instances of noncompliance that received compliance exceptions treatment.

- During an internal review, the entity identified that after an internal reorganization took place a year earlier, it had failed to document changes to the CIP senior manager within 30 calendar days of the effective date. The primary cause for the noncompliance was a lack of knowledge by the Primary Compliance Contact, who had been responsible for documenting the change, because the person had been in the position approximately six months at the time of the management change. The risk was minimal because the entity has no Critical Assets and is a small size utility.

[49] *Enforcement of Statutes, Regulations, and Orders*, 129 FERC ¶ 61,247 at P5 (2009); *order on reh'g.*, 134 FERC ¶ 61,054 (2011).
[50] *Id.*

- An entity self-identified that it had missed three work orders associated with three separate batteries each located at different generation facilities. The three instances of monthly frequency missed were from prior years and despite the missed work orders, the three batteries involved had been tested and maintained per prescribed frequency defined by the entity's program on a consistent basis.

- An entity self-identified that it failed to revoke access to Critical Cyber Assets (CCAs) within seven calendar days for personnel who no longer required such access to CCAs. The noncompliance was related to one employee who started working remotely and therefore did not need physical access to the CCAs. The helpdesk misinterpreted the email notification as no access removal is required since the employee is now working remotely.

The review, by the public, of these and other individual accounts of trivial, minimal risk noncompliance does not promote the reliability of the BPS.

6. Oversight by NERC

As discussed above, the resolution of noncompliance as compliance exceptions does not eliminate or reduce oversight or visibility regarding minimal risk noncompliance. NERC will continue to provide oversight of the program. All noncompliance, including that which is eligible for compliance exception processing, will continue to be entered into the Regional Entity compliance data systems and assigned a tracking identification number. Upon its determination that an item will be disposed of as a compliance exception, the Regional Entity will provide information to NERC on a monthly basis. The record will include the relevant Reliability Standard and requirement, a description of the issue, an assessment of the risk to the reliability of the BPS posed by the issue, and the actions taken (or to be taken) to mitigate the issue and prevent recurrence. As with all identified instances of noncompliance, NERC provides the information submitted by the Regional Entity to the Commission through non-public portals.

In 2014, NERC will continue to review all compliance exceptions. Beginning in 2015, however, NERC will, in a manner similar to its oversight of FFT, review a sample of compliance exceptions on a regular basis and provide guidance or adjustments on a prospective basis.

D. Self-logging Program

Beginning in October 2013, NERC and certain Regional Entities began to allow select registered entities with demonstrated effective management practices to self-identify, assess, and mitigate instances of noncompliance to log minimal risk noncompliance that would otherwise be individually self-reported. The logs contains a detailed description of the issue, the risk assessment with factual support, and the mitigating activities completed or to be completed by the Registered Entity. The log is periodically reviewed and approved by the Regional Entity (or in the case of multi-regional logs, Regional Entities). Logged items are presumed to be resolved as compliance exceptions once reviewed and approved by the Region(s). In that review and approval process, the Regional Entity determines that the issue is described accurately, that the minimal risk determination is justified and reasonable, and that the issue is adequately mitigated. This is consistent with the principle that minimal risk noncompliance that is self-identified, corrected, mitigated, and documented by the entity, should not be resolved through the formal enforcement process or incur a penalty absent a higher risk to the BPS.

The program relies on and promotes a closer understanding by Regional Entities of registered entities' management practices. In addition, it creates motivation and incentives for registered entities to implement effective controls to detect and correct instance of noncompliance as they arise. Registered entities currently participating in the program report that they see a significant benefit, particularly associated with the presumption that logged items

will be resolved as compliance exceptions and the efficiency gains associated with streamlining the processing of self-reports and mitigation plans.

1. Eligibility to Participate in the Program

In determining eligibility, the Regional Entities consider whether a registered entity is capable of self-identifying and mitigating minimal risk noncompliance on its own, as demonstrated by, among other things: (i) the registered entity's history of initiative and recognition of compliance obligations; (ii) the registered entity's reliable and accurate self-reporting of noncompliance to the Regional Entities; (iii) the registered entity's history of mitigating its noncompliance in a timely and thorough manner; (iv) the quality, comprehensiveness, and execution of the registered entity's internal compliance program; (v) the registered entity's cooperation with the Regional Entity during enforcement actions, compliance monitoring activities, and Regional Entity outreach; and (vi) the registered entity's performance during regional Compliance Audits.

An ICE, if performed, informs a Regional Entity's decision regarding participation in the self-logging program, but is not a prerequisite for participation. In fact, as noted above, an ICE may not always be necessary given the inherent risk posed by a particular entity for a particular function. However, the Regional Entity may inquire as to the internal controls in place to self-monitor and then identify, assess, and correct issues for which the registered entity is allowed to log minimal risk noncompliance. This inquiry will be scaled in accordance with the risk posed by the registered entity.

Eligibility for the self-logging program is not an all-or-nothing proposition. Each registered entity may receive a set of individualized parameters for its participation in the

program that reflects the risk posed by the registered entity and the strength and maturity of its practices in a given area. For example, a registered entity may be eligible to self-log noncompliance with certain Reliability Standards and not others.

Registered entities may lose eligibility to self-log for various reasons. A Regional Entity may remove a registered entity's ability to self-log minimal risk noncompliance for all or a subset of Reliability Standards if the registered entity has demonstrated deficiencies in identifying, assessing, or correcting noncompliance. Misrepresentation or repeated, avoidable inaccuracies in the log may also result in the loss of the registered entity's self-logging ability.

Participation in the self-logging program is voluntary. Registered entities may contact their Regional Entities regarding participation, but are not required to participate.

2. Processing and Recording of Self-Logged Noncompliance

Registered entities permitted to self-log must maintain a record of instances of noncompliance with NERC Reliability Standards that posed a minimal risk to the reliability of the BPS. Appropriate self-logging replaces the individual Self-Reports and accompanying formal Mitigation Plans for each such instance of noncompliance.

On the log, the registered entity records a detailed description of the minimal risk issue that it has identified, the basis of its minimal risk assessment, and the actions it has taken or will take to correct the issue, specifically the mitigating activities it has undertaken to address the issue and prevent reoccurrence. Because only minimal risk issues are eligible for inclusion on the log, the registered entity's processes in place to determine risk are key to its eligibility for self-logging. The log is currently in the form of a spreadsheet similar to that used for FFT issues.

It is expected that, in the future, subject to successful system upgrades, registered entities will be able to maintain their log electronically on the Regional Entity portal.

The registered entity submits its log for review by the Regional Entity every three months.[51] The Regional Entity must review the log to confirm that the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately corrected or identified the steps it will take to correct (i.e. mitigate) the noncompliance. The Regional Entity may submit any concerns, questions, or proposed revisions to the registered entity for consideration. Once the log is finalized, the log is submitted to NERC, and the minimal risk individual issues are processed as compliance exceptions. If compliance exception treatment is not appropriate for any individual instance of noncompliance recorded in the log, the matter may be resolved through any of the remaining disposition tracks. At this time, noncompliance posing a moderate or greater risk to the reliability of the BPS is ineligible for self-logging.

In the event the registered entity identifies a noncompliance and determines that it poses more than a minimal risk, or the registered entity is not certain of the level of risk posed by the noncompliance, the registered entity is encouraged to submit a Self-Report to its Regional Entity.

[51] The Regional Entity may adjust this period to six months based on its experience with the registered entity in the self-logging program.

3. Experience Gained during Pilot Phase

Self-logging began, as a pilot program, in October 2013A few representative experiences are related below.

The New York Power Authority ("NYPA"), a state public power organization, participated in a pilot program and shared its experience during a public webinar.[52] NYPA explained how compliance exceptions and self-logging are implemented and why it will benefit registered entities. NPCC used information gathered from several sources including a 2012 voluntary Entity Impact Evaluation[53] of NYPA and the results of a voluntary 2013 ICE of NYPA to determine the scope of Reliability Standards subject to self-logging. As part of its internal controls structure, NYPA conducts internal investigations of potential compliance concerns, which involve: (i) identification of a concern, (ii) a fact-finding investigation (interviews and evidence collection), (iii) a review of applicable standard requirements and regulatory guidance, (iv) identification of mitigating factors, (v) determination of whether a possible violation occurred and its status (ended or continuing), (vi) an assessment of the potential and actual risks, (vii) analyzing whether it had any previous violations related to the issue, and (viii) mitigation activities in progress or completed. After conducting its internal investigation, NYPA notified NPCC of any noncompliance and its risk assessment. For possible violations identified by NYPA as minimal risk, NPCC conducted a review and, if NPCC affirmed the minimal risk, included it as a violation in the log.

[52] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

[53] "Entity Impact Evaluation" was a working name for the IRA.

NYPA maintained and submitted tracking spreadsheets to NPCC at least once every six months. NPCC determined if any of the issues needed further mitigation or enforcement action. The implementation required NYPA to internally assess actual and potential risk, process, track, and remediate issues, have a notification procedure for a possible minimal risk issue, and conduct monthly conference calls with NPCC. During monthly conference calls, NPCC and NYPA reviewed actions from the last meeting, tracked spreadsheets, reviewed and discussed each issue, discussed implementation matters, and reviewed the RAI Pilot Program status. Self-logging allowed NYPA to test and investigate its internal controls and address the steps needed to mitigate possible violations.

The American Transmission Company ("ATC"), a multi-state, transmission-only utility, also participated in the June 2014 webinar. ATC explained the scoping process for its audit and espoused the value of compliance exceptions. ATC also indicated that it views self-logging as essential to a truly risk-based approach to compliance oversight.

After participating in the self-logging pilot, ATC communicated that its compliance program will be further enhanced and structured towards an internal controls framework in the future. ATC predicted that by transitioning into the reliability assurance model, it will strengthen its processes and programs that support the COSO fundamental concepts, refine its internal controls, better define activities to monitor the execution of internal controls, bring more formality and structure to its corrective action process, and enhance its position as "audit ready."

One pilot involved a multiregional registered entity, American Electric Power ("AEP"), one of the largest electric utilities in the U.S. AEP participated in an enforcement pilot with RF, Texas RE, and SPP RE. Based on the results of RF's evaluation of AEP's internal controls,

along with other considerations such as AEP's compliance history, its history of self-assessment and self-reporting possible violations, and the quality of its internal controls, AEP logged minimal risk noncompliance (that would otherwise qualify for FFT treatment) of certain CIP standards.

The log, as well as AEP's procedures for maintaining the log and ensuring that noncompliance was discovered, recorded, and mitigated, was periodically checked by the three Regional Entities. After review and approval by the Regional Entities, the minimal risk issues were treated as compliance exceptions.

4. Visibility and Accountability

The ERO Enterprise will continue to have visibility and accountability over all instances of self-logged noncompliance. In practice, as explained in more detail below, in many instances the logged instances of noncompliance may be more comprehensive than self-reports, because of the presumption of compliance exception treatment. The ERO Enterprise will use the information collected through the self-logging program primarily for trending purposes. However, to the extent that items are not properly logged or there is an issue with the risk assessment or mitigation activities, the Regional Entity may, as discussed above, remove the item for processing through any other means and may modify the scope of the entity's ability to log (or exclude the entity from the logging program altogether).

NERC and Regional Entities also will periodically evaluate the registered entities' participation in the self-logging program. If NERC or the Regional Entity determines that a registered entity is no longer eligible to participate in the self-logging program, or if they should

adjust the parameters of its participation, NERC or the Regional Entity will provide notice to the registered entity and each other including an explanation of such determination.

5. Benefits of Self-logging

To date, the ERO Enterprise has identified several benefits of self-logging. First, because the minimal risk issues have the presumption of compliance exception treatment, experience has shown, as noted above, that logs often increase visibility into noncompliance detected and corrected at the registered entity. The experience with the program shows that the registered entity may be more likely to record additional information on its log than it would include in a self-report. There are a number of incentives associated with logging of noncompliance. For instance, logged items treated as compliance exceptions will not incur a financial penalty. Further, logged items treated as compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties.[54] Given these incentives, registered entities have shown a greater inclination to identify potential noncompliance, including at times when they may be uncertain about whether the identified issue is a noncompliance.

Second, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports. As mentioned previously, efficiency does not necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. Once there is an understanding of the registered entity's internal processes associated with identification, assessment, and correction of noncompliance, and there is an alignment as to the expectations of the Regional Entity regarding the type of information to

[54] As explained above, a compliance exception is part of a registered entity's compliance history only to the extent that it serves to inform the ERO Enterprise of potential risk.

be included in the log, including for the risk assessment, the entities participating in the program have reported efficiency gains.

The third benefit of self-logging is that the log is an ideal forum for trend spotting because all minimal risk issues related to a particular area and the mitigation associated with them are contained on the log. Experience has shown that the log review and discussion may trigger productive dialogue between the Regional Entity and the registered entity regarding expanding mitigating activities to prevent broader issues in the future.

Fourth, because the registered entity must do its own risk assessment in order to determine whether the noncompliance qualifies for self-logging, and because the rationale contained within the log must support the risk assessment, Regional Entities see more analysis of risk on the registered entity's part when it comes to noncompliance with Reliability Standards than is common in self-reports.

Finally, self-logging is a valuable tool to recognize management practices around Reliability Standards and good performance on the part of registered entity, and at the same time allow the Regional Entities to focus time and resources on issues that pose a greater risk to reliability of the BPS.

6. Oversight by NERC

The Regional Entities inform NERC of registered entities allowed to self-log minimal risk noncompliance. NERC exercises oversight over the program to ensure it is administered consistently and appropriately.

Regional Entities document the factors they analyzed when determining the eligibility of each registered entity to self-log. In accordance with the program document,[55] this documentation includes (i) evaluation of the registered entity's compliance history, (ii) consideration of the timing and quality of the registered entity's Self-Reports, (iii) assurance of the registered entity's ability to assess the risk of noncompliance accurately, (iv) examination of the registered entity's mitigation performance, (v) review of the registered entity's internal compliance program documents, including the date of the latest review, (vi) determination of the registered entity's risk, including the results of an Inherent Risk Assessment, if applicable, (vii) justification for the scope of Reliability Standards for which the registered entity is permitted to self-log, and (viii) a description of the Regional Entity's structure and process for reviewing requests to join the self-logging program, including the department(s) responsible for making eligibility decisions.

NERC will periodically review the Regional Entities' eligibility determinations. NERC may also request information on eligibility determinations outside of a regular periodic review based on questions about a registered entity's participation.

[55] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf.

VI. CONCLUSION

The ERO Enterprise has developed the concepts, processes, pilots, and programs detailed above to implement a more robust, risk-based program for compliance monitoring and enforcement of Reliability Standards that benefits reliability. These processes are consistent with existing Rules of Procedure and allow registered entities and the ERO Enterprise to focus on areas posing greater risk to the reliability of the BPS while maintaining appropriate visibility over lesser-risk issues. NERC has posted guides and program documents and provided training and outreach efforts related to the new and expanded processes and programs to allow for full implementation in 2015. This implementation will accompany additional training and outreach efforts directed at ERO Enterprise staff and industry stakeholders. NERC oversight of all these risk-based processes and programs will ensure NERC will identify and address additional guidance and training to adapt quickly to specific implementation challenges. In identifying such areas, NERC will consider the feedback from registered entities, Regional Entities, and other stakeholders.

NERC respectfully requests that the Commission accept this filing for informational purposes.

VII. NOTICES AND COMMUNICATION

Notices and communications with respect to this filing may be addressed to the following:[56]

NERC

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

Charles A. Berardesco
Senior Vice President and General Counsel
Sonia C. Mendonca
Associate General Counsel and Senior Director of Enforcement
Teresina A. Stasko*
Senior Counsel and Manager of Enforcement Actions
Leigh Anne Faugust*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
sonia.mendonca@nerc.net
teresina.stasko@nerc.net
leigh.faugust@nerc.net

[56] 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.

FRCC
Stacey Dochoda
President & Chief Executive Officer
Linda Campbell*
Vice President & Executive Director – Standards & Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 600
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5646 – facsimile
sdochoda@frcc.com
lcampbell@frcc.com

MRO
Daniel P. Skaar
President & Chief Executive Officer
Sara E. Patrick*
Vice President of Enforcement and Regulatory Affairs
Midwest Reliability Organization
380 St. Peter Street, Suite 800
St. Paul, MN 55102
(651) 855-1760
(651) 855-1712 – facsimile
dp.skaar@midwestreliability.org
se.patrick@midwestreliability.org

NPCC
Edward A. Schwerdt
President & Chief Executive Officer
Stanley E. Kopman
Assistant Vice President of Compliance
Walter Cintron*
Manager of Compliance Enforcement
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas-10th Fl.
New York, N.Y. 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
eschwerdt@npcc.org
skopman@npcc.org
wcintron@npcc.org

RF
Timothy R. Gallagher
President & Chief Executive Officer
Robert K. Wargo
Vice President, Reliability Assurance & Monitoring
L. Jason Blake
General Counsel
Megan E. Gambrel*
Senior Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(330) 456-2488
tim.gallagher@rfirst.org
bob.wargo@rfirst.org
jason.blake@rfirst.org
megan.gambrel@rfirst.org

SERC
R. Scott Henry
President and Chief Executive Officer
Andrea B. Koch
Director of Compliance and Analytics
James M. McGrane*
Managing Counsel – Enforcement
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 357-7372
(704) 357-7914 – facsimile
shenry@serc1.org
akoch@serc1.org
jmcgrane@serc1.org

SPP RE
Ron Ciesiel*
General Manager
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223-4936
(501) 614-3265
(501) 482-2025 – facsimile
rciesiel.re@spp.org

Texas RE
Jim Albright
Vice President & Chief Program Officer
Curtis Crews, PE
Director, Compliance Assessments
Derrick Davis*
Director, Enforcement, Reliability Standards & Registration
Texas Reliability Entity, Inc.
805 Las Cimas Parkway, Suite 200
Austin, TX 78746
(512) 583-4915
jim.albright@texasre.org
curtis.crews@texasre.org
derrick.davis@texasre.org

WECC
Chris J. Luras
Director of Compliance Risk Analysis & Enforcement
Ruben H. Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103-1114
(801) 582-0353(801) 883-6894 – facsimile
cluras@wecc.biz
rarredondo@wecc.biz

Respectfully submitted

/s/ Teresina A. Stasko

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

Charles A. Berardesco
Senior Vice President and General Counsel
Sonia C. Mendonca
Associate General Counsel and Senior Director of Enforcement
Teresina A. Stasko*
Senior Counsel and Manager of Enforcement Actions
Leigh Anne Faugust*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
sonia.mendonca@nerc.net
teresina.stasko@nerc.net
leigh.faugust@nerc.net

Counsel for North American Electric Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 1, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Informational Filing Regarding Commissioner Philip D. Moeller's Inquiry into the Trading of Natural Gas, and the Proposal to Establish an Electronic Information and Trading Platform, FERC Docket No. AD14-19-000

Dear Ms. Bose:

On September 18, 2014, Commissioner Philip D. Moeller convened a meeting to discuss ideas to facilitate and improve the way in which natural gas is traded, and explore the concept of establishing a centralized information and trading platform for natural gas. As announced at the meeting, the above-captioned docket was created to allow interested parties to file written comments on any issue that was discussed at the meeting.[1]

The North American Electric Reliability Corporation ("NERC") has developed the attached report which is an analysis of the weather condition that occurred in early January of 2014 known as a polar vortex, where frigid arctic condition dipped down to much lower latitudes than normal, resulting in extreme cold weather. As expected, key factors during the event included fuel deliverability issues, natural gas pipeline outages, gas service interruptions, frozen electricity and gas equipment and other extreme cold weather operating challenges. The attached report analyzes the system impacts from the polar vortex and notes that the Bulk-Power System demonstrated resiliency, despite these challenging conditions.

As noted during the meeting convened by Commissioner Moeller, severe weather is a challenge to be addressed in exploring the concept of establishing a centralized information and trading platform for natural gas. For this reason, NERC is submitting the attached report for informational purposes.

Respectfully submitted,

/s/ Stacey Tyrewala
Stacey Tyrewala

Attorney for the North American Electric Reliability Corporation

[1] While the post-meeting notice requests that comments be limited to no more than five pages, NERC is not providing written comments on the conference, it is providing a report strictly for informational purposes.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Polar Vortex Review

September 2014

RELIABILITY | ACCOUNTABILITY






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

Table of Contents

Preface ii

Executive Summary iii

Introduction v

Review of Polar Vortex Weather v

Chapter 1 – Method of Analysis 1

GADS Data Review and Validation 1

Chapter 2 – Effects 2

System Operations 2

Florida Reliability Coordinating Council 6

Midwest Reliability Organization 7

Northeast Power Coordinating Council 8

ReliabilityFirst 9

SERC Reliability Corporation 10

Southwest Power Pool Regional Entity 11

Texas Reliability Entity 12

Generator Issues by Fuel Type 13

Chapter 3 – Discussion 17

Chapter 4 – Conclusion 19

Observations and Recommendations 19

Appendix A 21

Overview of GADS 21

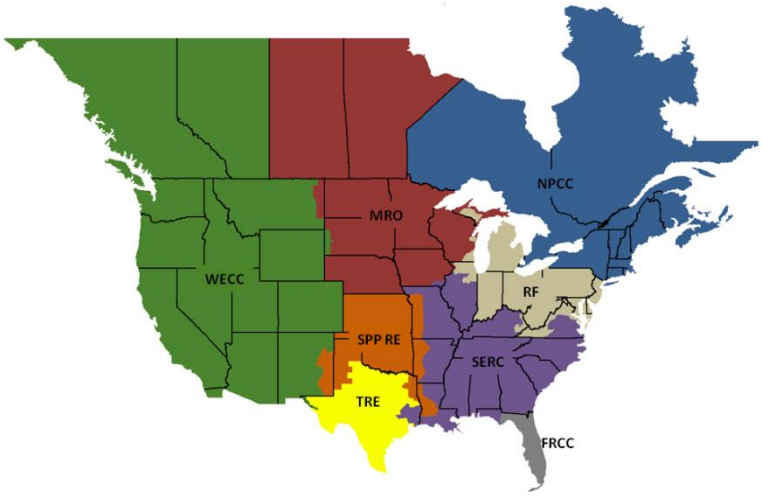
Appendix B 36

Historical GADS Analysis 37

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

This report describes what happened during the polar vortex and why some of the conditions occurred, and it presents lessons learned and recommendations for future actions. In early January of 2014, the Midwest, South Central, and East Coast regions of North America experienced a weather condition known as a polar vortex, where extreme cold weather conditions occurred in lower latitudes than normal, resulting in temperatures 20 to 30° F below average. Some areas faced days that were 35° F or more below their average temperatures. These temperatures resulted in record high electrical demand for these areas on January 6 and again on January 7, 2014.

During the polar vortex, the cold weather also increased demand for natural gas, which resulted in a significant amount of gas-fired generation being unavailable due to curtailments of gas. Balancing Authorities (BAs) and Load-Serving Entities in both the Electric Reliability Council of Texas (ERCOT) and the Eastern Interconnection were mostly able to maintain their operating reserve margins and serve firm load. By properly and appropriately communicating through the NERC Energy Emergency Alert (EEA) process using interruptible load, demand-side management[1] tools, and voltage reduction, only one BA was required to shed firm load. The amount shed was less than 300 MW, representing less than 0.1 percent of the total load for the Eastern and ERCOT Interconnections. Many outages, including a number of those in the southeastern United States, were the result of temperatures that fell below a plant's design basis.

Generation facilities have made improvements in their winter preparation activities since February 2011; however, every extreme event provides insight for future improvements. Generation facilities across all Regions have indicated that they have reviewed or implemented recommendations from the *February 2011 Southwest Cold Weather Event Lessons Learned*, as well as the *Generating Unit Winter Weather Readiness* reliability guideline.

System Operators had many challenging decisions to make as a result of lost capacity from both weather conditions exceeding the design basis of generating units, and from the lack of availability of natural gas. They successfully maintained reliability through extensive training and preparation. For example, during the polar vortex, several System Operators used load reduction techniques such as voltage reduction or interruptible loads. They also made effective use of emergency procedures to manage loads and generation.

While the NERC Event Analysis process has clearly defined categories for electric disturbances in small defined geographic areas, based on the combined unintended loss of generation during the three-day period (January 6–8), this event reached the equivalent of an ERO Event Analysis Process level of Category 5 (unintended loss of more than 10,000 MW of generation). WECC and the majority of the Canadian entities are not included in this analysis as the report is based on the geographic areas that observed effects of this extreme event.

The report also contains more than a dozen observations and recommendations to improve performance ahead of and during cold weather events. The recommendations include:

- Review natural gas supply and transportation issues and work with gas suppliers, markets, and regulators to develop appropriate actions.
- Review and update power plant weatherization programs, including procedures and staff training.
- Continue or consider implementing a program for winter preparation site reviews at generation facilities.
- Review internal processes to ensure they account for the ability to secure necessary waivers of environmental and/or fuel restrictions.

[1] The term for all activities or programs undertaken by Load-Serving Entity or its customers to influence the amount or timing of electricity they use.

- Continue to improve operational awareness of the fuel status and pipeline system conditions for all generators.
- Include in winter assessments reasonable losses of gas-fired generation and considerations of oil burn rates relative to oil replenishment rates to determine fuel needs for continuous operation.
- Ensure that on-site fuel and fuel ordered for winter is adequately protected from the effects of cold weather.
- Consider (where appropriate) the temperature design basis for generation plants to determine if improvements are needed for the plants to withstand lower winter temperatures without compromising their ability to withstand summer temperatures.
- Review the basis for reporting forced and planned outages to ensure appropriate data for unit outages and de-ratings.

Introduction

Review of Polar Vortex Weather

The effects of the polar vortex in the United States were initially felt in the far northwestern portion of the MRO footprint, but these low temperatures quickly spread to nearly all portions of the Eastern and Texas Interconnections. In many areas in the United States, temperatures were far colder than those normally experienced in winter, resulting in record winter peak electric demands associated with increased electric heating requirements.

The average daily temperature for the United States on January 6 was calculated to be 17.9° F (-7.8° C). The last time the average for the country was below 18° F was January 13, 1997. This 17-year period without the national average for the United States dropping below 18° F is the longest gap on record and, since then, a significant portion of the generating fleet is now fueled by natural gas.[2] On January 7, at least 49 record low temperatures were set across North America.

As shown in Table 1 and Figures 1 and 2, the polar vortex started in the northern Great Plains and moved south and east. The selected cities are representative of the Regional Entities affected by the extreme cold and are also large load centers.

Table 1: Average vs. Observed High Temperatures (Fahrenheit)

	Minneapolis, MN	Chicago, IL	St. Louis, MO	Dallas, TX	Columbus, OH	Indianapolis, IN	Columbia, SC	Washington DC	New York, Ny
Avg. High/Low[3]	24/8	32/19	40/23	56/37	36/23	35/21	55/35	43/29	38/27
Observed 5-Jan-14	-2/-20	31/-1	33/1	60/22	55/27	35/5	50/37	42/31	40/27
Observed 6-Jan-14	-12/-23	-1/-15	2/-7	33/14	33/-7	5/-15	60/21	49/11	55/19
Observed 7-Jan-14	5/-15	5/-11	22/-14	47/22	11/-7	8/-14	30/15	21/6	19/4
Observed 8-Jan-14	4/-11	15/-2	32/15	49/38	26/10	25/6	46/18	31/13	22/9

[2] Borenstein, Seth, January 10, 2014. "Weather wimps?" Salisbury Post. Associated Press. p. 1A.

[3] These high and low temperatures were gathered from www.accuweather.com and represent the both the average and actual high and low temperatures experienced during this timeframe

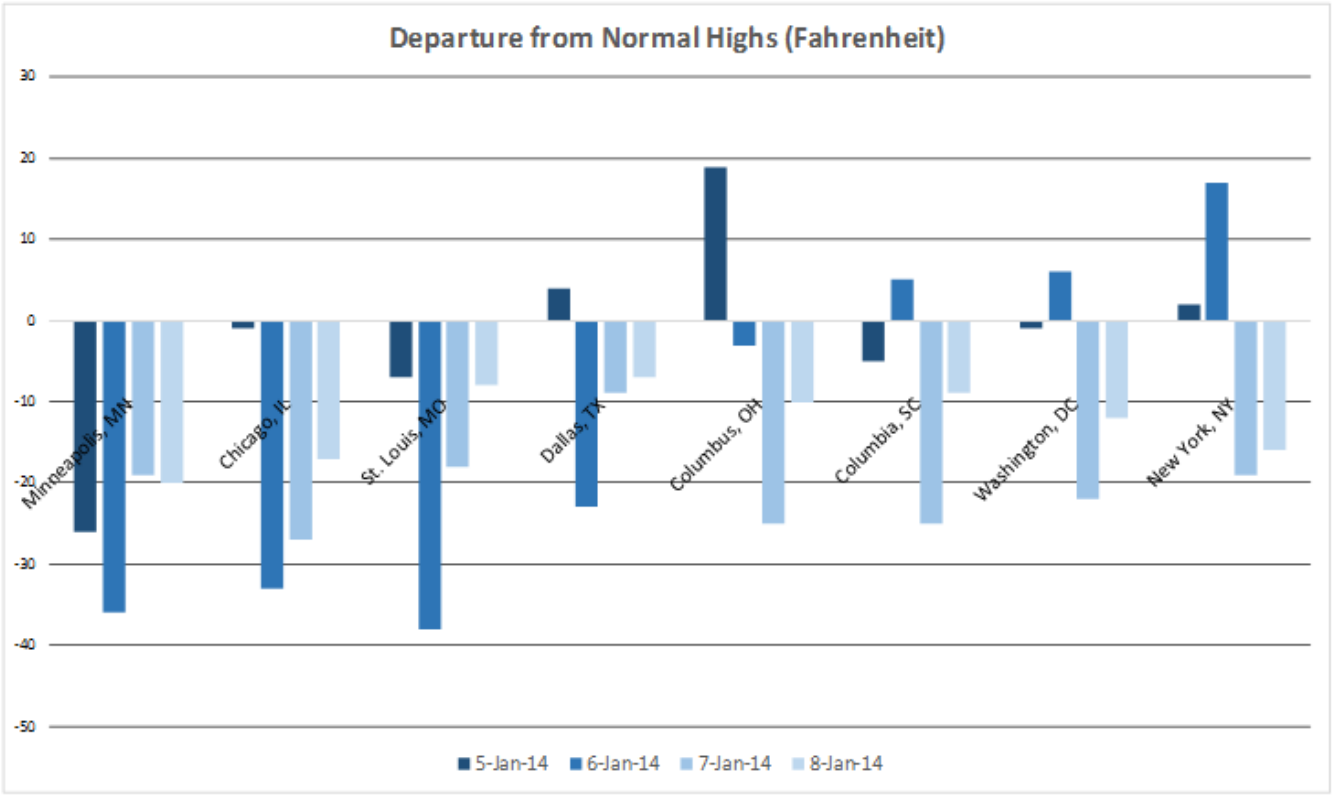


Figure 1: Departure from Normal High Temperatures

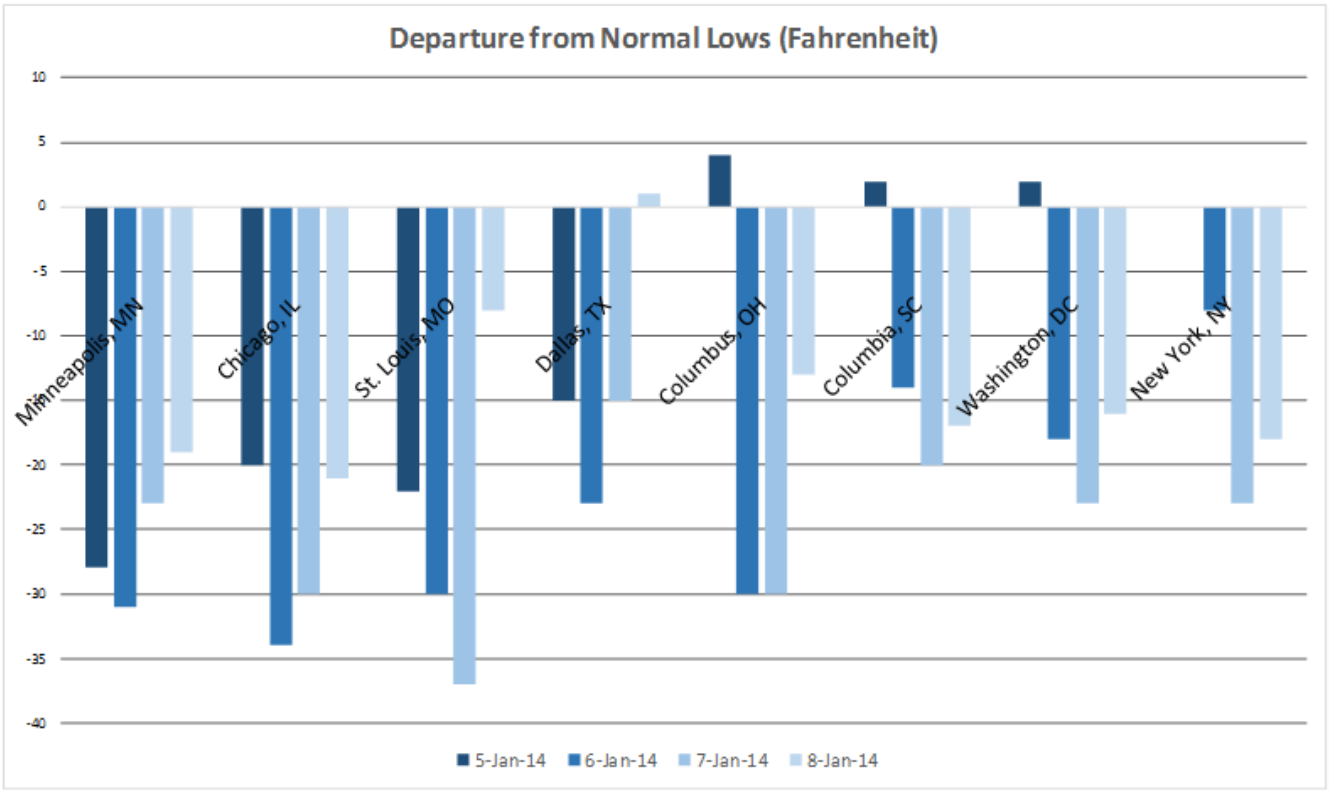


Figure 2: Departure from Normal Low Temperatures

The most significant impacts to the BPS in the MRO Region began on January 5, 2014, and persisted through January 7, 2014. The extremely cold temperature was the primary impacting factor, but heavy precipitation also affected large portions of the Region. Temperatures in many areas were the lowest experienced in 20 years. Minneapolis, where the average high for early January is 23° F, experienced 62 consecutive hours below 0° F from January 5 to January 7.

As the polar vortex extended south and east, it also began to impact the SPP, TRE, RF, SERC, and NPCC Regional Entities. As a result, the majority of the Eastern and ERCOT Interconnections experienced similar variances from normal. For example, St. Louis experienced temperatures up to 38° F below normal, and Chicago up to 34° F below normal; other parts of the country experienced temperatures between 23 and 30° F below normal. In Indianapolis, where they normally experience average highs of 35° F during this period, temperatures remained below 0° F for 33 consecutive hours.

Temperatures in the Canadian regions of MRO were even colder and started earlier. Saskatchewan, for instance, started to experience the polar vortex beginning the evening of January 3, with the greatest impact on the nights of January 5 and 6. Additionally, the city of Regina, Saskatchewan fell to below 0° F temperatures the night of Friday, January 3, and did not climb above 0° F until January 8. Winnipeg, Manitoba experienced a similar plunge in temperature with the mercury falling to -31° F on the night of Saturday, January 4, 2014. The night of January 5, 2014, they experienced a low of -36° F. The temperature in Winnipeg did not climb back above 0° F until Thursday, January 9, 2014.

As shown in Figure 3 and Table 2, these lower temperatures had a drastic impact on load, with many of the Reliability Coordinators (RCs) (e.g., Midcontinent Independent System Operator (MISO), PJM Interconnection (PJM), the Tennessee Valley Authority (TVA), the VACAR South RC (VACS RC), and Southeastern-RC) reporting record or near-record winter peak demands. PJM exceeded its historic winter peak on both January 7 and January 8, 2014, and MISO reported that they exceeded their historic winter peak for three straight days (January 6–8, 2014).

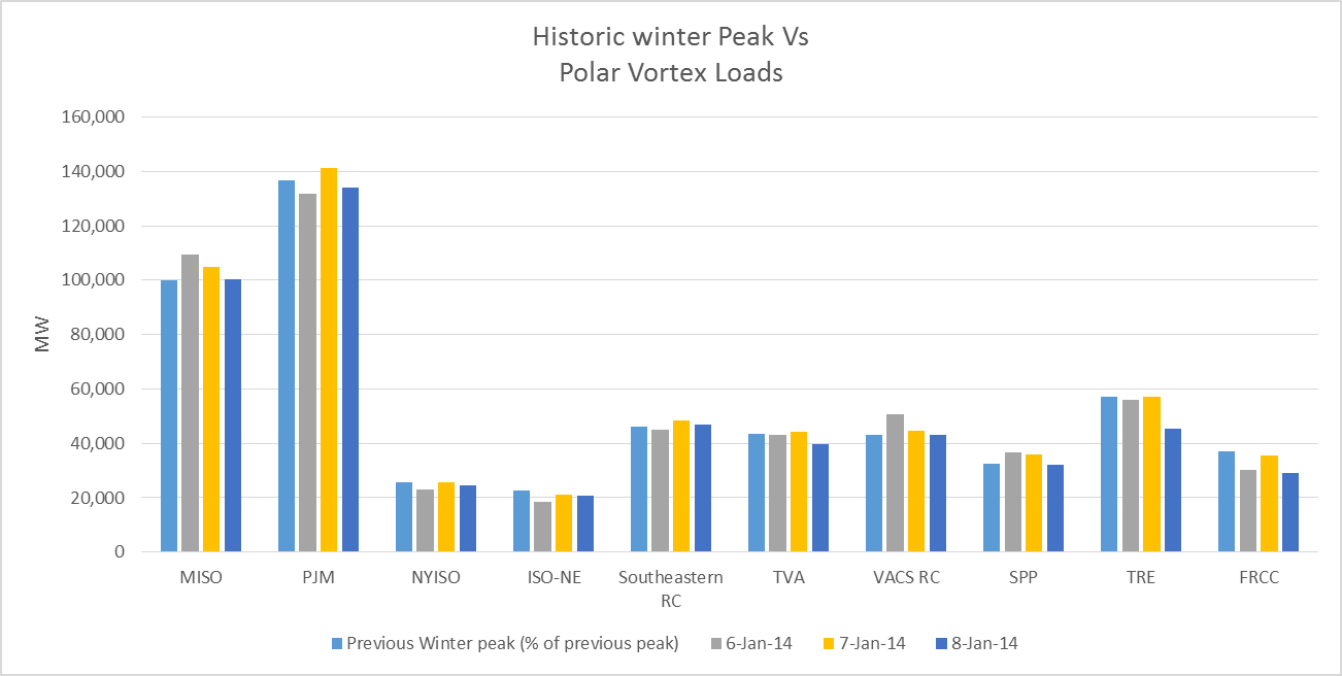


Figure 3: Historic All-Time Winter Peaks vs. Polar Vortex Loads

As seen in Table 2 and Figure 3, each of the RC areas were experiencing either new peak winter electric loads or loads that were close to the previous all-time winter peak, with eight of 10 areas setting new all-time peaks either on January 6 or 7, 2014. VACS RC experienced a new winter electric load peak that was almost 18 percent greater than the previous all-time winter peak.

Table 2: Historic Winter Peak Loads vs. Polar Vortex Loads by Percentage[4]

	MISO	PJM	NYISO	ISO-NE	South-eastern RC	TVA	VACS RC	SPP	ERCOT	FRCC
Previous Winter peak (% of previous peak)	99,855	136,675	25,541	22,818	46,259	43,384	42,983	32,635	57,265	36,926
6-Jan-14	109,307 (109.5%)	131,142 (95.5%)	23,197 (90.8%)	18,500 (81.1%)	44,871 (97.0%)	43,277 (99.8%)	50,659 (117.9%)	36,602 (112.2%)	56,031 (97.8%)	30,231 (81.9%)
7-Jan-14	104,746 (104.9%)	140,510 (103.5%)	25,738 (100.8%)	21,300 (93.3%)	48,279 (104.4%)	44,285 (102.1%)	44,654 (103.9%)	36,079 (110.6%)	57,277 (100.0%)	35,638 (96.5%)
8-Jan-14	100,154 (100.3%)	133,288 (98.1%)	24,551 (96.1%)	20,800 (91.2%)	47,005 (101.6%)	39,820 (91.8%)	43,203 (100.5%)	31,944 (97.9%)	45,281 (79.1%)	29,251 (79.2%)

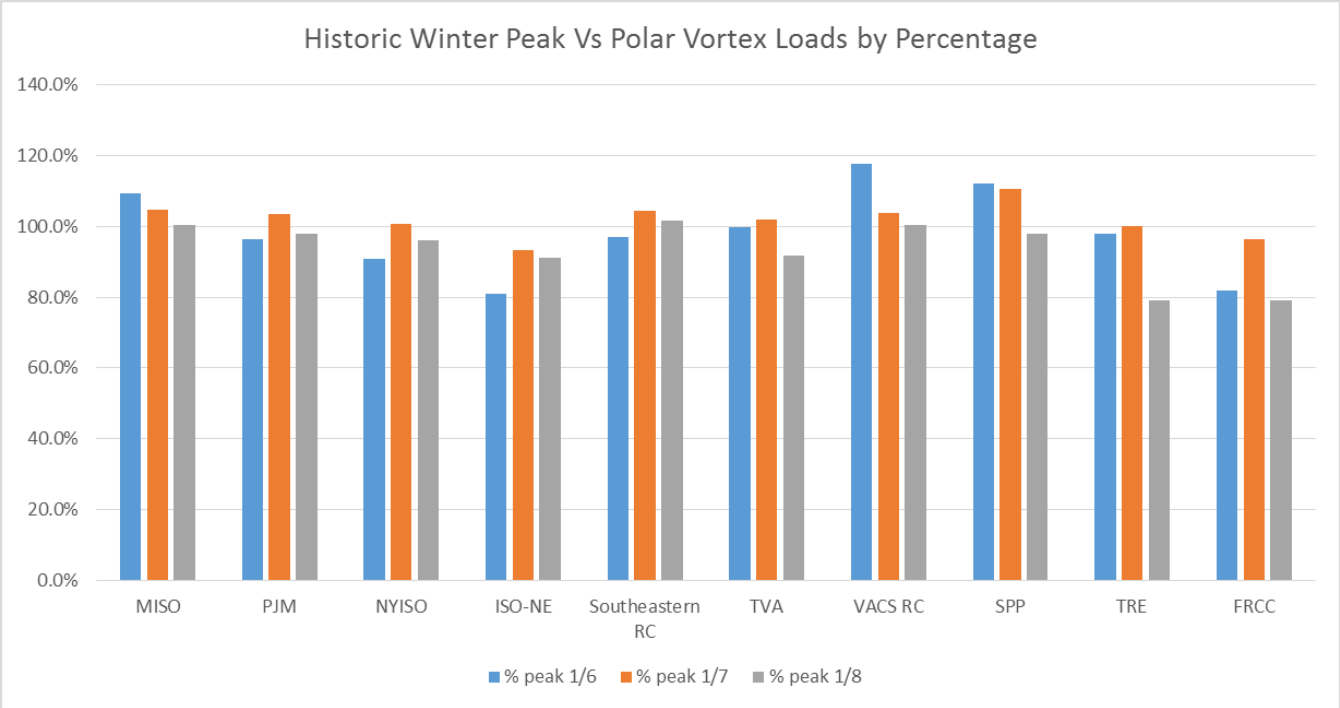


Figure 4: Historic All-Time Winter Peaks vs. Polar Vortex Loads by Percentage

With the significant temperature deviations and the accompanying increases in electric demand over such a wide area, it was challenging for BAs to supply sufficient generation to their areas, therefore making it challenging to

[4] Highlighted blue squares represent new all-time winter peak loads.

supply assistance to neighboring BAs. The peak loads experienced January 6–7 exceeded the combined noncoincident peaks achieved previously. On January 7, the combined load for the impacted BAs was 559,000 MW, or just under 3 percent higher than the nonsimultaneous historical peak.

Chapter 1 – Method of Analysis

GADS Data Review and Validation

NERC introduced the Generating Availability Data System (GADS) in 1982. GADS data is used to calculate important performance statistics and supports bulk power trend analysis by providing information on forced outages, maintenance outages, planned outages, and derates. The NERC Board of Trustees (Board) approved mandatory reporting of data to GADS for conventional generating units on August 4, 2011. Renewable generation (wind and solar) are not part of the mandatory data submittal requirements. The MW size of the conventional units was phased in, with units having a nameplate rating of 50 MW and larger starting January 1, 2012, and those with a nameplate rating of 20 MW and larger starting January 1, 2013. GADS data is collected from all Generator Owners on the NERC Compliance Registry under NERC's Rules of Procedures Section 1600, Request for Data or Information. Generating units less than 20 MW are encouraged to report unit information on a voluntary basis.

NERC collects the equipment information by class of outage and calculates statistics such as Equivalent Forced Outage Rate (EFOR) using IEEE Standard 762 definitions, thereby ensuring a high level of confidence that the statistics are calculated in a uniform process using an industry-approved method. Analysis of GADS data provides trend information on forced, maintenance, and planned outages and derations.

Further, NERC collects information on the fuels burned and fuel-switching activities (coal to gas, oil to gas, and bio-fuels to other fuels). Since GADS was a voluntary database prior to 2012, analysis of data prior to 2012 provides partial information. Additionally, since units less than 50 MW but greater than 20 MW were not reported to NERC until 2013, analysis of 2012 data may be biased toward larger units. With these factors in mind, NERC examined GADS data to determine an expected EFOR for the polar vortex time period. The complete summary of the data analysis is provided in Appendix A.

NERC used the GADS information to analyze generator availability during the polar vortex. A list of generation outages due to planned and forced outages could be obtained, as well as analysis of forced outage cause codes. This data was used to determine the amount of generation that was forced out specifically due to the polar vortex, as opposed to generation that was forced out due to other operational parameters.

GADS also collects additional generation information on a voluntary basis. Examples of this information include reasons for derates, verbal descriptions of outages, and explanatory cause codes. This information is extremely useful in analyzing individual events, but provides limited value when calculating trends of performance characteristics.

Since GADS is used to examine trending information on a high level, the system had never been used to analyze performance information for generating units on as granular a scale as that required for the polar vortex. This presented a few challenges in data validation.

The NERC Performance Analysis staff began by obtaining a list of all generation that had reported outages in GADS. The NERC Event Analysis staff then compared the forced outages and derations list with analysis that was performed by various NERC Regional Entities and registered entities. Discrepancies were sent to the respective Regional Entities for validation and correction. After a period of examination of generator outage data by Regional Entities, 95 percent of generation outage data during the polar vortex was validated.

Chapter 2 – Effects

System Operations

System Operators had many challenging decisions to make as a result of lost capacity from both weather conditions exceeding the design basis of generating units, and from lost fuel due to the lack of natural gas transportation. They successfully maintained reliability through previous extensive training, preparation, and use of tools.

One of the largest issues impacting gas-fired generation was the curtailment or interruption of fuel supply. Unlike other fuel sources, natural gas is not typically stored on-site. Generators rely on real-time delivery of natural gas from their suppliers. When units are not confident that they will be dispatched, the fuel is often obtained on the spot-market on a non-firm, interruptible basis. Therefore, if firm contracts are honored before interruptible contracts, if the firm customers require more gas, and the capacity of the gas transportation is based on firm contracts, less capacity is available for interruptible supply. This can result in generating units becoming unavailable as there is no pipeline capacity to supply interruptible gas.

Extreme cold weather also had a major impact on generator equipment. Of the approximately 19,500 MW of capacity lost due to cold weather conditions, over 17,700 MW was due to frozen equipment. Many outages, including a number of those in the southeastern United States, were the result of temperatures that fell below the plant's design basis for cold weather. At the height of generation outages (January 7 at 0800) the southeastern United States accounted for approximately 9,800 MW of the outages attributed to cold weather.

With the extended duration weather pattern affecting most of the Eastern Interconnection, several of the RCs used load reduction procedures such as voltage reduction, interruptible loads, and demand-side management. In only two instances were these procedures used to maintain generating reserves: PJM used voltage reduction to maintain reserves, and South Carolina Electric and Gas (SCE&G) shed less than 300 MW of firm load, while also using voltage reduction to maintain reliable operation of the BPS. While the shedding of firm load is typically used as a last resort, it is critical that a minimum level of generating reserves be maintained to ensure that the reliability of the BPS is not jeopardized for the loss of the next contingency, and that it is restored within the appropriate time frames after a contingency occurs.

Many areas made effective use of emergency procedures to manage loads and generation. They provided notification to industry through tools such as the Reliability Coordinator Information System (RCIS) and conference calls. For example, MISO issued a Cold Weather Alert for portions of its footprint on January 2 that was effective January 5. On January 3, MISO also declared a Conservative Operations period for January 5. Although MISO did not direct any emergency demand reductions, some of their members used voluntary load reduction procedures at various times during this period.

RCs used voltage reduction and public appeals during the event and provided emergency energy, when available, to other BAs in need. For example, New York ISO (NYISO) appealed to their customers to conserve energy, and at the request of PJM, NYISO also used demand-side management resources to create additional capacity to provide assistance to prevent the shedding of firm load in the neighboring PJM area. Also, ISO-New England (ISO-NE) provided assistance to PJM by dispatching additional units. In addition, ISO-NE issued their Master/Local Control Center Procedure No. 2, "Abnormal Conditions Alert," to ensure that no scheduled work was performed on active equipment. Neither TVA, Southeastern RC, nor SPP RCs made use of emergency procedures such as voltage reductions or load shedding.

In Texas, ERCOT declared an Energy Emergency Alert[5] (EEA) Level 1 and then an EEA Level 2, primarily due to the loss of a number of generating units during the morning load ramp. They were able to recover within two hours and 11 minutes by deploying Non-Spin Reserve Service (NSRS), Responsive Reserve Service from generators, load resources, and Emergency Response Service (ERS).[6]

Two RCs that also experienced challenges were the VACS RC and PJM. In VACS RC, two BAs experienced difficulties when faced with the cold weather. The SCE&G BA experienced record electric demand the evening of January 6, 2014, and the morning of January 7, 2014. During that time, SCE&G lost more than 850 MW of generation from multiple sources. SCE&G addressed this loss of generation by following internal company procedures, which called for implementation of local and reserve-sharing group reserves, obtaining Emergency Assistance from neighbors and neighboring RCs, use of customer standby generators and curtailment of retail interruptible contract customers, appeals for conservation, distribution-level voltage reduction, and controlled firm load shed when reserves were not available for a period. All actions taken by SCE&G were intentional and in accordance with regulatory requirements.

Additionally, on January 7, the Duke Energy Progress (DEP) Carolina Power and Light East (CPLE) and Carolina Power and Light West (CPLW) BAs experienced all-time peak demand during the hour ending 8:00 a.m. Demand-side management resources, including an initial 2.9 percent system-wide voltage reduction, a large industrial load curtailment rider, general public appeal for conservation, and a water heater and strip heat control program, were deployed in the DEP TOP/BA footprint. As part of its General Load Reduction Plan, and while in a NERC Energy Emergency Alert Level 2, CPLE and CPLW BAs subsequently activated a 5 percent system-wide voltage reduction on the distribution system for their footprints at 7:54 a.m. Through the use of generation and demand-side management resources, the CPLE and CPLW BAs were able to serve an all-time peak demand without shedding firm load.

The second RC that experienced challenges was PJM. On January 3, they issued a Cold Weather Alert at approximately 11:00 a.m. for January 6–7. In addition, they successfully used emergency procedures and the EEA process to maintain their required level of reserves. Some of the actions taken included scheduling shared reserves from NYISO and ISO-NE, issuing EERs, using demand response, and initiating a 5 percent voltage reduction across a portion of their operating area.

Figure 5 illustrates the challenges experienced by System Operators with regard to generation capacity unavailability during the study period. The graph shows the cumulative amount of MW unavailable due to forced outages in the following five general categories:

- Unrelated – Outages not related to cold weather or the extremes presented by the polar vortex
- Unknown – Outages still under review to determine cause
- Miscellaneous – Outage types potentially related to extreme cold weather (e.g., opacity issues)
- Cold – Outages directly attributable to cold weather, including on-site fuel issues such as frozen coal piles, frozen equipment and/or sensors under the control of the generating plant, and gelled fuel
- Fuel – Outages that are directly related to the inability of the plant to receive fuel from their provider

[5] An Energy Emergency is a condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements.

[6] An emergency service consistent with P.U.C. SUBST. R. 25.507, Electric Reliability Council of Texas (ERCOT) Emergency Response Service (ERS), used during an Energy Emergency Alert (EEA) Level 2 to assist in maintaining or restoring ERCOT system frequency. ERS is not an Ancillary Service.

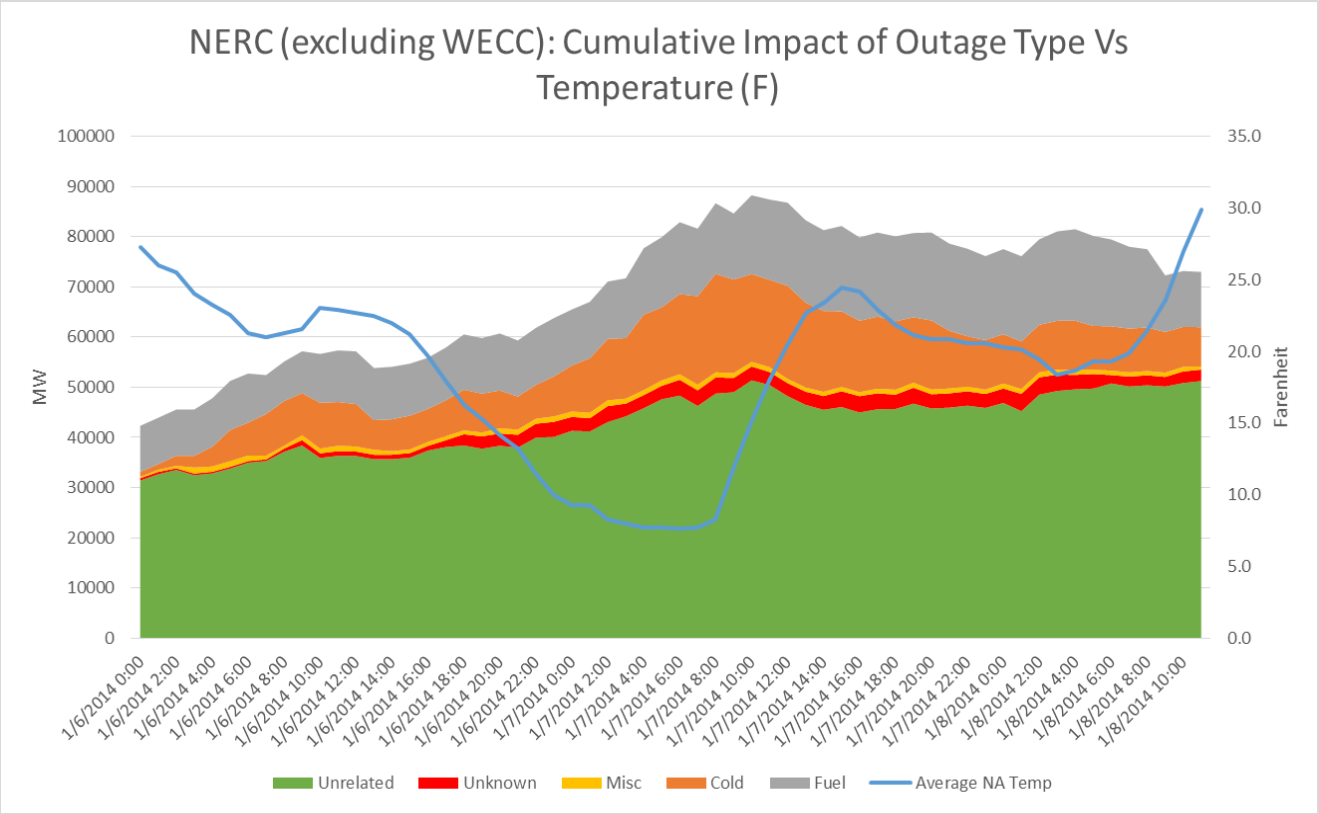


Figure 5: Total Outages in the Eastern Interconnection and ERCOT by Outage Type vs. Temperature

The North American temperature displayed in Figure 5 represents an average of seven selected cities in the approximate geographic centers of the seven studied Regions. The selected cities for each NERC Region are identified in the legends of Figures 6–12. It is important to note that Figures 5–12 are not normalized in any manner; thus, the additive number of the forced-out rate is understandably higher based on the greater number of generators being dispatched. Additionally, figures do not maintain the same scale for total forced-out MW values so that the relationships can be clearly seen between temperature and the outages.

Units were called on to start or increase output as the cold air mass swept down into the United States. The extreme weather challenged the units' preparedness and abilities to withstand ambient conditions, resulting in either forced outages or deratings. Once the cold air was established and units were running, the outages unrelated to cold weather maintained a fairly consistent rate throughout the remainder of the polar vortex time frame even though the number of generators and their individual run times were significantly increased.

All areas of the Eastern and Texas Interconnections were impacted by the polar vortex. These impacts were partially the result of the severe and extended cold spell, but there was also a significant reduction of generating capacity due to curtailments and interruptions of natural gas delivery. The cold weather and issues from fuel combined for over 35,000 MW of outages during the height of the polar vortex weather conditions.

One of the largest issues impacting gas-fired generation was the curtailment or interruption of fuel supply. Unlike other fuel sources, natural gas is not typically stored on site. As a result, generators rely on real-time delivery of natural gas from their suppliers. Often, as units are not confident that they will be dispatched, the fuel is obtained on the spot market as an interruptible fuel supply.

Extreme cold weather also had a major impact on generator equipment. Of the approximately 19,500 MW of capacity lost due to cold weather conditions, over 17,700 MW was due to frozen equipment. Many outages, including a number of those in the southeastern United States, were the result of temperatures that fell below the plant's design basis for cold weather. At the height of generation outages (January 7 at 0800) the southeastern United States accounted for approximately 9,800 MW of the outages attributed to cold weather.

In the following sections, each Region's forced outages have been plotted by type as a stacking chart, with temperature overlaid. A large city close to the center of the Region was selected to represent the temperature for the Region over the 60-hour period. For example, Orlando was chosen for the FRCC Region, and Pittsburgh, PA was chosen for the RF Region. However, cities near large moderating bodies of water, such as New York, Cleveland, and Chicago, were avoided. While these are large cities with significant electric loads, those temperatures may not reflect the temperatures experienced by the RE as a whole.

Florida Reliability Coordinating Council

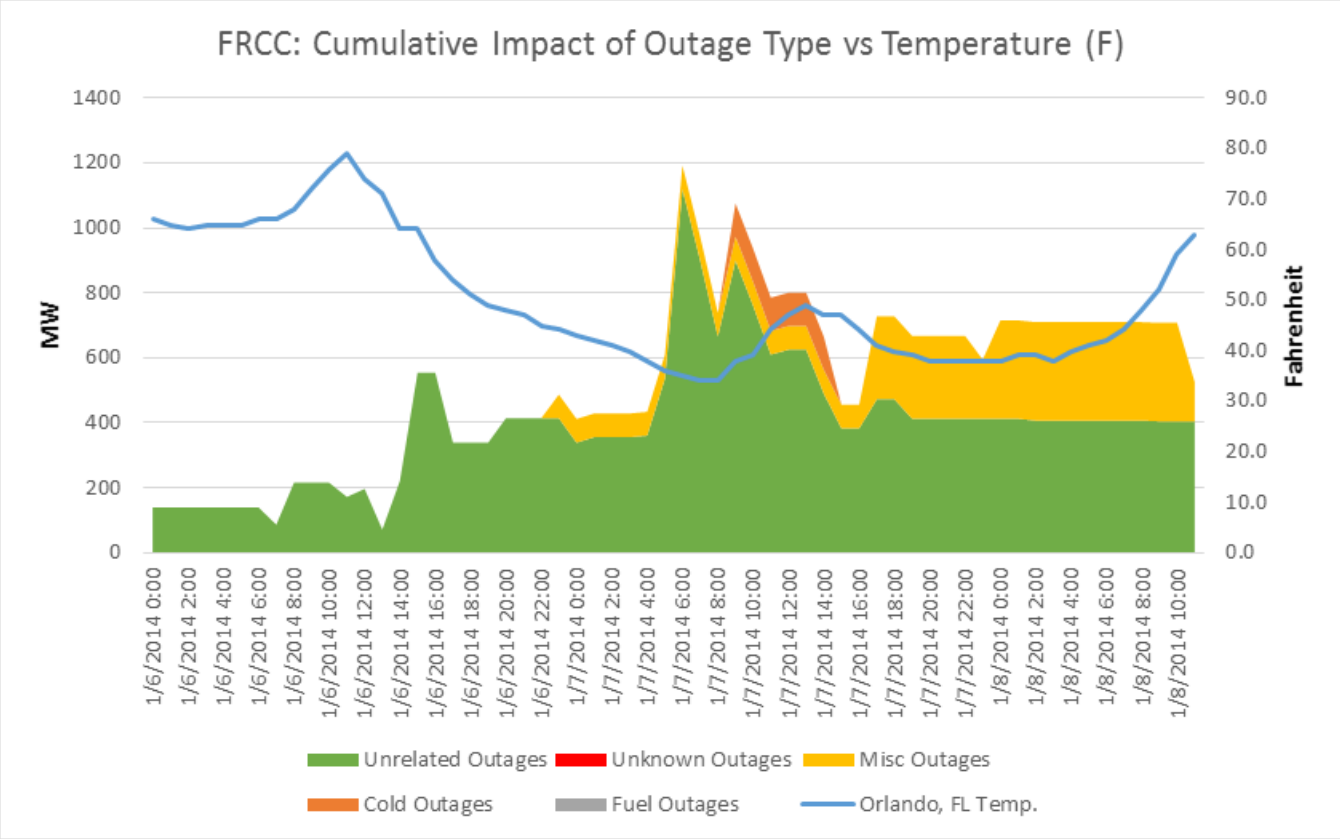


Figure 6: FRCC Cumulative Impact of Outage Type vs. Temperature (F)

While the majority of the outages in FRCC were unrelated to the polar vortex, there was a six-hour period with 102 MW of cold-related outages. Additionally, several units (303 MW) ran into emissions-related outages and derations. Otherwise, the FRCC Region did not experience significant impacts to their system during the polar vortex. Though FRCC is typically an importing Region, it was able to export 1,500 MW to aid the SERC Region during the polar vortex.

Midwest Reliability Organization

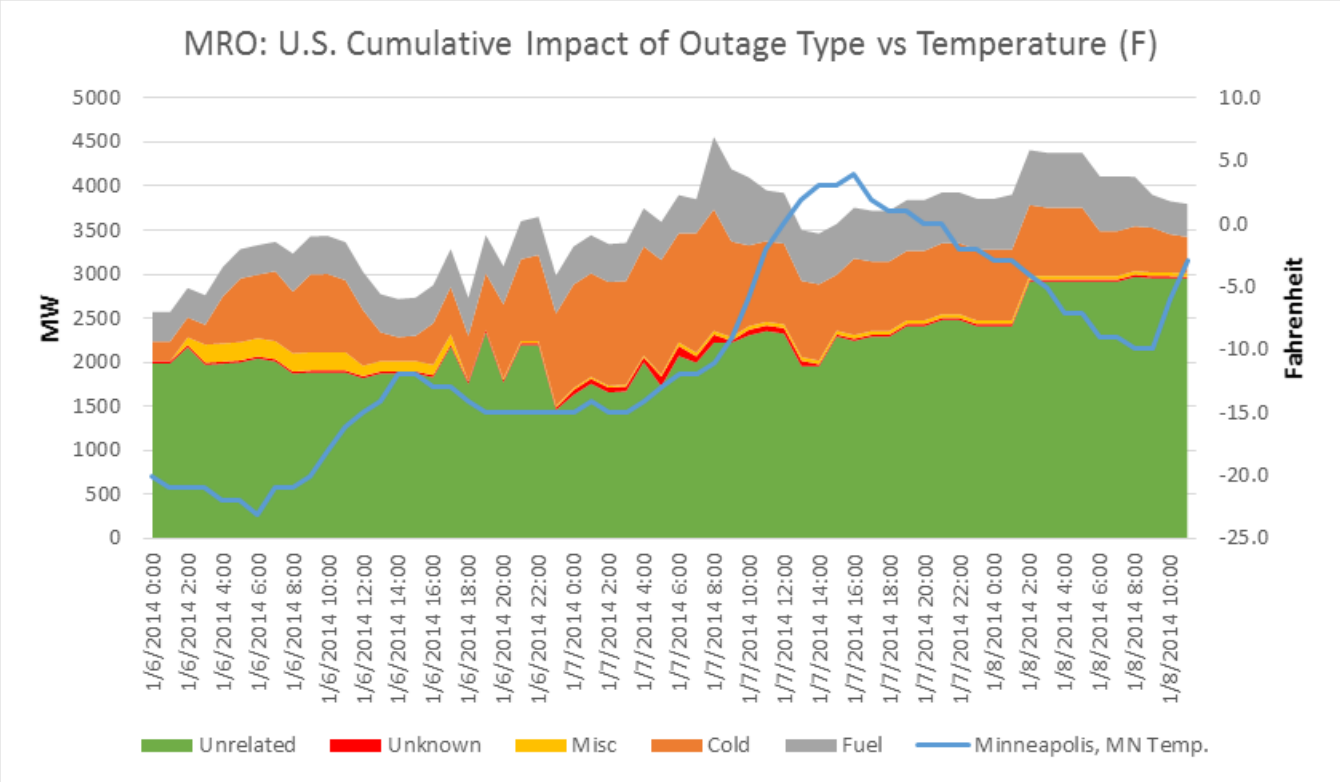


Figure 7: MRO (US): Cumulative Impact of Outage Type vs. Temperature (F)

As shown in Figure 7, unrelated outages were the majority of the generator outages in the MRO Region. The prolonged sub-zero weather eventually resulted in 1,379 MW of cold-weather-related impacts. MRO also experienced as much as 820 MW of generation loss due to fuel issues, with nearly 620 MW due to curtailments and interruptions of natural gas delivery to the plant. As shown in Figure 7, only seven of the 60 hours of interest were above 0° F in Minneapolis, MN.

MRO Generator Owners were prepared for the extreme cold because the design basis for generators in MRO accounts for operation in temperatures well below freezing (7° F is the historical average low in January). Additionally, Generator Owners recognize the reliability significance of outages and the market incentives for availability and continue to look for ways to improve capacity availability during cold weather. For example, MISO's Electric and Natural Gas Coordination Task Force is exploring solutions regarding emerging natural gas issues. The MISO Reliability Subcommittee reviews seasonal preparations by generation owners and Transmission Owners, including cold weather readiness. Additionally, the MISO Supply Adequacy Working Group (SAWG) evaluates appropriate accounting of generation capacity in the Planning Reserve Margin (PRM) calculations and accreditation of capacity to meet the PRM requirements. Currently the SAWG is considering changing from the use of annual capacity values to the use of seasonal capacity values.

Northeast Power Coordinating Council

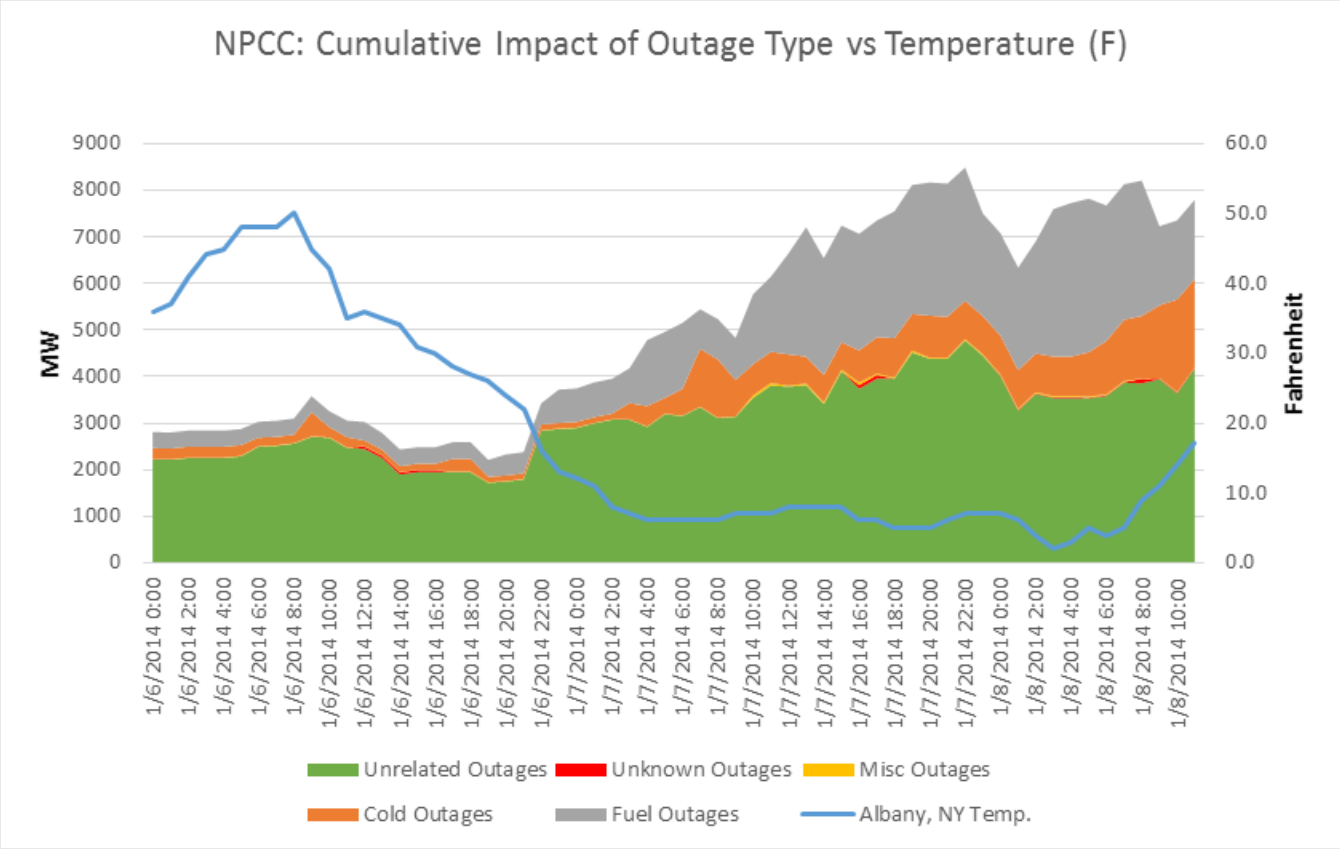


Figure 8: NPCC (US): Cumulative Impact of Outage Type vs. Temperature (F)

NPCC did not experience many cold weather outages at the start of the time frame identified by this report, with a peak of 518 MW of outages in the first 30 hours. However, as the cold air mass that comprised the polar vortex made its way into the Northeast, NPCC did experience more outages from the stress of the extreme event, reaching up to 1,984 MW of lost capacity. A significant portion of the cold-related outages, especially in the final hours of the polar vortex study period, were related to fuel-gelling issues. Of the 1,984 MW of cold-weather-related outages reported at 10:00 a.m. on January 8, 2014, 770 MW were related to fuel-gelling issues. Some dual-fuel units experienced challenges ranging from a lack of natural gas required for starting the alternate fuel, to fuel freezing in the injectors. While many of these units' preparations included testing of the dual-fuel switchover capability, none of the testing was performed under the actual extreme conditions. Excluding the fuel-gelling issues, the non-Canadian portions of NPCC experienced eight hours in the time frame of interest during which the amount of cold-weather-related generation outages exceeded 1,000 MW and never exceeded more than 1,300 MW.

Excluding unrelated outages, outages related to curtailments and interruptions of natural gas delivery were the significant contributor of the NPCC generator outages. These outages totaled a maximum of 3,296 MW of generators and, as shown in Figure 8, they significantly impacted NPCC's generation resources starting at approximately 10:00 a.m. on January 7, 2014.

ReliabilityFirst

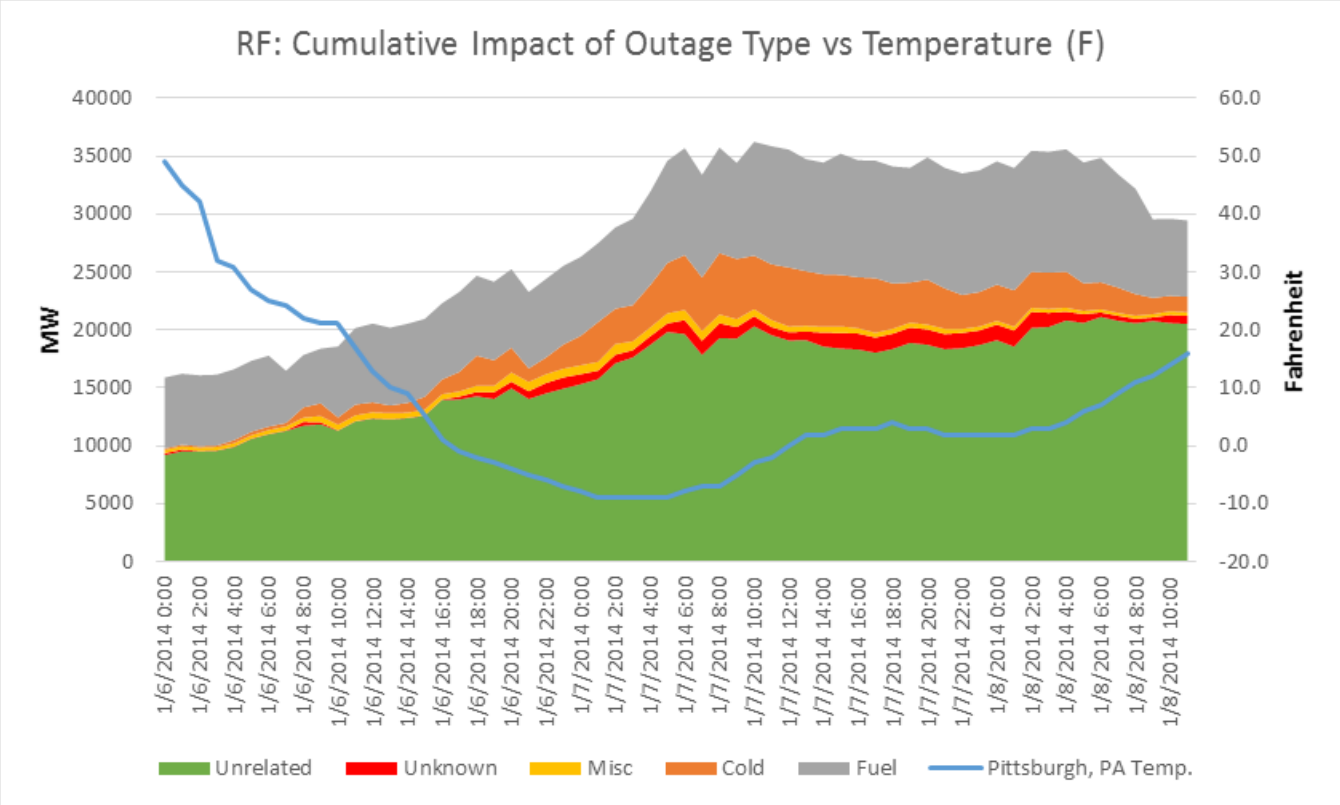


Figure 9: RF: Cumulative Impact of Outage Type vs. Temperature (F)

ReliabilityFirst experienced the greatest number of generator outages of all the Regions. While some of these outages were the result of cold weather, it was the number of units that were either unavailable or derated due to the lack of natural gas availability that was the major issue for RF. This situation was exacerbated by the loss of a natural gas compressor station in Delmont, PA on January 7, 2014, which reduced the delivery capacity of the Texas Eastern (TE) pipeline by 575,000 DTh/day. While the conversion of DTh/day to generating capacity can vary depending on the specific generators and type of generation (simple cycle vs. combined cycle, for instance), this represents approximately 1,700–2,300 MW of generation running 24 hours a day. The variance depends on the heat rates of the units involved, with the higher estimate obtained from the most efficient unit types.

Overall, RF experienced a maximum of just over 5,300 MW of outages due to cold weather issues, and only 13 of the 60 hours had 4,000 MW or more of cold-weather-related outages. In contrast, RF experienced over 9,000 MW of fuel-related outages in 25 of the 60 hours of interest, and reached a peak outage level of approximately 10,700 MW due to fuel.

SERC Reliability Corporation

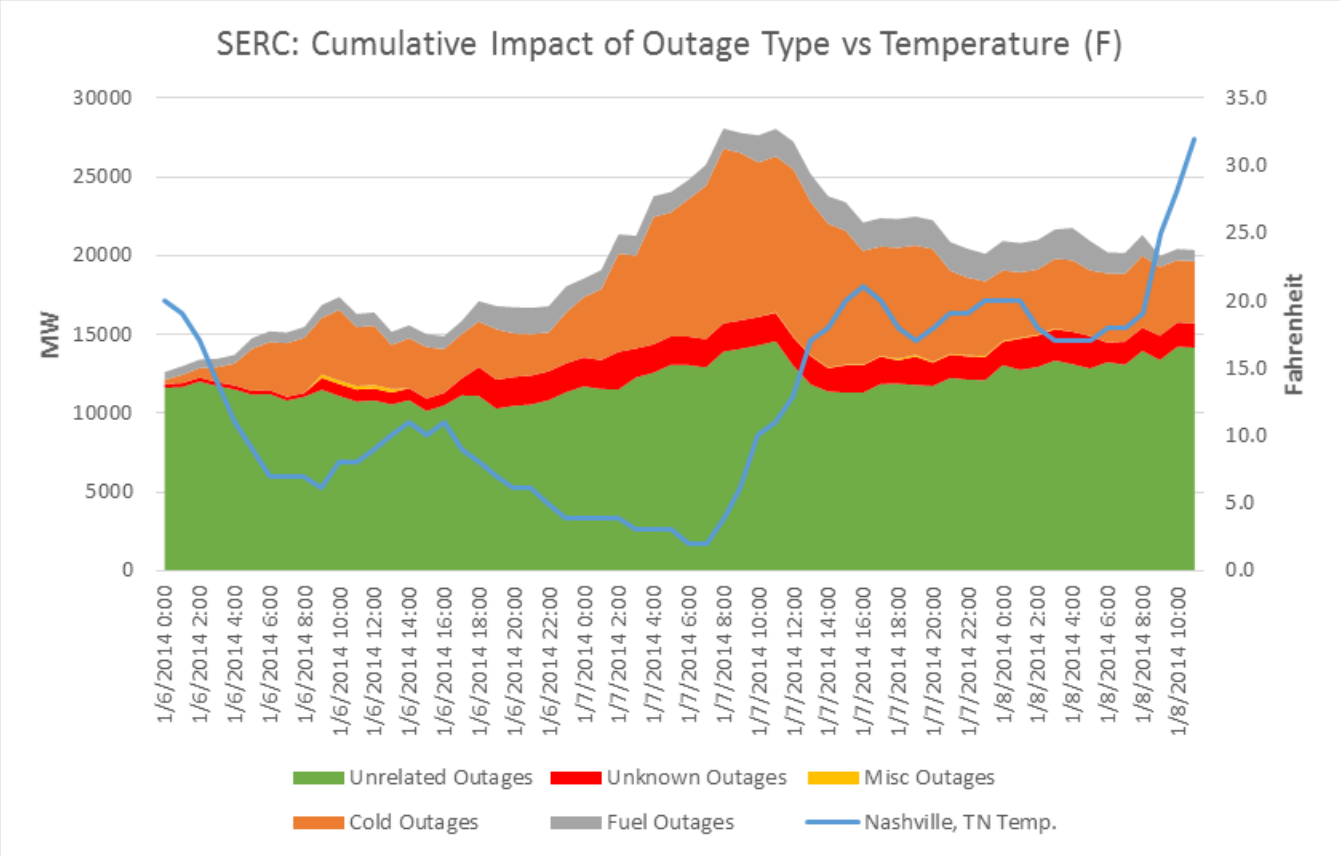


Figure 10: SERC: Cumulative Impact of Outage Type vs. Temperature (F)

Figure 10 shows that SERC's main driver of outages and derations related to polar vortex issues was cold weather, impacting approximately 11,000 MW of generation at 8:00 a.m. on January 7, 2014. Of this generation capacity, approximately 10,600 MW were related to equipment issues. These equipment issues included heat trace, insulation, regulators reacting slowly to change in pressures, frozen sensors, and even cold lubricants. Typically, generation equipment in this geographical area is designed for an expected low of 10° F. The extreme departure from design temperatures coupled with severe wind chills within SERC resulted in significant impact to generation capacity. The extended time below freezing is extremely rare for the southern United States, with the temperatures outside most winter generation design characteristics.

As compared to other Regions, fuel availability issues played a small role within SERC, impacting approximately 2,050 MW of generation. These outages were largely related to curtailments and interruptions of natural gas delivery to the plant. The grid within SERC performed extremely well for the conditions across the three days. As mentioned above, the extended time of below-design-criteria conditions for three days impacted the performance of generators. Entities within SERC have started a thorough review of the event and a review of their practices and procedures for winter preparation, including those that were implemented as a result of the 2011 Southwest Cold Weather event.

Southwest Power Pool Regional Entity

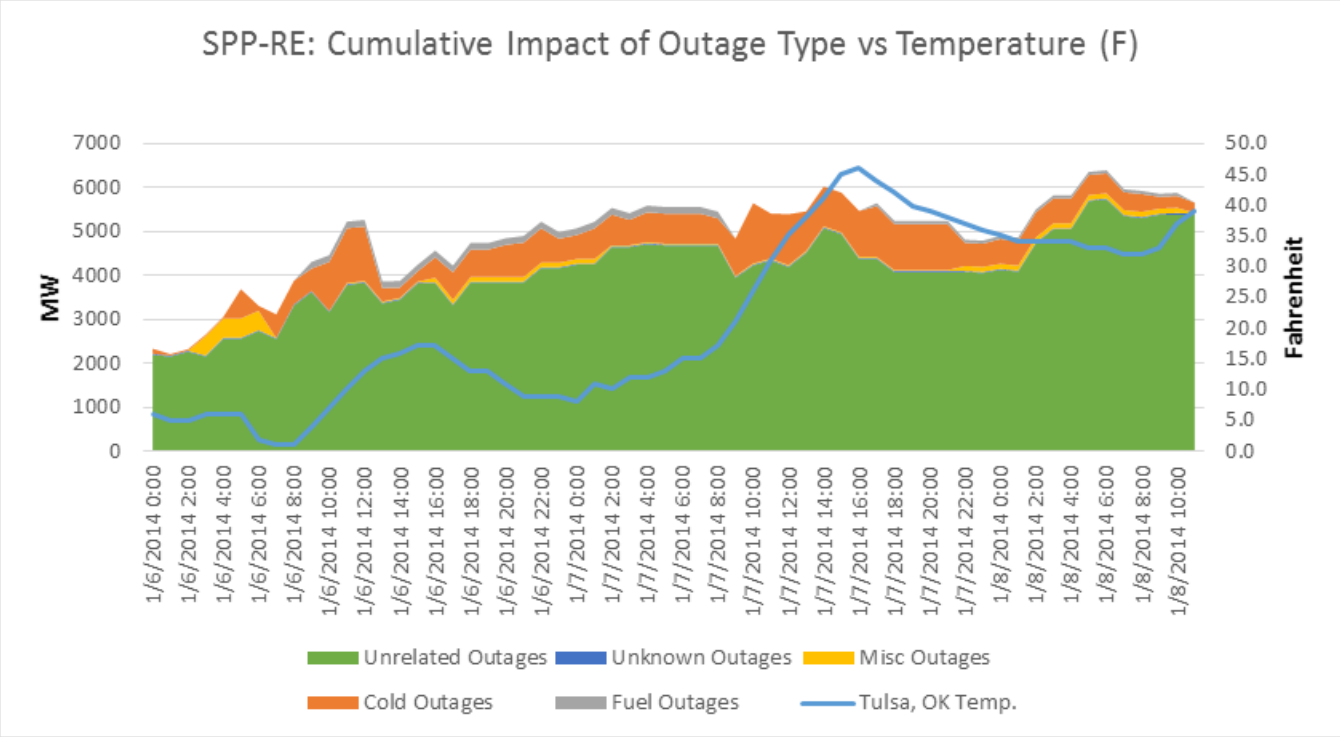


Figure 11: SPP: Cumulative Impact of Outage Type vs. Temperature (F)

SPP was minimally impacted by the fuel outages, with a maximum of approximately 150 MW of fuel-related outages. Additionally, cold weather directly impacted a maximum of approximately 1,200 MW of generation, with 41 hours being under 700 MW of cold-impacted outages. Excluding Florida, SPP experienced the lowest number of cold-impacted outages, despite being one of the first areas impacted by the polar vortex.

Texas Reliability Entity

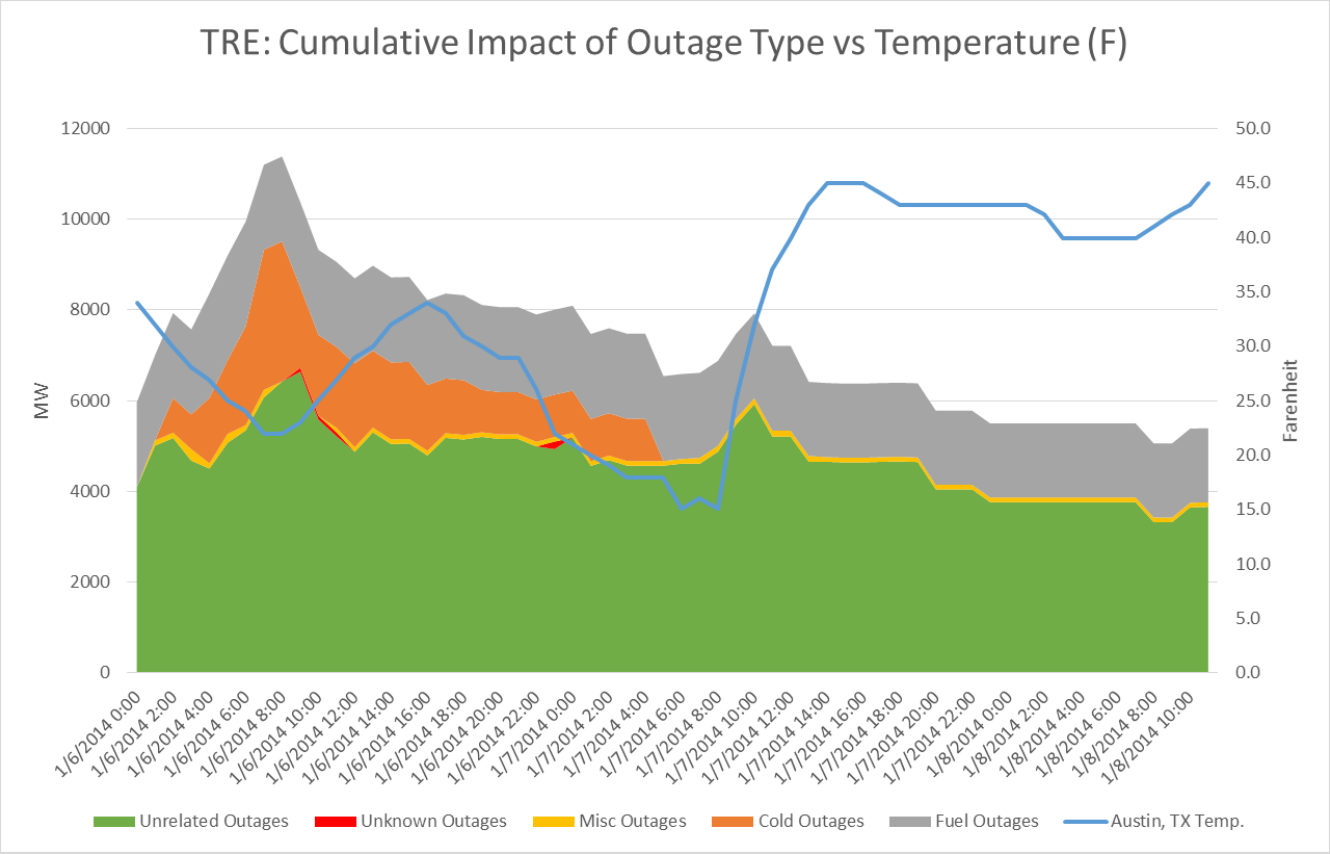


Figure 12: TRE: Cumulative Impact of Outage Type vs. Temperature (F)

Texas Reliability Entity experienced a maximum of 3,087 MW of cold-weather-related generation outages, but by the end of the start of peak hours of January 7, 2014, the interconnection had completely recovered from the cold weather issues. The cold-impacted generation capacity does not include over 700 MW of wind generation low-temperature-related trips, which are currently not reported in GADS. These outages were due to cold temperatures outside the operating limits of the wind turbines. Based on GADS data, the maximum capacity affected by forced outages and derations was 11,385 MW.

Fuel-related issues were fairly consistent, however, ranging from a high of 2,309 MW down to a low of 1,634 MW. These restrictions were the result of the natural gas transportation system experiencing extremely high demand, resulting in fuel restrictions to power plants located near a major metropolitan area.

Generator Issues by Fuel Type

Figure 13 illustrates the percentage of installed capacity sorted by the appropriate fuel types located within the Eastern and ERCOT Interconnections. Of the three major fuel types, representing 83 percent of all generation, over 40 percent is natural gas, 31 percent is coal, and 12 percent is nuclear. Figure 13 shows that of these three fuel types, the polar vortex had the least impact on nuclear plants. Coal plants accounted for 26 percent of the outages. Natural gas represented over 55 percent of the total outages during the polar vortex.

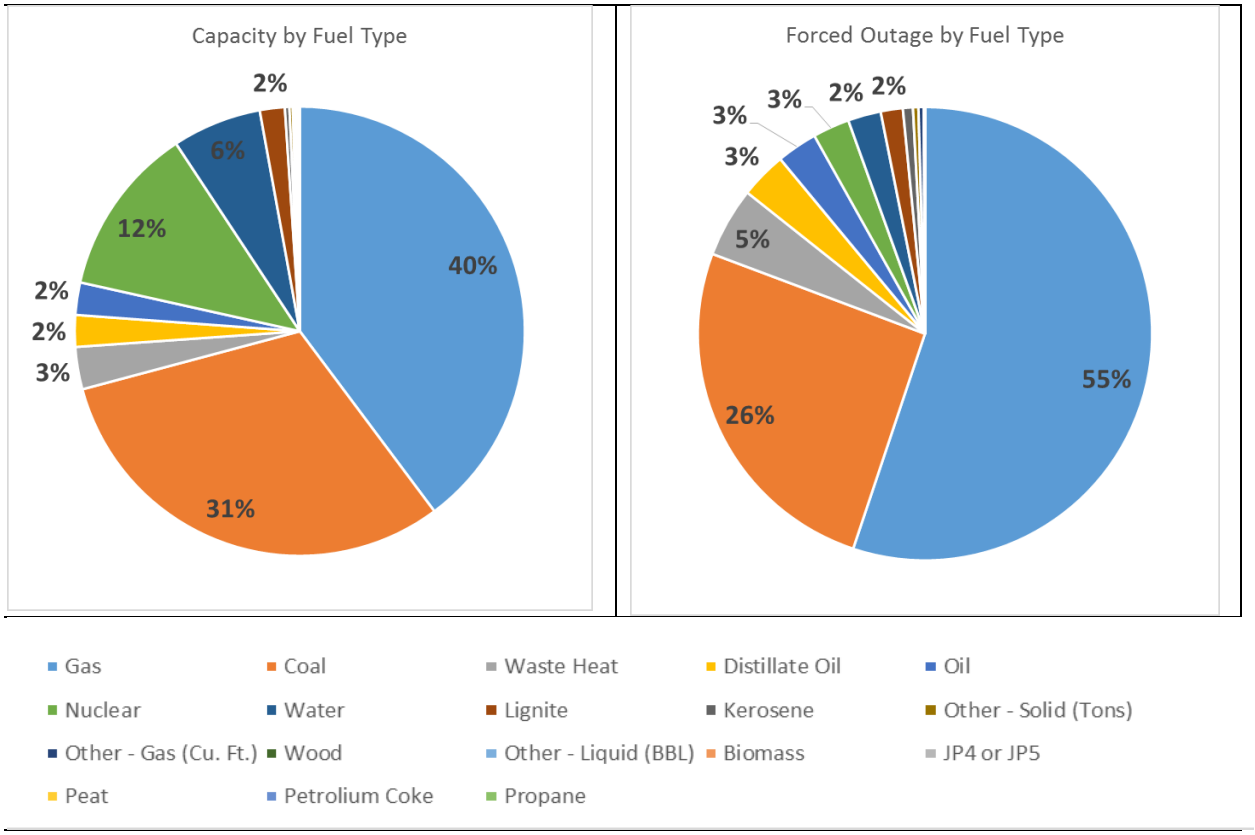


Figure 13: Percentage of Net Dependable Capacity by Fuel Type (left); Percentage of Capacity Lost During Polar Vortex by Fuel Type (right) in Eastern and ERCOT Interconnections

One of the largest issues that impacted gas-fired generation was the curtailment or interruption of fuel supply. Unlike coal and fuel oil, natural gas is not typically stored on site. As a result, generators rely on real-time delivery of natural gas from their suppliers. As natural gas is widely used outside the power sector, the demand from other sectors—in particular residential heating demand during cold winter weather—can critically affect the ability of pipeline operators and suppliers to deliver natural gas to the power sector.

Cold weather effects on equipment

The extreme cold weather had a major impact on generation equipment. Of the approximately 19,500 MW of capacity lost due to cold weather, over 17,700 MW was due to frozen equipment.

The following list illustrates some of the challenges faced by generator owners and operators due to the effects of cold weather on equipment. These challenges affected almost every dimension of the generation, from instrumentation, to fuel quality, to air-fuel mix, etc. Newer generation units' cold weather preparations were tested for potentially the first time for these temperature extremes, and many older units experienced extremes beyond what they were designed to operate. The examples below are individual occurrences that are

representative of the challenges faced during this extreme period. Not all of these instances resulted in a forced outage; many just delayed the unit's ability to come on-line or resulted in the unit's derating.

Examples of extreme cold weather effects on generation:

- The drum level transmitter sensing lines froze, indicating a false drum level and consequently tripping the boiler.
- Moisture ingress caused gear boxes, valve positioners, and solenoid valves to fail due to freezing.
- Heat trace electric circuits not working prior to the event tripped during the event, or were miswired.
- Cold air backflow down the stack and into the boiler affected performance.
- During start-up from the previous outage, the B phase stab disconnect was not fully engaged, which resulted in voltage differential between phases. The unit had to be removed from service to repair the disconnect. Upon investigation, the damage to the disconnect was caused by ice build-up from the unit's cooling towers.
- Circulating water was frozen, causing a loss of supply of needed cooling water.
- Extreme cold weather and cold oil resulted in oil pressure control tripping.
- A plant steam pressure transmitter froze due to extreme cold conditions, which limited the operation of the condenser air removal equipment, and the unit tripped on low vacuum. The transmitter is located inside the main building close to an exterior wall louver.
- Impulse tube lines, level transmitters, or pressure sensing lines were uninsulated or underinsulated, resulting in freezing components.
- A transformer had water in it and froze.
- A feedwater heater pressure sensing line froze, which required the unit to be taken off-line.
- Fan damper operation was sluggish during cold weather due to cold grease, and a deaerator level indication had a frozen sensing line.
- Steam and water flow transmitters were uninsulated or underinsulated, resulting in freezing components.
- The unit tripped due to a frozen super heat pressure transmitter.
- A collector ring failure was caused by insufficient brush tension resulting from very cold temperatures.
- Air entrainment in the sensing lines caused a transmitter to fail. The line did not actually freeze, but it interfered with instrument compensation.
- A frozen gas valve caused a unit outage.
- The diesel fuel changed consistency, rendering the fuel unusable in the cold weather.
- Moisture in an air line to the inlet bleed heat valve froze.
- The static frequency converter initiated a trip during preparation of Static Frequency Converter & Static Excitation System (SFC/SES) caused by not receiving exciter circuit breaker checkback signal for the closed position. Subsequent failures were caused by not receiving the checkback signals from the start disconnect switch in the generator breaker. Extreme cold temperatures caused grease on start disconnect switch stabs to become tacky and not allow it to close without binding.
- Oil pressure was affected due to cold oil from the lube oil (LO) cooler entering the LO supply header too rapidly. The LO temperature control valve has no cold ambient bias to slow down movement in winter.

- Frozen NO_X water header pressure sensing lines in the unit resulted in no available NO_X water injection for emissions control.
- Water froze in a water manifold that had not been purged of water.
- Generator logic tripped the turbine due to a frozen water flush transmitter. The transmitter was frozen due to cold weather; however, the logic should not have tripped the unit.
- The outage was due to a failure of the water injection heating system. Cold weather may have contributed to but was not the primary cause of the outage. Power was removed from the heating system due to a water leak that caused an electrical short circuit. It is not known if cold weather caused or contributed to the initial water leak. Once power was removed from the heat tracing on the water injection pipes, they froze. The situation was corrected by placing a tent around the problem area and using a torpedo heater to unfreeze the water lines.
- A unit water injection variable frequency drive (VFD) controller tripped due to extreme weather, requiring a unit shutdown to prevent emission exceedance.
- A unit heater tripped, which affected operation of VFD. During restarting the water injection VFD, unit was at upper load and flamed out from inrush of water.
- A frozen water valve located outside for the oil cooling system caused the unit to trip. The ambient temperature at the time of the trip was -3° F with an 8 mph SW wind.
- The unit would not transfer to "Pre-Mix Steady State" due to operating in the cold ambient temperatures; it required combustion tuning for the colder conditions.
- A gas transfer purge valve froze.
- The pressure dropped due to regulator not being able to react quickly enough because of the extreme cold temperature.
- An output breaker would not close due to the cold.
- The premix line froze due to heat tracing failure.
- Fuel oil gelled the filters due to the cold temperatures.
- A hydraulic starter pressure sensing line froze.
- Lube oil temperature was below 50° F, causing the unit to be in a not-ready-to-start state.
- The diesel fuel being provided to the starting motor gelled due the extreme cold temperatures.
- The diesel starting engine failed to provide enough turbine speed to initiate firing.
- A liquid fuel modulating valve frozen (located in unheated engine compartment when off-line).
- A starter duct pressure switch located in unheated engine compartment froze.
- A unit tripped on loss of flame due to the combination of fuel oil delivery temperature being low and ignition gas being insufficient to maintain the flame.
- A unit could not start due to hydraulic temperatures too low for proper operation of fuel valves.
- Frozen regulator on monitor valve at meter station caused low fuel gas pressure.
- The inlet air intake was covered with snow and ice.
- Moisture in a fuel oil pressure switch froze and the pressure switch diaphragm burst.

- The fogging and overspray were put in a winterized state. The systems were available but required additional time to return to service.
- Cold weather caused water injection lines to become frozen, which resulted in a transmitter control issue.
- The gas control and purge valves were sluggish due the extreme temperature. The control timers for the valves were adjusted to allow for the longer valve operating time.
- The relay setting did not take into account the higher-than-normal output for the extreme cold weather.
- The lube oil was too cold because the compartment heater malfunctioned. This caused the lube oil temp alarm to trip the unit in start-up.
- A solenoid was frozen on the water injection system. This caused an emissions issue.
- Compressor blade icing caused a unit outage.
- Units tripped when the units were being transferred from gas to liquid fuel. These CTs were running on gas when the site was asked to transfer them to liquid fuel due to limited gas availability. Extremely cold temperatures along with the liquid fuel heaters being out of service contributed to an increase in fuel oil viscosity that led to a high filter differential pressure and subsequent fuel system fault trips while attempting to transfer to liquid fuel.
- Low ambient temperature led to fuel waxing and clouding.
- Frazil ice blocked the intake, causing insufficient water supply to the turbine.
- Due to low temperature, the seal oil regulator froze, allowing the oil pressure to rise above the hydrogen pressure, therefore putting oil inside the steam turbine generator.
- A steam turbine exhaust pressure switch for HP turbine froze, which signaled a false high pressure, thereby tripping the steam turbine.
- Cold temperature caused materials on the generator hydrogen cooler cooling water loop to contract, and the flanged joint at generator shell began to leak hydrogen. The flange bolting was re-torqued to stop the leak.
- A seal steam pressure transmitter sensing line froze, causing pressure to read high opening bypass to condenser, which in turned caused loss of sealing steam to turbine.
- A unit tripped due to cooling tower drift freezing onto and restricting flow through the inlet bird screen; with enough build-up, this caused the implosion doors to open.
- While switching from gas to oil, a process step was missed, resulting in the trip.
- A unit was shut down for inspection because a noise could be heard during the hourly inspections. Ice was found on the inlet guide vanes.

Chapter 3 – Discussion

Increased reliance on natural gas during the polar vortex exposed the industry to various challenges with fuel supply and delivery. This increased reliance, compounded by generation outages during the extreme conditions, increased the risks to the reliable operation of the BPS.

As the industry relies more on natural-gas-fired capacity to meet electricity needs, it is important to examine potential risks associated with increased dependence on a single fuel type. The extent of these concerns varies from Region to Region; however, they are most acute in areas where power generators rely on interruptible natural gas pipeline transportation.

Unlike coal and fuel oil, natural gas is not typically stored on site. As a result, real-time delivery of natural gas through a network of pipelines and bulk gas storage is critical to support electric generators. Natural gas is widely used outside the power sector, and the demand from other sectors—particularly coincident end-user gas peak demand during cold winter weather—critically affects gas providers' ability to deliver interruptible transportation service in the power sector. Additionally, demand for natural gas is expected to grow in other sectors (e.g., transportation, exports, and manufacturing).

The following excerpts are from industry participant discussions about the polar vortex:

> *"Some gas-fired units have the capability to use an alternate fuel (dual-fuel capability), which increases flexibility when gas supply becomes tight. The predominant alternate fuel is oil. While dual-fuel units increase flexibility, there were still challenges operating the units on oil. PJM requested dual-fuel generation owners unable to secure gas to operate their units on oil during the extremely cold weather events. Even with this flexibility, generation owners encountered issues including run-time limits related to permit-defined environmental restrictions, resupply challenges and increased failure rates for unit startup. Units that switch to oil operate with increased emissions, which limits their maximum run times due to environmental constraints. In other cases, units operating on oil may have had only limited ability to make and store demineralized water for the injection systems that must be operated to reduce nitrogen oxide emissions when running on oil. PJM coordinated with generation owners that needed to decrease the maximum run time per day for their units in order to conserve emission credits. Identification and tracking of fuel limitations was done manually by PJM and the generator owners. There were approximately 1,000 MW of generation with decreased run times for emission reasons.*
>
> *The increase in demand for oil caused another challenge for generation owners. Many units in the Northeast switched to oil as gas became unavailable increasing demand for oil. In some cases, oil suppliers began to run low on inventory or deliveries were slow because increased demand was unexpected and available delivery trucks were limited. Generation owners found it difficult to keep oil tanks full on a daily basis and had to limit run hours for their units. There were approximately 2,000-3,000 MW of generation affected by oil supply and delivery issues. Also, generating units running on oil have an increased failure-to-start rate due to clogged fuel lines."*[7]

Many outages, including a number of those in the southeastern United States, were the result of extreme cold weather that was below the design basis of generating units. Industry should identify and protect against failures that occurred within the design basis of their plants. As illustrated in Figure 10 (Chapter 2), SERC experienced 25 hours during the study period where they were below their typical temperature design basis, including 17 continuous hours below that basis.

[7] PJM Report: http://www.pjm.com/~/media/documents/reports/20140509-analysis-of-operational-events-and-market-impacts-during-the-jan-2014-cold-weather-events.ashx pg. 39-40

The analysis of the GADS data provided in Appendix A shows that most generating units performed in the expected range of EFOR during the month of January 2014, based on historical analysis. Overall, most units performed with an EFOR within or slightly better than (i.e., below) the expected range, based on the past five years. The exception is natural gas units, which in two Regions experienced a higher-than-expected EFOR. This observation validates the concerns that NERC raised in the *2013 Long-Term Reliability Assessment*[8] on increased dependence on natural gas for electric power.

[8] http://www.nerc.com/pa/RAPA/ra/Reliability_Assessments_DL/2013_LTRA_FINAL.pdf, pg. 35

Chapter 4 – Conclusion

Unlike the February 2011 Southwest Cold Weather Event, the 2014 polar vortex resulted in many generator outages from entities exceeding the design basis of their plants and difficulties facing the natural gas transportation sector. System Operators were faced with many difficult decisions and were able to successfully maintain reliability through extensive previous training and preparation. During the polar vortex, several System Operators used load reduction techniques such as voltage reduction, interruptible loads, and demand-side management. Many System Operators also made effective use of emergency procedures to manage loads and generation.

Observations and Recommendations

Lessons Learned from the February 2011 Southwest event highlighted the importance of preparation for extreme weather events. The following observations and recommendations are based on the analysis in this report:

Observations

1. Generation facilities have made improvements in their winter preparation activities since February 2011; however, every extreme event provides insight for future improvements. Generation facilities across all Regions have indicated that they have reviewed and/or implemented recommendations from the *February 2011 Southwest Cold Weather Event Lessons Learned*[9] as well as the *Generator Winter Weather Readiness* guideline.
2. The value of regular training and annual drills was demonstrated during events, as the operators and other RC area entities were able to effectively and successfully implement emergency procedures.
3. Proactive communication and coordination between the RCs and within the RC areas themselves helped ensure appropriate situational awareness was maintained and facilitated rapid response as needed.
4. Planned and forced generation outages in some Regions exceeded the worst-case assumptions used in seasonal assessments. These assumptions warrant further review; in particular, the assumptions for generating unit forced and planned outage rates.
5. Some ISO/RTOs conducted detailed seasonal fuel assurance surveys to include gas transportation arrangements, starting oil inventories, and oil replacement capabilities (oil transportation capability).
6. Many outages, including a number of those in the southeastern United States, were the result of extreme ambient temperatures that were below the design basis of the generating unit.

Recommendations

1. Examine and review the natural gas supply issues encountered during the event. Industry should also work with gas suppliers, markets, and regulators to quickly identify issues with natural gas supply and transportation so that appropriate actions can be developed and implemented to allow generators to be able to secure firm supply and transportation at a reasonable rate.
2. Review and update power plant weatherization programs as a result of lessons learned from this event. This includes review of plant procedures, training programs for severe weather and winter weather events, and availability of material and equipment for response to these events. Entities should continue

[9] http://www.nerc.com/pa/rrm/ea/Pages/February-2011-Southwest-Cold-Weather-Event.aspx

to follow the Reliability Guideline (*Generating Unit Winter Weather Readiness – Current Industry Practices*).[10]

3. Continue or consider implementing a program of periodic site reviews of generation facilities' winter preparation. These programs produced tangible benefits in the ERCOT Interconnection by improving generator winter preparation and sharing of good industry practices, and can be implemented within an individual company, an ISO/RTO, an appropriate Regional Entity, or any combination.
4. Review the basis for forced and planned generation outages used in seasonal assessments to ensure that appropriate outage rates for the extreme cases are correct and that unit derates are appropriately included.
5. Review generation and transmission outage scheduling processes to limit planned outages during possible peak winter periods.
6. Entity winter assessments should include base assumptions and stress cases for the loss of varying amounts of gas-fired generation, and should consider oil burn rates relative to oil replenishment rates to determine the duration of continuous operation for oil-fired generation.
7. Continue to improve operations management awareness of the fuel status of all generators, including improved awareness of pipeline system conditions. This might include a daily fuel inventory solicitation process, ability to dispatch plants early in anticipation of extreme winter weather, and increased communication channels with electric and gas industries during extreme events.
8. Ensure that the fuel on hand and/or ordered for the winter season is appropriately protected from the effects of cold weather at the expected extreme temperatures.
9. Industry should work to identify and protect against outages that occurred within the cold weather design basis of the plant. Additionally, entities should review the winter cold weather temperature design basis for their generating units to determine if improvements are needed, while ensuring that the generating unit's ability to withstand higher temperatures in the summer is not compromised.
10. Industry should review internal processes to ensure they are ready to take proactive actions to secure the waivers (market, environmental, fuel, etc.) from the appropriate entities. For example, PJM requested waivers of certain provisions of PJM's governing documents that would permit them to share certain non-public information with natural gas pipeline operators during the forecasted extreme weather conditions. FERC responded promptly to PJM's filing, which enabled those communications to commence quickly.[11]

[10] http://www.nerc.com/pa/rrm/ea/ColdWeatherTrainingMaterials/Relibility_Guideline_Generating_Unit_Winter_Weather_Readiness.pdf

[11] PJM Report: http://www.pjm.com/~/media/documents/reports/20140509-analysis-of-operational-events-and-market-impacts-during-the-jan-2014-cold-weather-events.ashx pg. 11

Appendix A

Overview of GADS

GADS was developed by utility designers, operating engineers, and system planners to meet the information needs of the electric utility industry. For this purpose, specific objectives for the GADS program were established: compilation and maintenance of an accurate, dependable, and comprehensive database capable of monitoring the performance of electric generating units and major pieces of equipment. GADS is not a substitute for the detailed, often unique, data systems typically found at power plants, or for maintenance data programs that record detailed equipment failures and repair techniques. The objectives of the GADS program can be met through the collective effort of participating GADS members, the cooperation in reporting to GADS, and sharing information with the industry.

Based on research by the IEEE 762 committee, the boundary between the GENCOs and TRANSCOs is as follows: "A generating unit includes all equipment up to (in preferred order): (1) the high-voltage terminals of the generator step-up (GSU) transformer and the station service transformers; (2) the GSU transformer (load) side of the generator-voltage circuit breakers; or (3) at such equipment boundary as may be reasonable considering the design and configuration of the generating unit."

An event occurs any time a generating unit's operating status or capability changes. Four general classifications of events are reported to GADS: outages, deratings, reserve shutdowns, and non-curtailing events. Reporting event data, in addition to performance and design data, provides all the information needed to evaluate generating unit availability. Event data are especially useful since they are often used to do specialized unit and equipment operation and design analyses.

Participation in the GADS program is mandatory for all conventional units 20 MW and larger (as of January 1, 2013). Reporting the level of detail requested in these GADS Data Reporting Instructions enables industry analysts to perform detailed, useful analyses.

All units except hydro and pumped storage units without automatic data recording equipment are required to report reserve shutdown events. All other events (forced, maintenance, and planned) must be reported.

Calculations used to determine equivalent forced outage rate

Service hours (SH) is the sum of all unit service hours.

Available hours (AH) is the sum of all service hours (SH) + reserve shutdown hours (RSH) + pumping hours + synchronous condensing hours.

Period hours (PH) is the number of hours that the unit was in the active state.

Forced outage hours (FOH) is the sum of forced outages + startup failures hours.

Equivalent forced derated hours (EFDH) – Each individual forced derating (D1, D2, and D3) is transformed into equivalent full outage hour(s). This is calculated by multiplying the actual duration of the derating (hours) by the size of the reduction (MW) and dividing by the net maximum capacity (NMC). These equivalent hour(s) are then summed.

Equivalent forced derated hours during reserve shutdown (EFDHRS) – Each individual forced derating (D1, D2, and D3) that occurred during a reserve shutdown (RS) is transformed into equivalent full outage hour(s). This is

calculated by multiplying the actual duration of the derating (hours) by the size of the reduction (MW) and dividing by the NMC. These equivalent hour(s) are then summed.

Equivalent Forced Outage Rate (EFOR) is calculated by:

$$EFOR = \frac{(FOH + EFDH)}{(FOH + SH + Synchronous\ Condensing\ Hours + Pumping\ Hours + EFDHRS)}$$

Weighted versus time-based methods for pooled statistics

Two methods are used to calculate pooled (grouping) unit statistics for generation:

1. Unweighted (time-based) methods for calculating pooled (grouping) unit statistics.
2. Weighted (capacity-based) methods for calculating pooling (grouping) unit statistics.

When a single generating unit's performance statistics are calculated, it does not matter whether unweighted or weighted-based statistics are used. The answer will generally be the same. The real difference between the unweighted and weighted statistics is in pooling (or grouping) of a set of generating units. In such cases, a group of units of similar size will show little or no difference, but for groups of units where the MW size is very different (greater than 50 MW), the statistics will be very different.

With unweighted statistics, all units are considered equal in outage impact. In the unweighted equations, no MW size is introduced into the equations, and the results are based on time, not energy produced (or not produced). In such cases, a 50 MW gas turbine and a 1,000 MW nuclear unit have the same impact of the resulting statistics.

With weighted statistics, the larger MW size unit in the group has more impact on the final statistics than a smaller generating unit. That is because the MW size of the unit (NMC) is part of the equation. In such cases, a 1,000 MW nuclear unit would have 20 times the impact on the final outcome of the calculation than would its 50 MW gas turbine companion.

This study used the weighted method for calculating pooling (grouping) unit statistics for generation.

Analysis of EFOR by Regional Entity

The following is an analysis of EFOR for the months of January, February, and March for 2009–2014. Also, for the purposes of this analysis, FRCC and WECC will not be examined, since they were not directly involved in the polar vortex. In addition, all values of EFOR in this appendix are calculated monthly.

Coal

Figures A1, A2, and A3 provide historical EFOR for coal units for January, February, and March by year and Regional Entity. In all Regions examined, coal units experienced an EFOR in January 2014 well within the range of expected EFOR based on the prior five winter operating periods. The historical winter monthly EFOR performance of coal units in MRO ranged from 4.8 to 7.6 percent, and in January 2014 they experienced an EFOR of 5.3 percent. In NPCC, the historical winter monthly EFOR performance ranged from 6.9 to 21.2 percent, and coal units experienced an EFOR of 7.3 percent in January 2014. Likewise, coal units in RF experienced an EFOR of 9.3 in January 2014, compared with a historical range of 8.5 to 14.2 percent. In SERC, coal units experienced an EFOR of 4.9 in January 2014, which was better than any historical winter monthly EFOR for the years examined (prior monthly values ranged from 5.0 to 10.2). The EFOR performance of coal units in SPP ranged from 3.2 to 13.6 percent, and in January 2014 they experienced an EFOR of 6.4 percent. Finally, coal units in TRE experienced an EFOR of 12.8 percent in January 2014, compared with a historical range of 0 to 14.3 percent.

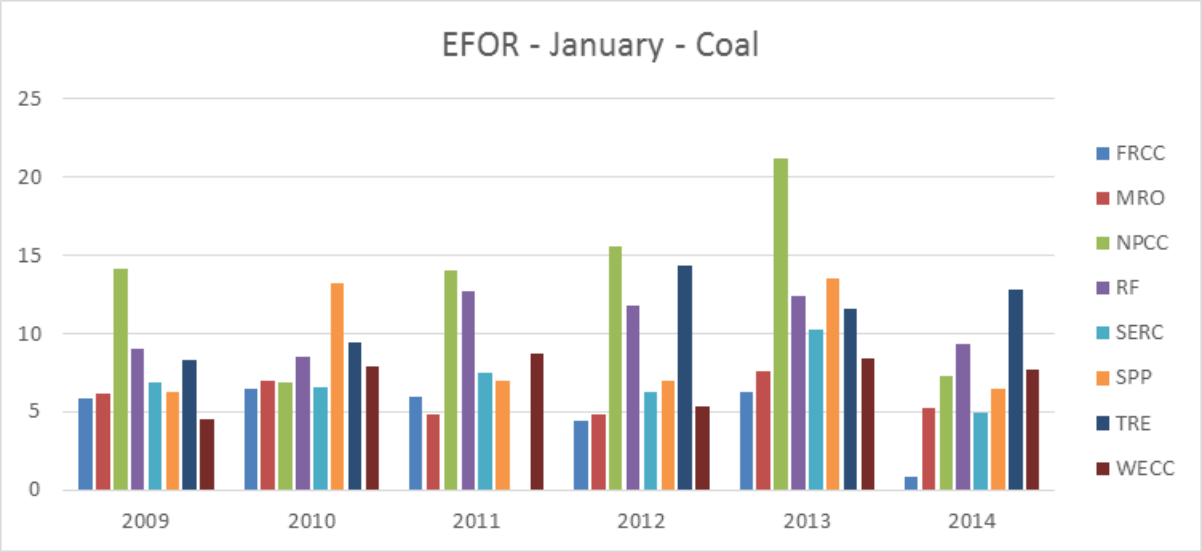


Figure A1: Historical EFOR for Coal Units in January by Year and Regional Entity

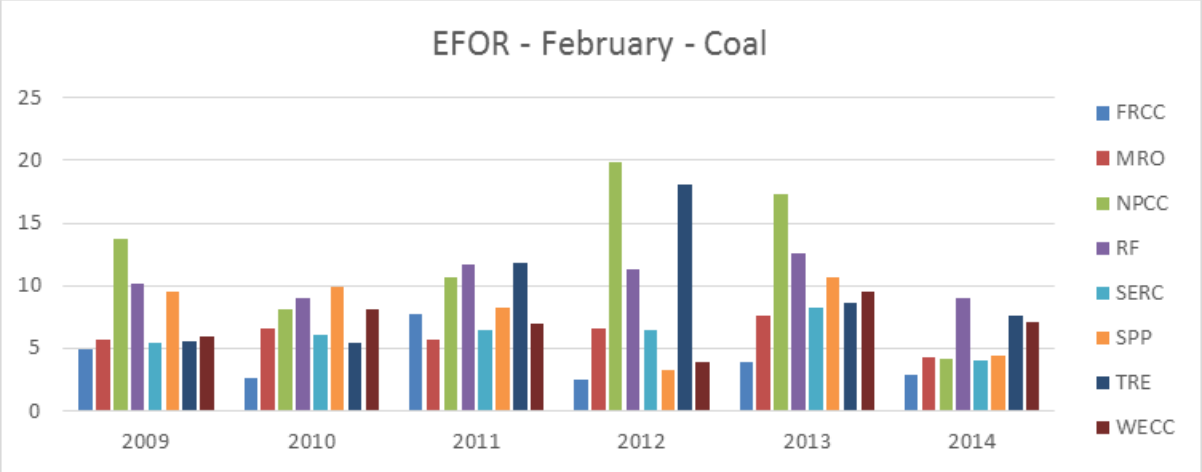


Figure A2: Historical EFOR for Coal Units in February by Year and Regional Entity

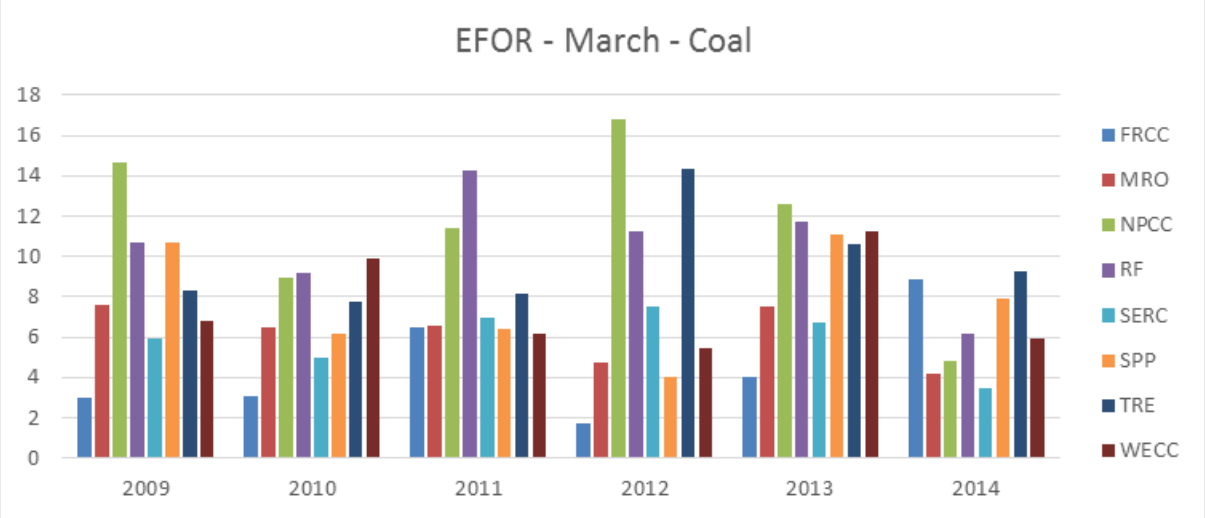


Figure A3: Historical EFOR for Coal Units in March by Year and Regional Entity

Natural Gas

Figures A4, A5, and A6 provide historical EFOR for natural gas units for January, February, and March by year and Regional Entity. In all Regions examined, natural gas units experienced an EFOR in January 2014 within the range of expected EFOR based on the prior five winter operating periods. The EFORs in NPCC, SERC, and SPP were near the top end of the range for their respective Region.

The historical winter monthly EFOR performance of natural gas units in MRO ranged from 8.3 to 18.3 percent, and in January 2014 they experienced an EFOR of 17.8 percent. In NPCC, the historical winter monthly EFOR performance ranged from 16.5 to 39.2 percent, and natural gas units experienced an EFOR of 35.4 percent in January 2014. Likewise, natural gas units in RF experienced an EFOR of 18.5 percent in January 2014, compared with a historical range of 4.8 to 25.5 percent. In SERC, natural gas units experienced an EFOR of 11.4 percent in January 2014, which was the same as the worst monthly EFOR calculated for the years examined (prior monthly values ranged from 6.3 to 11.4 percent). The EFOR performance of natural gas units in SPP ranged from 5.8 to 21.1 percent, and in January 2014 they experienced an EFOR of 19.5 percent. Finally, natural gas units in TRE experienced an EFOR of 5.3 percent in January 2014, compared with a historical range of 2.7 to 16.8 percent.

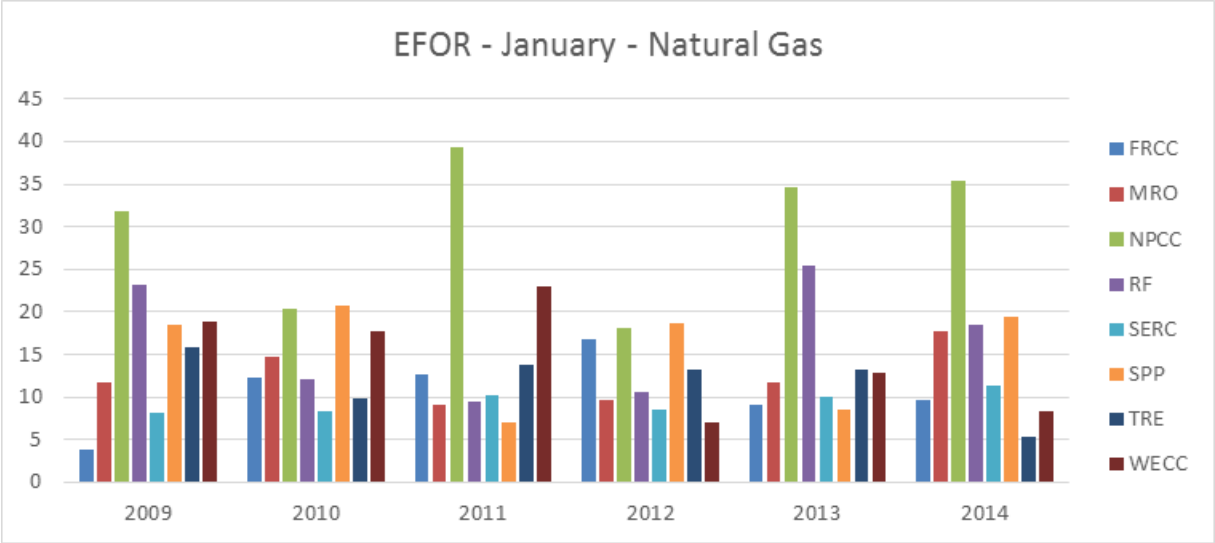


Figure A4: Historical EFOR for Natural Gas in January by Year and Regional Entity

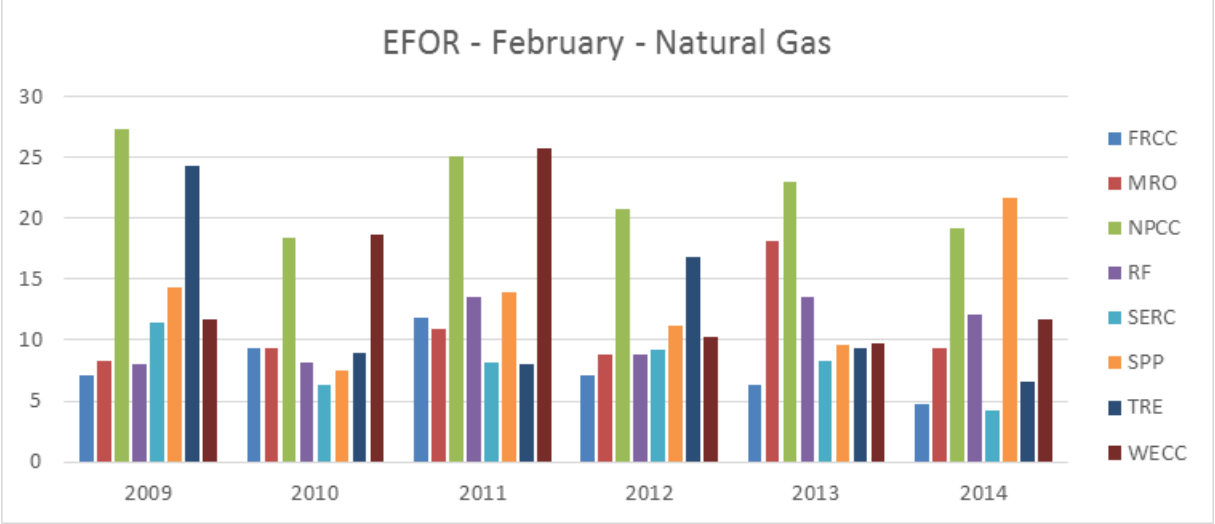


Figure A5: Historical EFOR for Natural Gas in February by Year and Regional Entity

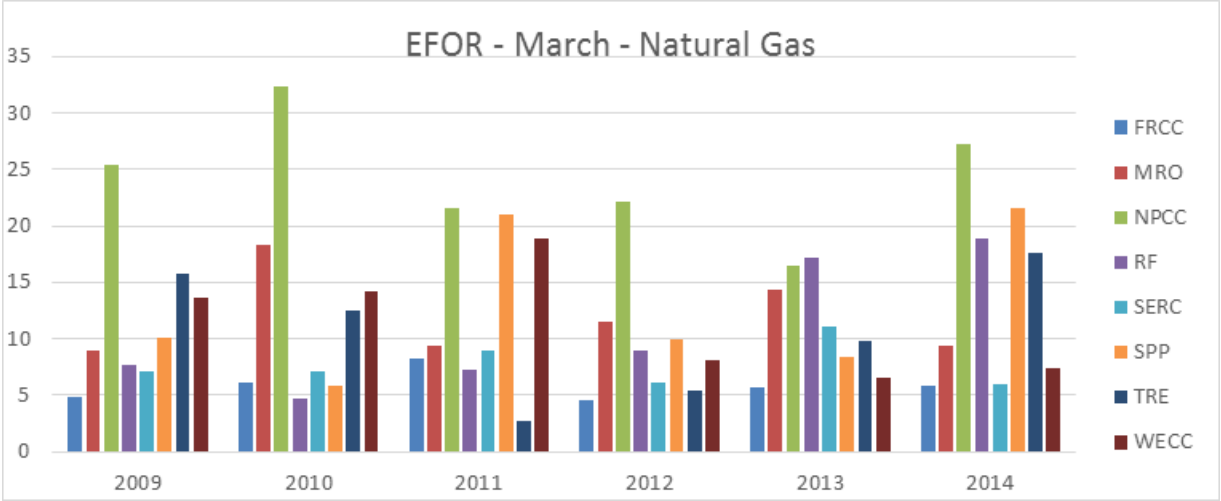


Figure A6: Historical EFOR for Natural Gas in March by Year and Regional Entity

Diesel Units

Figures A7, A8, and A9 provide historical EFOR for diesel units for January, February, and March by year and Regional Entity. Since participation in the GADS program is mandatory for all conventional units 20 MW and larger, many diesel units do not report to GADS. The comparative analysis, therefore, is of limited value and not provided.

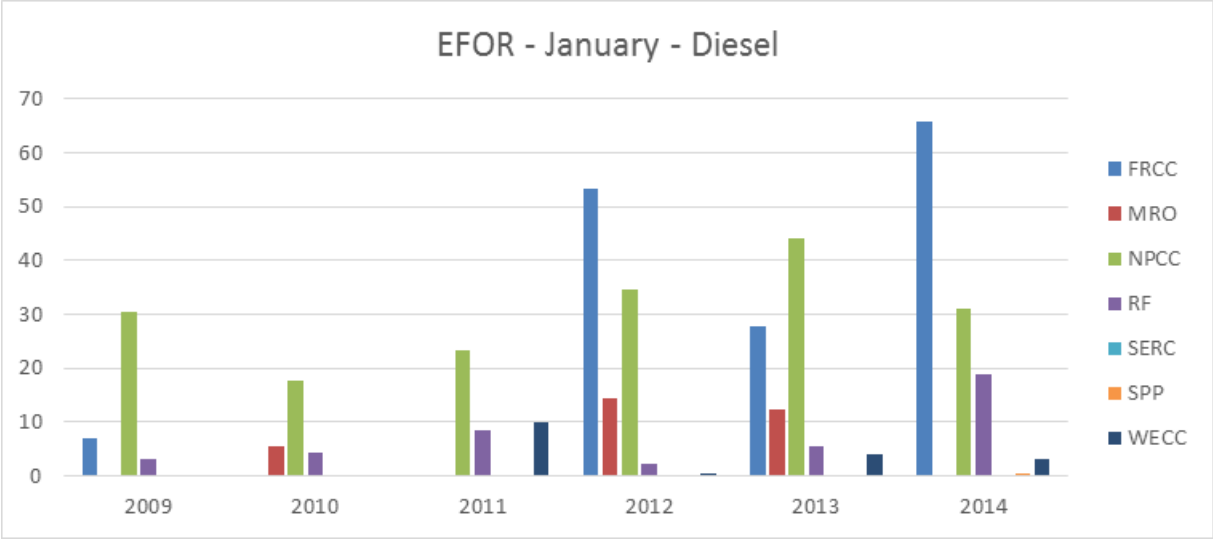


Figure A7: Historical EFOR for Diesel Units in January by Year and Regional Entity

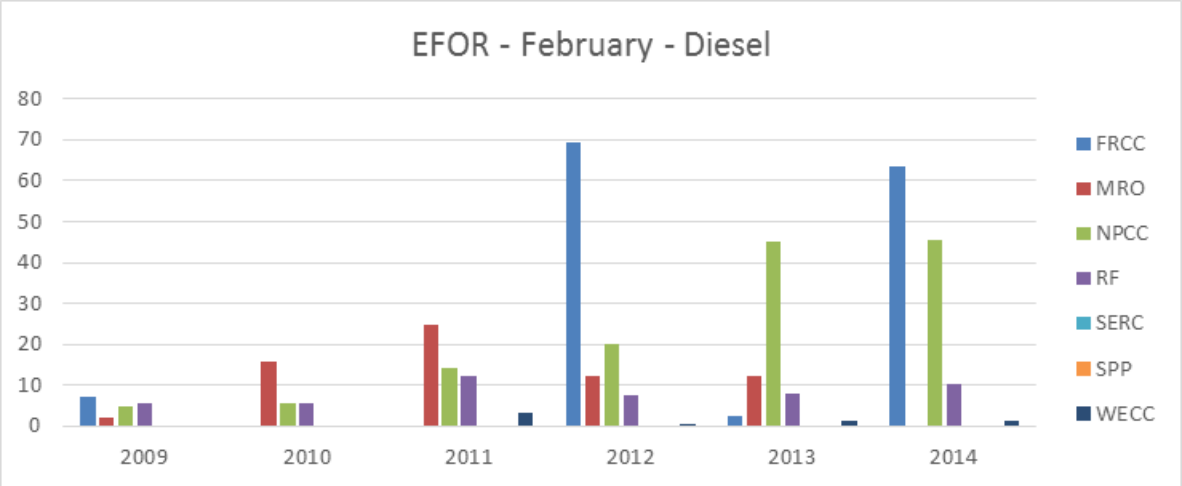


Figure A8: Historical EFOR for Diesel Units in February by Year and Regional Entity

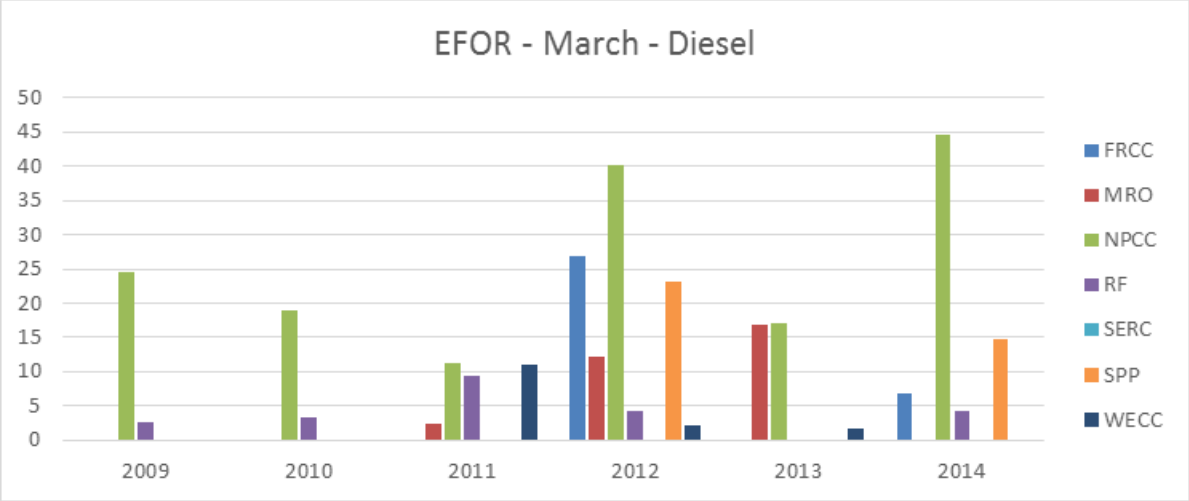


Figure A9: Historical EFOR for Diesel Units in March by Year and Regional Entity

Fluidized Bed Units

Figures A10, A11, and A12 provide historical EFOR for fluidized bed units for January, February, and March by year and Regional Entity. NPCC and SPP have no fluidized bed units reported in their Regions. In all other Regions examined, fluidized bed units experienced an EFOR in January 2014 within the range of expected EFOR based on the prior five winter operating periods.

The historical winter monthly EFOR performance of fluidized bed units in MRO ranged from 0.3 to 34.1 percent, and in January 2014 they experienced an EFOR of 3.2 percent. Fluidized bed units in RF experienced an EFOR of 0.1 percent in January 2014, compared with a historical range of zero to 22.6 percent (excluding the month of March 2013, which was an anomaly at 87.5 percent). The EFOR performance of fluidized bed units in SERC ranged from 0 to 25.4 percent, and in January 2014 they experienced an EFOR of 4.5 percent. Finally, fluidized bed units in TRE experienced an EFOR of 2.9 percent in January 2014, compared with a historical range of zero to 29.6 percent.

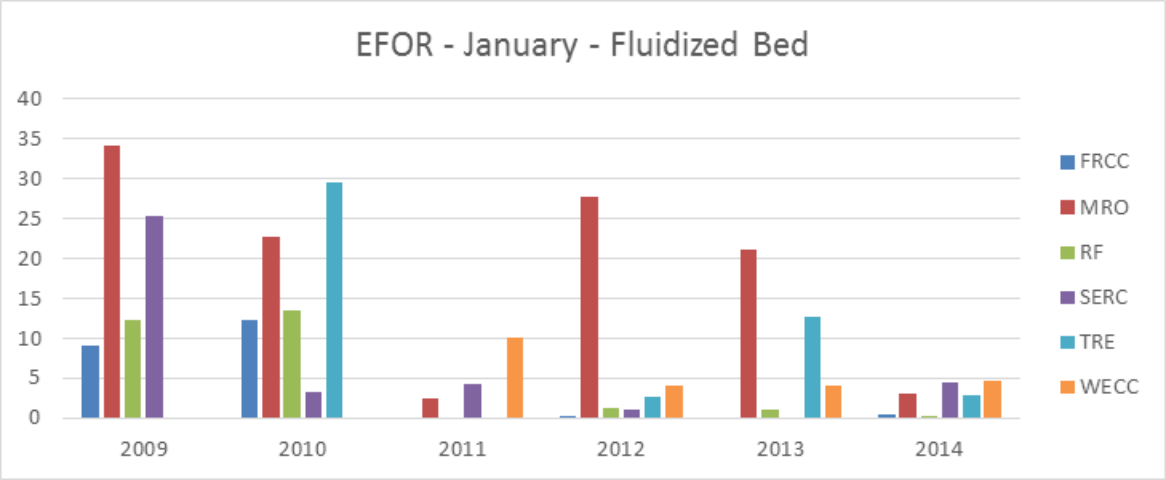


Figure A10: Historical EFOR for Fluidized Bed Units in January by Year and Regional Entity

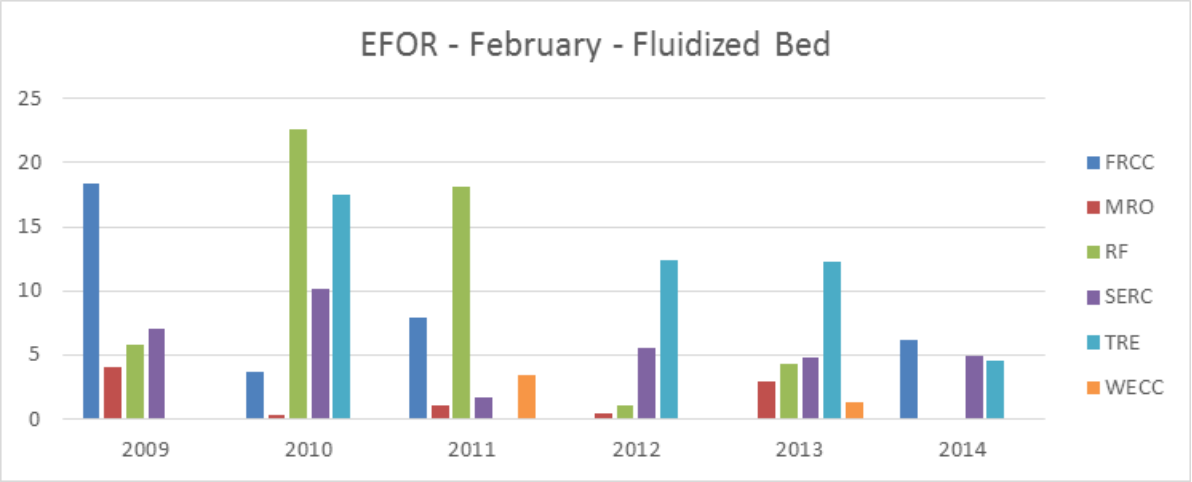


Figure A11: Historical EFOR for Fluidized Bed Units in February by Year and Regional Entity

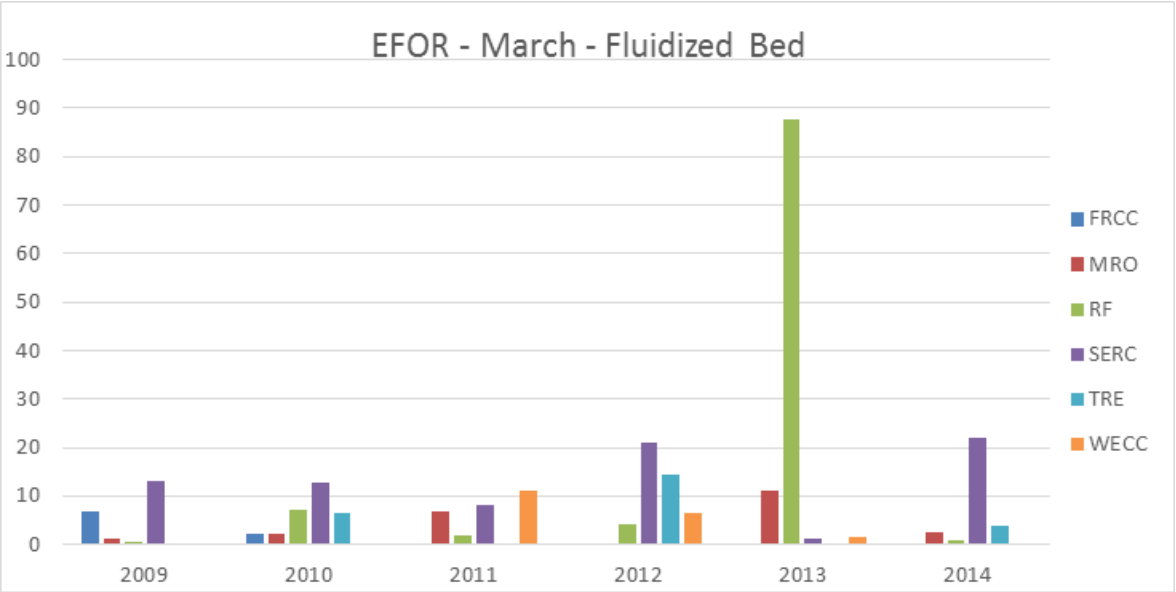


Figure A12: Historical EFOR for Fluidized Bed Units in March by Year and Regional Entity

Hydro/Pumped Storage

Figures A13, A14, and A15 provide historical EFOR for hydro and pumped storage for January, February, and March by year and Regional Entity. In all Regions examined, hydro and pumped storage experienced an EFOR in January 2014 within the range of expected EFOR based on the prior five winter operating periods.

The historical winter monthly EFOR performance of hydro and pumped storage in MRO ranged from 0.3 to 3.3 percent, and January 2014 they experienced an EFOR of 0.8 percent. In NPCC, the historical winter monthly EFOR performance ranged from 1.5 to 11 percent, and hydro and pumped storage experienced an EFOR of 0.3 percent in January 2014. Hydro and pumped storage in RF experienced an EFOR of 8.6 percent in January 2014, compared with a historical range of 0.9 to 10.4 percent. In SERC, hydro and pumped storage experienced an EFOR of 1.5 percent in January 2014, compared with a historical range of 1 to 9.7 percent. The EFOR performance of hydro and pumped storage in SPP ranged from zero to 12.7 percent, and January 2014 they experienced an EFOR of 0.4 percent. Finally, hydro and pumped storage in TRE experienced an EFOR of 0.5 percent in January 2014, compared with a historical range of zero to 21.5 percent.

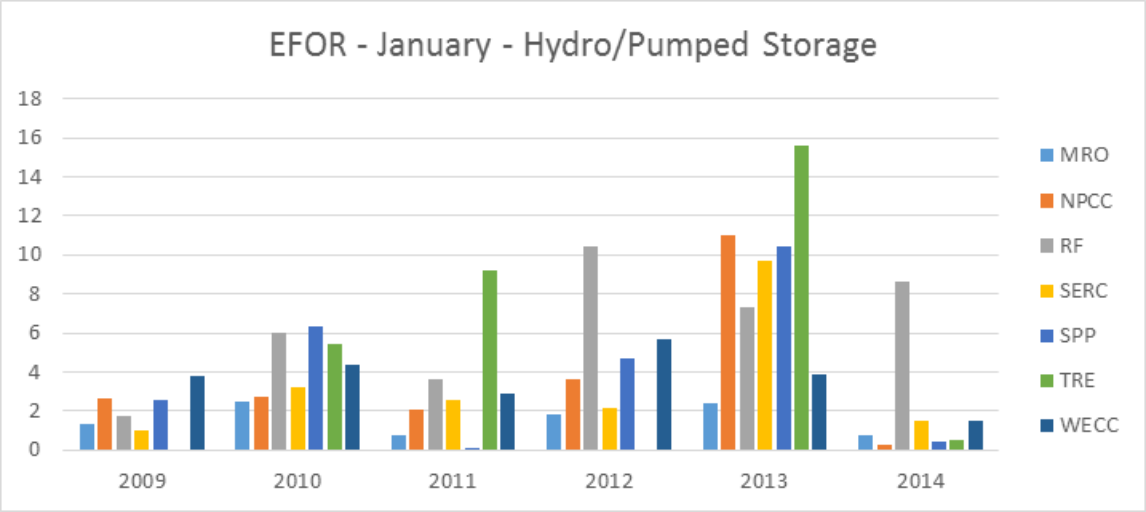


Figure A13: Historical EFOR for Hydro/Pumped Storage in January by Year and Regional Entity

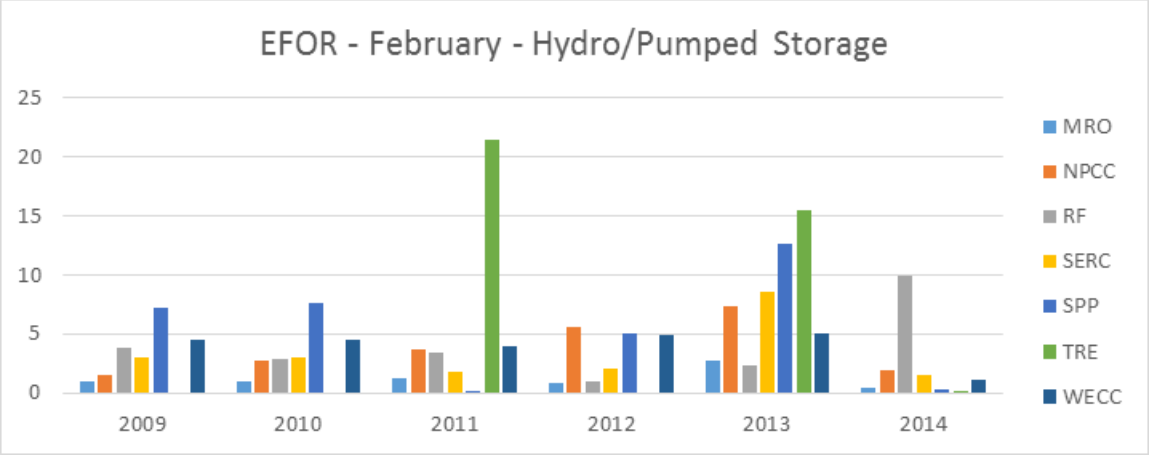


Figure A14: Historical EFOR for Hydro/Pumped Storage in February by Year and Regional Entity

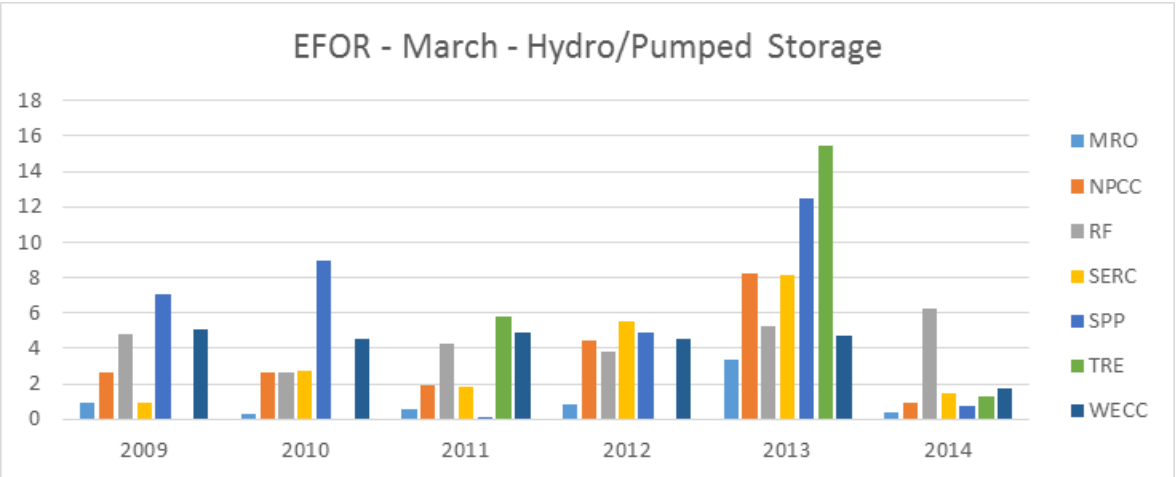


Figure A15: Historical EFOR for Hydro/Pumped Storage in March by Year and Regional Entity

Nuclear

Figures A16, A17, and A18 provide historical EFOR for nuclear units for January, February, and March by year and Regional Entity. In all other Regions examined, nuclear units experienced an EFOR in January 2014 within the range of expected EFOR based on the prior five winter operating periods.

The historical winter monthly EFOR performance of nuclear units in MRO ranged from 0 to 11.7 percent, and in January 2014 they experienced an EFOR of 10.3 percent. In NPCC, the historical winter monthly EFOR performance ranged from 0 to 7.2 percent, and nuclear units experienced an EFOR of 0.3 percent in January 2014. Nuclear units in RF experienced an EFOR of 0.03 percent in January 2014, compared with a historical range of 0.5 to 4.4 percent. In SERC, nuclear units experienced an EFOR of 1.8 percent in January 2014, compared with a historical range of 0 to 4.7 percent. The EFOR performance of nuclear units in SPP ranged from zero to 23.6 percent, and in January 2014 they experienced an EFOR of 0.0 percent. Finally, nuclear units in TRE experienced an EFOR of 3.9 percent in January 2014, compared with a historical range of zero to 26.4 percent.

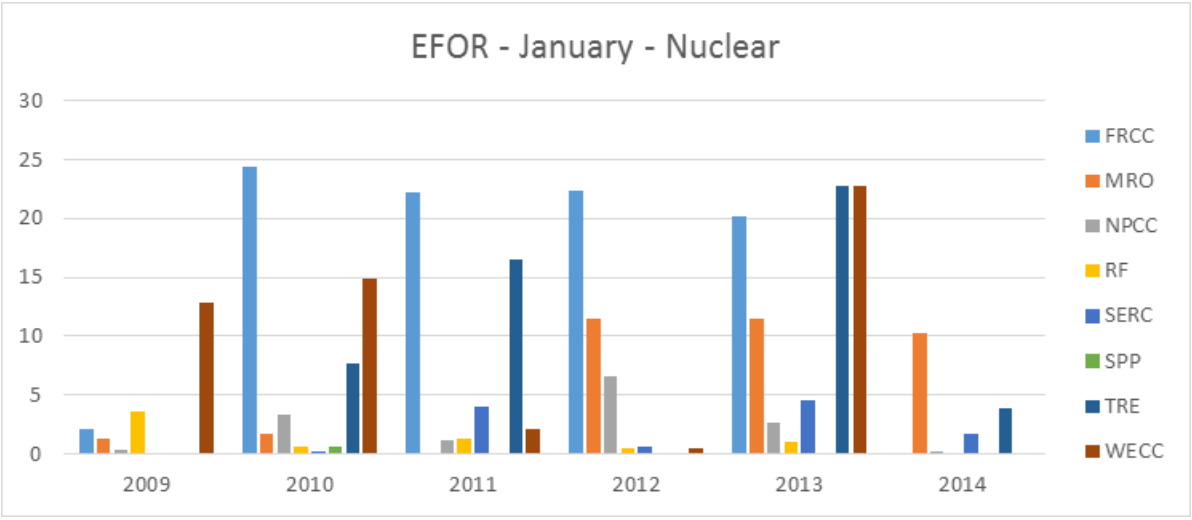


Figure A16: Historical EFOR for Nuclear Units in January by Year and Regional Entity

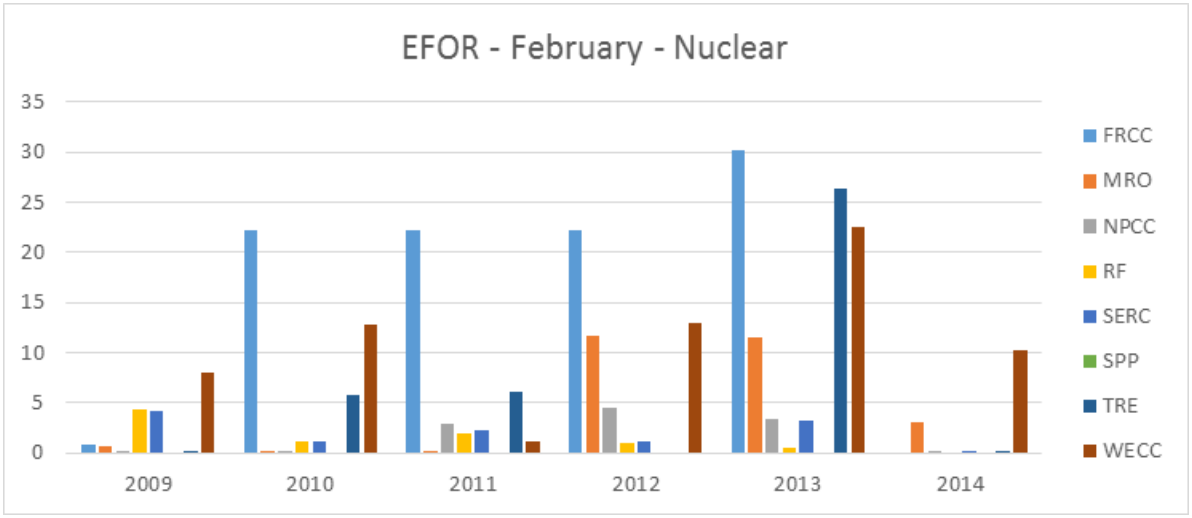


Figure A17: Historical EFOR for Nuclear Units in February by Year and Regional Entity

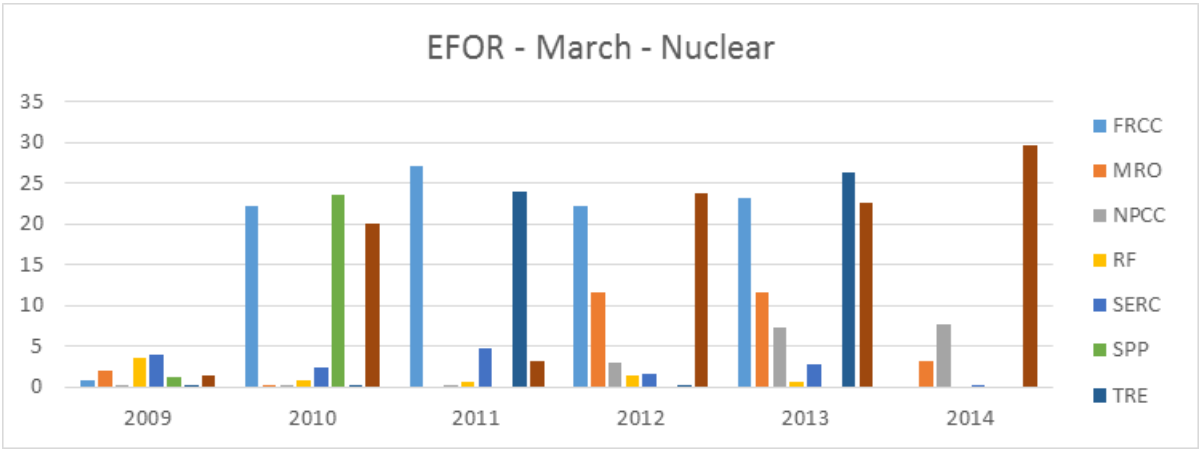


Figure A18: Historical EFOR for Nuclear Units in March by Year and Regional Entity

Other Units

Generation with other fuel types was considered for evaluation but is not included in this analysis. These units represent a small portion of power produced historically, and outage rates and MW produced vary from year to year. They also do not represent a significant portion of generation involved in the polar vortex analysis.

Summary

Most generation units, grouped by fuel type, performed in the expected range of EFOR, based on historical analysis. During the polar vortex, generation units could be expected to perform in the ranges provided in Table A1. Rows highlighted in yellow are for fuel types that experienced an EFOR greater than the previous high, and rows highlighted in light blue are for fuel types that experienced an EFOR less than the previous low. Overall, most units performed with an EFOR in the expected range, based on the past five years.

Table A1: EFOR Expected Range by Regional Entity and Fuel Type

		EFOR range - January to March			EFOR range - January only		
Region	**Fuel**	**Low**	**Jan-14**	**High**	**Low**	**Jan-14**	**High**
MRO							
	Coal	4.8	5.3	7.6	4.9	5.3	7.6
	Natural Gas	8.3	17.8	18.3	9	17.8	14.7
	Fluidized Bed	0.3	3.2	34.1	2.5	3.2	34.1
	Hydro	0.3	0.8	3.3	0.8	0.8	2.5
	Nuclear	0	10.3	11.7	0	10.3	11.5
NPCC							
	Coal	6.9	7.3	21.2	6.9	7.3	21.2
	Natural Gas	16.5	35.4	39.2	18.1	35.4	39.2
	Fluidized Bed	N/A	N/A	N/A	N/A	N/A	N/A
	Hydro	1.5	0.3	11	2	0.3	11
	Nuclear	0	0.3	7.2	0.3	0.3	6.7
RF							
	Coal	8.5	9.3	14.2	8.5	9.3	12.7
	Natural Gas	4.8	18.5	25.5	9.5	18.5	25.5
	Fluidized Bed	0	0.1	22.6	1.1	0.1	13.4
	Hydro	0.9	8.6	10.4	1.7	8.6	10.4
	Nuclear	0.5	0.03	4.4	0.5	0.03	3.6
SERC							
	Coal	5	4.9	10.2	6.3	4.9	10.2
	Natural Gas	6.3	11.4	11.4	8.1	11.4	10.3
	Fluidized Bed	0	4.5	25.4	0	4.5	25.4
	Hydro	1	1.5	9.7	1	1.5	9.7
	Nuclear	0	1.8	4.7	0	1.8	4.5
SPP							
	Coal	3.2	6.4	13.6	6.3	6.4	13.6
	Natural Gas	5.8	19.5	21.1	7	19.5	20.8
	Fluidized Bed	N/A	N/A	N/A	N/A	N/A	N/A
	Hydro	0	0.4	12.7	0	0.4	10.5

Table A1: EFOR Expected Range by Regional Entity and Fuel Type							
		EFOR range - January to March			EFOR range - January only		
Region	Fuel	Low	Jan-14	High	Low	Jan-14	High
	Nuclear	0	0	23.6	0	0	0.6
TRE							
	Coal	0	12.8	14.3	0	12.8	14.3
	Natural Gas	2.7	5.3	16.8	9.9	5.3	15.8
	Fluidized Bed	0	2.9	29.6	0	2.9	29.6
	Hydro	0	0.5	21.5	0	0.5	15.6
	Nuclear	0	3.9	26.4	0.1	3.9	22.7

Appendix B

Background on NERC's Long-Term Assessment of Increasing Dependency on Natural Gas

As of 2008, natural gas is the primary fuel source for on-peak capacity in North America. This trend is expected to continue with the addition of 40 GW of planned gas-fired capacity, accounting for nearly half of all capacity additions over the next decade. An additional 100 GW of gas-fired capacity is included in the generator queue and is not considered in Figure B-1 below.[12] By 2023, natural gas will contribute to well over 50 percent of the on-peak resource mix.

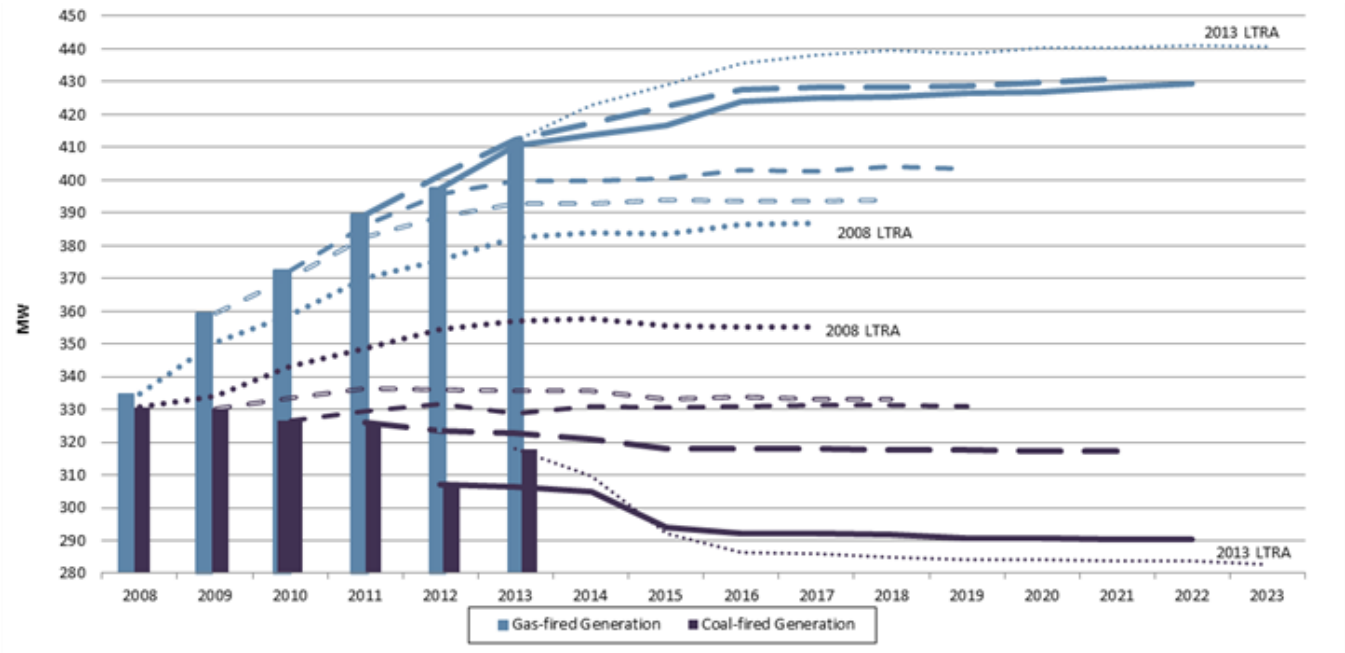


Figure B-1: Gas and Coal On-Peak Capacity: 10-Year Projected Outlook

This trend results from a variety of drivers that make natural-gas-fired capacity an attractive option for resource planners. First, the price of natural gas remains low, relative to other fuels, with abundant supplies due to new access to shale formations throughout North America. The emergence of natural gas combined cycle (NGCC) generating technology provides higher efficiency, and these units often require lower engineering, procurement, and construction costs. NGCC plants are oftentimes less challenging to procure because of shorter build times that might exist with other options. Perhaps the most impactful benefit is the lower carbon emissions when compared to coal-fired power plants without carbon capture and sequestration. Finally, natural-gas-fired units can provide System Operators with needed flexibility to address increased variability as additional renewable resources such as wind and photovoltaics are added to the system.

As the industry relies more on natural-gas-fired capacity to meet electricity needs, it is important to also examine potential risks associated with increased dependence on a single fuel type. The extent of these concerns varies from Region to Region. These concerns are most acute in areas where generators rely on interruptible natural gas pipeline transportation, and in times when the natural gas demand for power generation grows rapidly.

As highlighted in NERC's 2013 Special Assessment, *Accommodating an Increased Dependence on Natural Gas for Electric Power,*[13] a growing dependence on gas-fired generation can increase the BPS's exposure to disruptions from insufficient fuel supply, transportation, and delivery. While the likelihood is low and is largely correlated with

[12] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2013_LTRA_FINAL.pdf
[13] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf

extreme conditions, disruptions in natural gas supply and transportation to power generators have prompted industry to seek an understanding of the reliability implications associated with increasing gas-fired generation. With fleets of gas-fired generation being more prevalent across North America, common-mode failures are a significant risk for the electric industry.

Unlike coal and fuel oil, natural gas is not easily stored on site. As a result, real-time delivery of natural gas through a network of pipelines and bulk gas storage is critical to support electric generators. Natural gas is widely used outside the power sector, and the demand from other sectors—particularly coincident end-user gas peak demand during cold winter weather—critically affects the gas providers' ability to deliver interruptible transportation service in the power sector. Additionally, demand for natural gas is expected to grow in other sectors (e.g., transportation, exports, and manufacturing).

As observed during the polar vortex, increased reliance on natural gas exposed the industry to various challenges with fuel supply and delivery. These challenges are predicted to escalate as more baseload generating plants are retired. While baseload generators are replaced with renewables, they are generally not available at full rated capacity during extreme weather events and do not significantly contribute to capacity during these periods.

Historical GADS Analysis

NERC has been collecting GADS data since 1982. The NERC Board of Trustees approved mandatory GADS reporting for conventional generating units (excluding renewable generation such as wind and solar) starting January 1, 2012. GADS data was used to perform a historical analysis of natural gas generator outages.

Generators report fuel unavailability related outages to GADS under two different outage (cause) codes:

- **9130 Lack of fuel** (water from rivers or lakes, coal mines, gas lines, etc.) where the operator is not in control of contracts, supply lines, or delivery of fuels
- **9131 Lack of fuel** (interruptible supply of fuel part of fuel contract)

Outages related to lack of fuel are recorded regardless of a unit's dispatch. If the unit becomes unavailable due to fuel unavailability, the event is recorded as an outage in GADS even if the unit is not dispatched. GADS records outage start and end days and hours by Region, unit type, and utility.

Figure B-2 shows the trend of the total gas-fired unit outages reported within the last decade due to lack of fuel (code 9130 and 9131). There were 3,716 hours of cumulative generator outages in the first quarter of 2014, but there were over 80 GW of cumulative net dependable capacity lost. It should be noted that 2014 data only represents the first quarter.

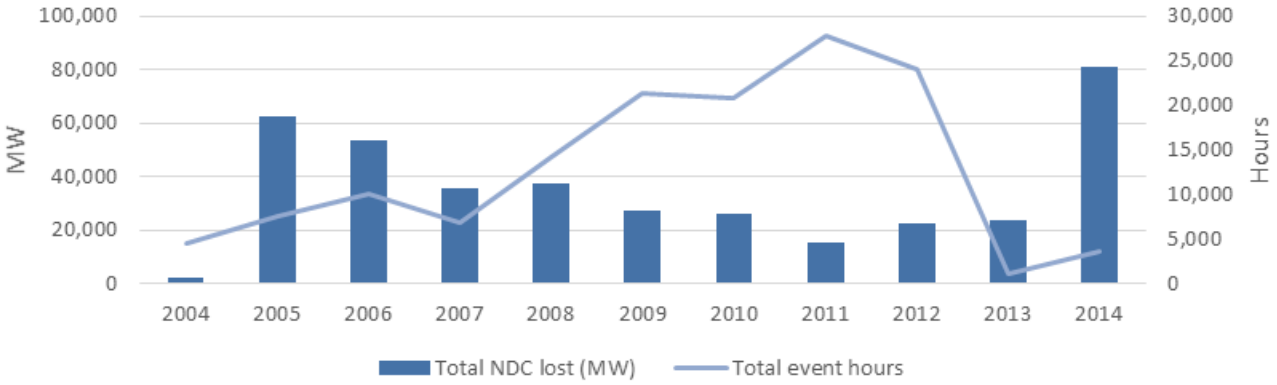


Figure B-2: Natural Gas Historical Outage Events Due to Lack of Fuel (2004–2014Q1)

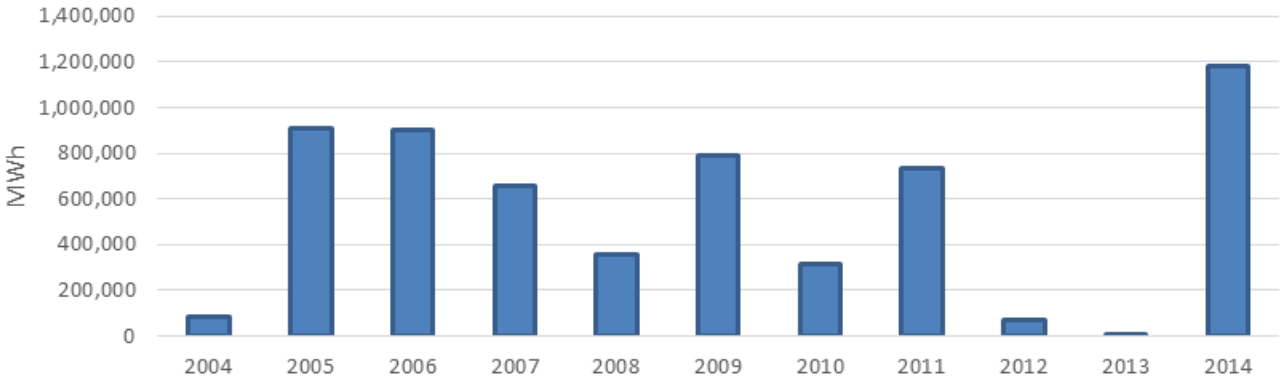


Figure B-3: Natural Gas Generation Historical Q1 and Q4 Energy Outages (MWh) Due to Lack of Fuel (2004–2014)

Plotting the number of events over time measures the trends outside of the normal event-count averages. Figure B-3 shows the total events reported by category. Values from 2014 increased the average to 363 events per year; meanwhile, the average for the last decade was around 296 events per year. The code U1 (Unplanned (forced) Outage – Immediate) accounts for 73 percent of the total events reported since 2004. Code U1 was reported 924 times (90 percent) in 2014 compared to 316 (64 percent) time in 2013. Again, there is a significant increase in 2014 (Q1).

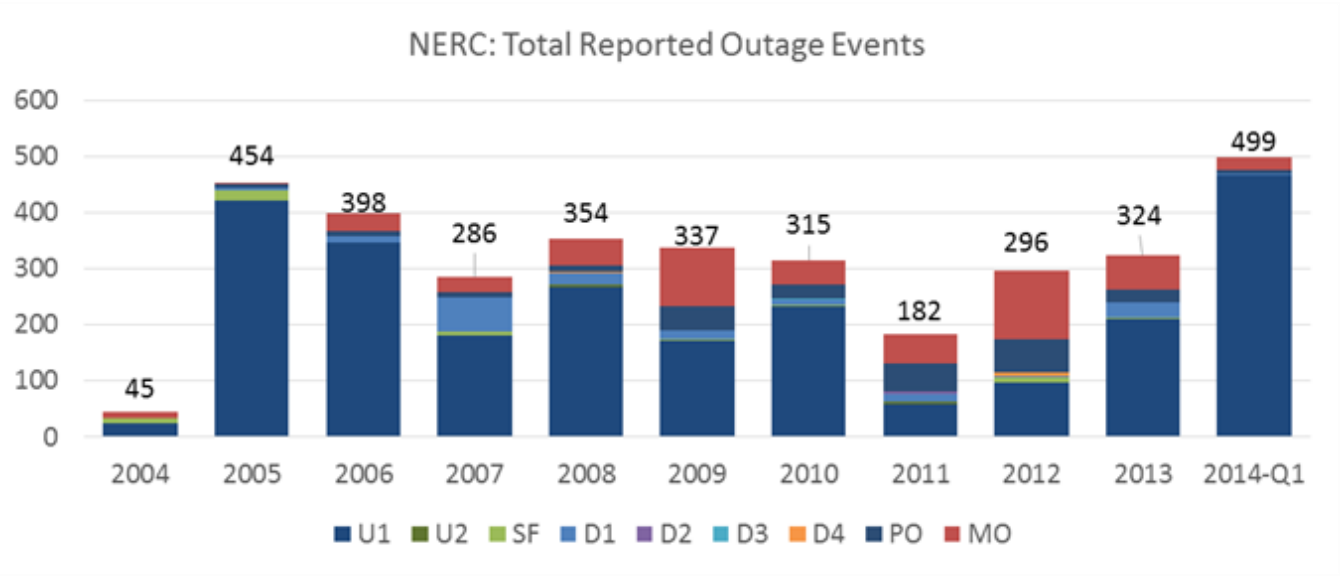


Figure B-4: Total Number of Outage Events Reported[14]

Event Type Codes Used	
Event Type	**Definition**
U1	Unplanned (Forced) Outage — Immediate - An outage that requires immediate removal of a unit from service, another Outage State, or a Reserve Shutdown state. This type of outage usually results from immediate mechanical/electrical/hydraulic control systems trips and operator-initiated trips in response to unit alarms.
U2	Unplanned (Forced) Outage — Delayed - An outage that does not require immediate removal of a unit from the in-service state but requires removal within six hours. This type of outage can only occur while the unit is in service.

[14] More information on GADS and GADS code used are available at GADS Event Reporting

Event Type Codes Used	
Event Type	**Definition**
SF	Start-up Failure - An outage that results when a unit is unable to synchronize within a specified start-up time following an outage or Reserve Shutdown.
D1	Unplanned (Forced) Derating — Immediate - A derating that requires an immediate reduction in capacity.
D2	Unplanned (Forced) Derating — Delayed - A derating that does not require an immediate reduction in capacity but requires a reduction within six hours.
D3	Unplanned (Forced) Derating — Postponed - A derating that can be postponed beyond six hours but requires a reduction in capacity before the end of the next weekend.
D4	Maintenance Derating - A derating that can be deferred beyond the end of the next weekend (Sunday at 2400 or before Sunday turns into Monday) but requires a reduction in capacity before the next Planned Outage (PO). A D4 can have a flexible start date and may or may not have a predetermined duration.
PO	Planned Outage - An outage that is scheduled well in advance that is of a predetermined duration, lasts for several weeks, and occurs only once or twice a year. Turbine and boiler overhauls or inspections, testing, and nuclear refueling are typical Planned Outages.
MO	Maintenance Outage - An outage that can be deferred beyond the end of the next weekend (defined as Sunday at 2400 hours or as Sunday turns into Monday), but requires that the unit be removed from service, another outage state, or Reserve Shutdown state before the next Planned Outage (PO). Characteristically, an MO can occur any time during the year, has a flexible start date, may or may not have a predetermined duration, and is usually much shorter than a PO.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Tilden Mining Company L.C. and Empire Iron Mining Partnership (Complainants)	)	**Docket No. EL14-103-000**
v.	)	
Midcontinent Independent System Operator, Inc., and Wisconsin Electric Power Company (Respondents).	)	

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 212 and 214 of the Federal Energy Regulatory Commission's (the "Commission" or "FERC") Rules of Practice and Procedure, 18 C.F.R. §§ 385.212 and 385.214, the North American Electric Reliability Corporation ("NERC") moves to intervene and comment on the Complaint filed by Tilden Mining Company L.C. and Empire Iron Mining Partnership (collectively "the Mines") on September 19, 2014 in the above-referenced docket ("Complaint").

The Complaint against Midcontinent Independent System Operator, Inc. ("MISO") and the Wisconsin Electric Power Company ("WEPCo"), mischaracterizes NERC's action in the review and subsequent certification of WEPCo's proposed Michigan Upper Peninsula Balancing Authority ("MIUP BA"). The Mines assert that the split of WEPCo's BA[1] and establishment of the MIUP BA will result in a significant shift in the allocation of System Support Resource ("SSR") costs under the MISO tariff. The Mines are seeking Commission action to ensure that the SSR rates charged pursuant to MISO's Tariff are just and reasonable under the unique

[1] Under the MISO tariff, Balancing Authorities are referred to as local Balancing Authorities or LBAs. For the purposes of this filing, NERC is using the terms interchangeably.

circumstances of this case. While NERC is not a named party in the Complaint, NERC requests leave to intervene and comment in response to the improper representation of NERC's action set forth therein.

I. 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, N.E.
Suite 600, North Tower
Atlanta, G.A. 30326
(404) 446-2560
(404) 446-2595 – facsimile

* Persons to be included on the Commission's official service list.

Charles A. Berardesco*
Senior Vice President and General Counsel
Meredith M. Jolivert*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
meredith.jolivert@nerc.net

II. MOTION TO INTERVENE

NERC has a substantial interest in this proceeding as it is a party to a complaint pending before FERC on a related matter[2] and to correct the record regarding NERC's certification of the MIUP BA. The Commission certified NERC as the Electric Reliability Organization ("ERO") for the purpose of establishing and enforcing Reliability Standards for the Bulk Power System ("BPS") in the United States.[3] As the ERO, NERC's mission is to improve the reliability and security of the BPS in North America.[4] Under its FERC-approved Rules of Procedure, NERC certifies entities such as BAs to ensure that a newly operating entity "(*i.e.*, an applicant [seeking]

[2] *See Michigan Pub. Serv. Comm'n. v. No. American Elec. Reliability Corp. and Wisconsin Elec. Power Co.*, Docket No. EL14-104-000.
[3] *North American Electric Reliability Council, Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").
[4] *See Id.*

to be an RC, BA, or TOP that is not already performing the function for which it is applying to be certified as) has the tools, processes, training, and procedures," to meet the "Requirements/sub-Requirements of all Reliability Standards applicable to the function(s) for which it is applying."[5]

While the Mines acknowledge that issues related to the allocation of SSR costs are outside of NERC's purview, the Mines accuse NERC of being an unwitting participant to WEPCo's scheme to shift the allocation of SSR costs under MISO's Tariff between customers in Wisconsin and those in the Upper Peninsula of Michigan. No other party can adequately represent NERC's interests or adequately respond to the Mines' improper representation of NERC's action. Therefore, it is in the public interest to permit this intervention.

III. COMMENTS

Despite NERC's efforts to advise the Mines of the FERC-approved rules governing the certification of BAs, the Mines continue to misrepresent NERC's action as "approving WEPCo's proposal."[6] NERC did not approve WEPCo's proposal; NERC only certified WEPCo's proposed MIUP BA in accordance with its FERC-approved Rules of Procedure ("ROP") and, in its review of that certification, evaluated the competency of WEPCo to reliably operate the BA. NERC advised the Mines of its jurisdiction before the Mines filed the instant complaint with FERC.[7] NERC's role in the certification process is to ensure that entities are technically capable of performing their functions so as to better ensure grid reliability; issues such as cost allocation are not relevant to that determination and are beyond the scope of NERC's jurisdiction.

[5] *See* ROP § 501.
[6] *See* Complaint at 2.
[7] *See* NERC's August 29, 2014 Letter to W. Demarest (The Mines counsel), Complaint at Exhibit L.

In addition to improperly describing NERC's action as approving the WEPCo proposal, the Mines allege that NERC does not have jurisdiction to certify the MIUP BA. The Mines assert that "[a]s a cost-shifting mechanism rather than a reliability enhancement, the cost allocation consequences of the split of the WEC LBA and formation of the MIUP LBA fall outside NERC's purview."[8] NERC does not dispute FERC's jurisdiction over the cost allocation issues that flow from MISO's tariff and the calculation of SSR costs; however, the certification of the newly formed MIUP BA falls squarely within NERC's jurisdiction. NERC's certification process is governed by the FERC-approved ROP and is tied to registration on the NERC Compliance Registry and not, as the Mines assert, tied to reliability enhancements.

The NERC certification process flows from NERC's obligation to "clearly identify those entities that are responsible for compliance with the FERC approved Reliability Standards."[9] Under the FERC-approved ROP, for all geographical or electrical areas of the BPS, NERC is to register entities on the NERC Compliance Registry to ensure that: (i) no areas are lacking any entities to perform the duties and tasks identified in and required by NERC's Reliability Standards to the fullest extent practical; and (ii) there is no unnecessary duplication of such coverage or of required oversight of such coverage.[10] In addition to NERC's registration requirements as outlined above, NERC is to certify all entities such as BAs with primary reliability responsibilities.[11] NERC's certification review evaluates the competency of a registered entity to perform the evaluated functions.[12] The proper scope of NERC's review is not to ensure that the proposed BA remedies any physical reliability issues; rather, NERC's

[8] *See* Complaint at 13 (*internal quotation marks omitted).*
[9] *See* ROP at § 501.
[10] *See* ROP at § 501.1.4; *see also* § 501.1.4.2 *et seq.*
[11] *See* ROP at § 502.
[12] *See* ROP §§ 501.2–501.2.5 (specifying the criteria NERC is to use before issuing certification of a new BA).

certification review is designed to assure that the proposed BA does not create any reliability issues.

IV. CONCLUSION

WHEREFORE, NERC respectfully requests that the Commission grant this motion for leave to intervene and accept the comments herein.

Respectfully submitted,
/s/ Meredith M. Jolivert

Charles A. Berardesco
Senior Vice President and General Counsel
Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
meredith.jolivert@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: October 9, 2014

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 9th day of October, 2014.

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Counsel for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Michigan Public Service Commission	)	
	)	
Complainant,	)	
v.	)	**Docket No. EL14-104-000**
	)	
North American Electric Reliability Corporation, and	)	
	)	
Wisconsin Electric Power Company	)	
	)	
Respondents.	)	

THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION'S ANSWER TO THE MICHIGAN PUBLIC SERVICE COMMISSION'S COMPLAINT

Pursuant to Rules 206(f) and 213 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure[1] and the Commission's "Notice of Complaint" issued on September 22, 2014, the North American Electric Reliability Corporation ("NERC") hereby submits this Answer to the Complaint filed by the Michigan Public Service Commission ("MPSC") in the above-captioned docket ("the Complaint"). MPSC seeks an order from the Commission that reverses NERC's certification outlined in the August 28, 2014 Balancing Certification Final Report ("Certification")[2] issued by ReliabilityFirst ("RF"). MPSC alleges, among other things, that NERC's August 28 Certification approved Wisconsin Electric Power Company's ("WEPCo") proposal to split its existing WEC Balancing Authority ("BA") footprint into two BAs - the new Michigan Upper Peninsula ("MIUP") BA and the WEC BA. MPSC further argues NERC's approval of the new BA could result in an unjust and

[1] *See* 18 C.F.R. §§ 385.206(f) and 385.213 (2013).
[2] *See* Complaint at Exhibit MI-1.

unreasonable change in the allocation of System Support Resource ("SSR") costs. As discussed in greater detail below, MPSC's Complaint should be dismissed given that it mischaracterizes NERC's action in the certification of WEPCo's proposed MIUP BA, and as a result, seeks an improper form of relief.

I. SUMMARY OF MPSC'S COMPLAINT AND EXECUTIVE SUMMARY OF NERC'S ANSWER

A. SUMMARY OF MPSC'S COMPLAINT

At the core of the MPSC Complaint are the following three allegations:[3]

1) The administrative decision-making process before ReliabilityFirst was procedurally defective, and denied affected parties an opportunity to be heard and to present evidence regarding the impact of WEPCo's proposal upon ratepayers of affected Load Serving Entities ("LSEs");

2) NERC failed to address evidence that WEPCo's proposed split of its BA between the portion covering Wisconsin and the portion covering the Michigan Upper Peninsula, either intentionally or coincidentally, could result in a dramatic and unjust and unreasonable change in the allocation of SSR costs recently approved by the Commission in its July 29 Order; and

3) There is a lack of substantial evidence supporting any finding that the requested split is needed to address any physical reliability issues.

MPSC argues that for these reasons, NERC's Certification of the MIUP BA should be reversed. In the alternative, MPSC requests that the Commission make clear that NERC's approval will not have any impact upon the allocation of SSR costs that would otherwise occur under the Midcontinent Independent System Operator ("MISO") Tariff and the related MISO Business Practice Manual. MPSC argues that without the requested reversal or clarification, NERC's approval could "impose dramatic and unreasonable shifts in the allocation of SSR costs without providing any opportunity or forum for affected parties to be heard and present evidence

[3] Complaint at 4–5.

concerning the impact of proposed changes to BA boundaries upon areas potentially outside of NERC's purview, such as cost allocation."[4]

B. EXECUTIVE SUMMARY OF NERC'S ANSWER

In response to MPSC's Complaint, NERC asserts the following:

1) The administrative decision-making process before RF was not procedurally defective. NERC complied with its FERC-approved Rules of Procedure ("ROP) in certifying the MIUP BA.

2) NERC was not obligated to address evidence that the proposed split of WEPCo's BA could result in a change in the allocation of SSR costs. Issues related to costs such as the SSR allocation are beyond the scope of NERC's jurisdiction.

3) NERC's Certification review was properly scoped to evaluate whether the proposed split of the WEC BA would cause reliability concerns. The proper scope of NERC's review is not to ensure that the proposed BA remedies any physical reliability issues; rather, NERC's certification review is designed to ensure that the proposed BA does not create any reliability issues.

As a threshold matter, MPSC's Complaint fails to meet even the minimal requirements set forth in Rule 206 of the Commission's Rules of Practice and Procedure.[5] The Complaint does not "clearly identify the action or inaction which is alleged to violate applicable statutory or regulatory requirements" and does not "explain how the action or inaction violates applicable statutory standards or regulatory requirements."[6] Instead, the Complaint requests the Commission's reversal of NERC's Certification for failure to consider evidence that NERC has no jurisdiction to consider. MPSC's Complaint should be dismissed and evidence relating to the allocation of SSR costs, the underlying cause of MPSC's concern, should be evaluated by the only entity with the requisite jurisdiction—FERC.

[4] Complaint at 2.
[5] 18 C.F.R. § 385.206(b).
[6] *Id*. at (b)(1) and (b)(2).

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, N.E.
Suite 600, North Tower
Atlanta, G.A. 30326
(404) 446-2560
(404) 446-2595 – facsimile

* Persons to be included on the Commission's official service list.

Charles A. Berardesco*
Senior Vice President and General Counsel
Meredith M. Jolivert*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
meredith.jolivert@nerc.net

III. ANSWER

A. NERC'S CERTIFICATION OF THE MIUP BA WAS NOT PROCEDURALLY DEFECTIVE

NERC's certification of the MIUP BA was done in full accordance with the FERC-approved ROP. The certification review was not procedurally defective and any claims to the contrary demonstrate a fundamental misunderstanding of NERC's processes. The ROP clearly sets forth the process for registration and certification of a BA. Under the ROP, the purpose of NERC's Certification program is to ensure that a "new entity (*i.e.*, an applicant seeking to be an RC, BA, or TOP that is not already performing the function for which it is applying to be certified as) has the tools, processes, training, and procedures," demonstrating its ability to meet the "Requirements/sub-Requirements of all of the Reliability Standards applicable to the function(s) for which it is applying," demonstrating that it is qualified for certification and operation.[7]

[7] *See* ROP § 501.

The registration and certification process requires NERC to ensure that all geographical or electrical areas of the Bulk Power System ("BPS"): (i) do not lack any entity to perform the duties and tasks identified in and required by NERC's Reliability Standards to the fullest extent practical; and (ii) that there is no unnecessary duplication of such coverage or of required oversight of such coverage.[8] NERC evaluates each proposed BA under specific criteria articulated in the ROP. In doing so, NERC is to: (i) ensure an applicant's ability to meet certification requirements; (ii) document the certification process; (iii) maintain records of currently certified entities; and (iv) issue a Certification document to an applicant that successfully demonstrates its competency to perform the evaluated functions.[9] NERC made each of the relevant determinations required by the ROP.

Contrary to MPSC's allegations otherwise, NERC is not required to entertain comments or evidence from stakeholders. NERC's evaluation is limited to a technical evaluation of the entity's operational capabilities and ability to meet NERC's Reliability Standards. NERC conducted an in-depth review of WEPCo's capacity to reliably operate the MIUP BA. Specifically, NERC's evaluation included: (i) interviewing MIUP's management and reviewing pertinent documentation to verify necessary requirements for BA operation; (ii) reviewing procedures and other documentation developed by MIUP to meet applicable standards and requirements; (iii) interviewing MIUP system operations personnel; (iv) reviewing MIUP's Energy Management System, communication facilities, operator displays, etc., to assess its capabilities; (v) performing other validation review as necessary; and (vi) conducting an in-person site check on August 12, 2014 through August 13, 2014.[10] NERC's evaluation confirmed

[8] *See Id.* at § 501.1.4.; *see also* § 501.1.4.2 *et seq.*
[9] *See* ROP §§ 501.2–501.2.5 (specifying the criteria NERC must use before issuing certification of a new BA).
[10] *See* Complaint at Exhibit MI-1.

WEPCo's competency to operate the MIUP BA reliably and thus NERC issued its Certification report on August 28, 2014.

B. MPSC MISCHARACTERIZED NERC'S ACTION: NERC CERTIFIED THE MIUP BA, NERC DID NOT APPROVE WEPCO'S PROPOSAL

Despite NERC's efforts to inform the MPSC of its process and responsibilities, the MPSC has repeatedly failed to recognize NERC's limited and narrowly scoped certification process. Instead, the MPSC continues to assert that NERC approved WEPCo's proposal to create a new BA. NERC did not approve any such proposal, and advised the MPSC of that fact[11] before MPSC filed its Complaint with FERC. NERC only certified WEPCo's proposed MIUP BA and, in its review of that Certification, evaluated the competency of WEPCo to reliably operate the BA.[12] NERC's role in the certification process is to ensure that entities are technically capable of performing their functions so as to better ensure grid reliability; issues such as cost allocation are not relevant to that determination and are beyond the scope of NERC's jurisdiction. In fact, under the ROP, cost allocation is not among the factors NERC is to consider as part of its registration or certification program.[13]

MPSC's concerns about cost allocation issues relate to tariff revisions proposed by the MISO that are currently before the Commission in a separate proceeding.[14] Pursuant to Section 205(a) of the FPA, the Commission has exclusive jurisdiction over all rules that affect or pertain to rates and charges received by any public utility for or in connection with the transmission and sale of electric energy. MISO's tariff and the related allocation of SSR rates falls squarely in the

[11] *See, inter alia*, NERC's August 29, 2014 Letter to the Michigan Public Service Commission, Attachment L to the Complaint.
[12] *See Id.*
[13] *See* ROP § 500 (governing NERC's registration and certification process for BAs); *see also* Appendices 5A and 5B of the ROP (providing the criteria evaluated and guidance for evaluation in NERC's certification process).
[14] *See, inter alia*, Docket Nos. ER14-1242 and ER14-1243 (In a January 31, 2014 filing, MISO proposed a *pro rata* allocation of SSR costs associated with the Presque Isle generators to all LSEs of the ATC LLC footprint).

Commission's jurisdiction. Therefore, NERC does not have the jurisdiction or ability to evaluate evidence relating to these issues as they are entirely within the Commission's purview.

NERC's Certification of the MIUP BA should not be improperly expanded to provide the MPSC with another attempt to change the Commission's ruling on SSR costs. MPSC has had the opportunity to comment on MISO's tariff restructuring before FERC,[15] and NERC's certification process is not meant to address these issues.

C. NERC's certification review was properly scoped to evaluate whether the proposed split of the WEC BA would cause reliability concerns.

The proper scope of NERC's review is not to ensure that the proposed BA remedies any physical reliability issues; rather, NERC's certification review is designed to assure that the proposed BA does not create any reliability issues. On February 17, 2014, WEPCo submitted an Entity Certification form to RF for certification and registration of the MIUP BA. In its request, WEPCo provided all required documentation including a reliability proposal, procedures, and list of personnel needed for NERC to evaluate and determine whether the MIUP BA would cause any reliability concerns.[16] NERC's primary objective for conducting its certification review is to ensure that the MIUP BA can competently fulfill its responsibilities as a BA and comply with NERC's Reliability Standards (*i.e.* the MIUP BA will not affect reliability in the region).[17] NERC met its responsibility in the evaluation of the MIUP BA and subsequent determination that it has the technical ability to act as a BA. That is the limited, technical role that NERC plays in this process, despite MPSC's protestations to the contrary.

[15] *See Id.*
[16] *See* ROP § 501 (requiring any utility seeking registration to provide proper documentation demonstrating its ability to satisfactorily function as a BA); *see also* Complaint at Exhibit MI-1.
[17] *Id.*

IV. CONCLUSION

WHEREFORE, NERC respectfully requests that the Commission deny the relief sought by MPSC and uphold NERC's certification of the MIUP BA.

Respectfully submitted,

/s/ Meredith M. Jolivert

Charles A. Berardesco
Senior Vice President and General Counsel
Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
meredith.jolivert@nerc.net

Counsel for North American Electric Reliability Corporation

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a copy of this document upon all parties listed on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Washington, D.C. this 9th day of October, 2014.

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Counsel for North American
Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability	**)**	
Corporation	**)**	**Docket No. FA11-21-000**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC")[1] submits this compliance filing in accordance with the Commission's January 16, 2013 Order in Docket No. FA11-21-000.[2] In the January 16 Order, the Commission approved a Settlement Agreement between the Office of Enforcement ("Enforcement") and NERC related to Enforcement's findings and recommendations arising out of its 2012 performance audit of NERC. Specifically, Section II.7(b)(i) of the Settlement Agreement requires that:

> Within forty-five days of the end of each quarter, beginning with the quarter ending March 31, 2013, NERC will file with the Commission the unaudited report of the NERC budget-to-actual spending variances during the preceding quarter. This report will include information regarding sources and uses of operating and working capital reserves and will match or exceed the level of detail of the quarterly budget-to-actual variance report of NERC expenditures attached to the agenda of NERC Board of Trustees Finance and Audit Committee's October 2012 meeting.[3]

Attached hereto is the unaudited report of NERC's budget-to-actual variance information for the third quarter of 2014, in accordance with the January 16 Order. This variance information was

---

[1] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] *See North American Electric Reliability Corporation, Order Approving Settlement Agreement*, 142 FERC ¶ 61,042 (2013) ("January 16 Order").

[3] *Id.*

posted on NERC's website and reviewed in open session at the November 6, 2014 conference call of the NERC Finance and Audit Committee. The unaudited report was accepted by the NERC Board of Trustees at its meeting on November 13, 2014.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:[4]

Michael Walker*
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-9740
(404) 467-0474 – facsimile

Meredith M. Jolivert*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
meredith.jolivert@nerc.net

*Persons to be included on the Commission's official service list

[4] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2012), to allow the inclusion of more than two persons on the service list in this proceeding.

II. CONCLUSION

NERC respectfully requests that the Commission accept this filing as compliant with Section II.7(b)(i) of the Settlement Agreement and the Commission's January 16 Order in Docket No. FA11-21-000.

Respectfully submitted,

/s/ Meredith M. Jolivert

Michael Walker
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-9740
(404) 467-0474 – facsimile

Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
meredith.jolivert@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: November 14, 2014

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 14th day of November, 2014.

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Counsel for North American
Electric Reliability Corporation

ATTACHMENT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Electric Reliability Corporation- Review of September 30, 2014 Unaudited Results – Budget to Actual Variance Analysis

Summary of Results as of September 30, 2014

The Total Budget for expenses plus fixed asset purchases was under budget $4.1M, 9.6%, through September 30, 2014, which is generally consistent with June 30th results, which were $2.9M, 10.0%, under budget. With the exception of rent expense and professional services, all expense categories were under budget.

SEPTEMBER YTD ACTUAL VERSUS BUDGET BY CATEGORY COMPARED TO JUNE YTD

	As of September 30, 2014				Results through June 30, 2014		
	2014 YTD Actual	2014 YTD Budget	2014 YTD Variance Over(Under)	%	Variance Over/(Under)		Change in Variance Compare September to June
TOTAL FUNDING	**40,309,534**	**40,326,786**	**(17,253)**	**0.0%**	**(83,510)**	**-0.3%**	**66,258**
BUDGET - EXPENSES and FIXED ASSETS							
PERSONNEL EXPENSES	24,754,205	25,675,186	(920,983)	-3.6%	(445,147)	-2.6%	(475,836)
MEETINGS, TRAVEL and CONFERENCE CALLS	2,666,057	2,792,895	(126,839)	-4.5%	(114,860)	-6.1%	(11,979)
CONSULTANTS and CONTRACTS	4,226,724	5,431,535	(1,204,811)	-22.2%	(994,544)	-26.8%	(210,267)
RENT	1,978,560	1,962,974	15,586	0.8%	593	0.0%	14,993
OFFICE COSTS, PROFESSIONAL SERVICES and MISCELLANEOUS	4,398,026	4,337,865	60,161	1.4%	(79,932)	-2.7%	140,093
Other Non-Operating Expenses	84,770	108,000	(23,230)	-21.5%	(57,482)	-79.8%	34,252
FIXED ASSET PURCHASES (excludes the credit for depreciation)	459,647	2,338,343	(1,878,695)	-80.3%	(1,184,078)	-76.0%	(694,617)
TOTAL BUDGET	**38,567,989**	**42,646,798**	**(4,078,811)**	**-9.6%**	**(2,875,449)**	**-10.0%**	**(1,203,362)**
FTEs	**179.16**	**189.53**	**(10.37)**	**-5.5%**	**(12.17)**	**-6.4%**	**1.80**

As reflected in the following table, we project to be approximately $2.4M under budget at the end of the year, compared to the June 30, 2014 year-end projection of $944.7k under budget, which was utilized in preparation the final 2015 business plan and budget. The change in the year-end projection is primarily due to: (i) lower projected personnel expenses as a result of staff vacancies and turnover; (ii) lower projected contract and consulting expenses due to reductions in the cost of various IT projects and outside consulting support for internal controls and risk management; and (iii) lower fixed asset expenditures for software application development. Significant contract and consultant expenses projected for the fourth quarter include: (i) $150k for FAC3 and $230k for study of the reliability effects of GMD in RAPA; (ii) $135k for SOCCED database; (iii) $80k for a survey assessing ERO effectiveness; and (iv)

approximately $618k for various projects in IT as further described below. The projection also reflects approximately $1.4M in fixed assets costs to complete or begin ERO Enterprise projects and for NERC IT infrastructure investments. The year end projection does not include approximately $285k in costs to make various improvements to the company's office space in Atlanta which are required to accommodate existing and projected staff. Further information regarding these improvement costs is included under the discussion below related to fixed asset purchases. These costs were not anticipated at the time the 2014 business plan and budget was prepared.

2014 YEAR-END PROJECTION VERSUS BUDGET BY CATEGORY

	As of September 30, 2014				As of June 30, 2014	
	2014 Projection	2014 Annual Budget	2014 Projected Variance from Budget Over(Under)	%	2014 Projected Variance from Budget as of June 30, 2014	Change in Projected Variance
TOTAL FUNDING	53,586,819	53,735,382	(148,563)	-0.3%	**(132,500)**	**(16,063)**
BUDGET - EXPENSES and FIXED ASSETS						
PERSONNEL EXPENSES	32,974,998	34,059,655	(1,084,657)	-3.2%	(270,107)	(814,550)
MEETINGS, TRAVEL and CONFERENCE CALLS	3,524,929	3,789,525	(264,596)	-7.0%	(325,079)	60,483
CONSULTANTS and CONTRACTS	7,100,985	6,828,973	272,012	4.0%	687,146	(415,134)
RENT	2,720,299	2,617,299	103,000	3.9%	33,000	70,000
OFFICE COSTS, PROFESSIONAL SERVICES and MISCELLANEOUS	5,760,631	5,832,854	(72,223)	-1.2%	(99,467)	27,244
Other Non-Operating Expenses	95,061	144,000	(48,939)	-34.0%	(64,633)	15,693
FIXED ASSET PURCHASES (excludes the credit for depreciation)	1,805,558	3,117,790	(1,312,232)	-42.1%	(905,593)	(406,639)
TOTAL BUDGET	**53,982,460**	**56,390,096**	**(2,407,636)**	**-4.3%**	**(944,733)**	**(1,462,902)**
FTEs	**179.87**	**189.53**	**(9.66)**	**-5.1%**	**(4.02)**	**(5.64)**

Year-to-date actual results and the 2014 year end projection reflected in the tables above do not include any expenses or funding related to CRISP. Further information regarding CRISP contract, budget and funding status is set forth in a separate section below.

Actual to Budget Variances for Expenses and Fixed Assets by Category

Personnel expenses were under budget $921.0k, 3.6%, under budget through September 30th and are projected to be $1.1M, 3.2%, under budget at year end. Total FTEs were under budget 10.4, 5.5%, as of September 30th and are projected to be 9.7, 5.1%, under budget at year end.

- Salaries expense, which includes salaries, ($663.0k under budget), incentive compensation, ($133.2k over budget), employment agency fees, ($130.9k over budget), and temporary office services, ($22.9k over budget), was $376.0, 1.9%, under budget as of September 30th. Salaries expense is projected to be $475.8k, 1.8%, under budget at year end due to lower than budgeted salaries as a result of staff vacancies, offset by: (i) higher than budgeted incentive compensation based upon the 3-year average of 18.4%; (ii) higher than budgeted employment agency fees; and (iii) higher than budgeted temporary office services which have been utilized during periods of staff vacancies and to support NERC's current operations.

- Payroll taxes were $49.6k, 3.7% over budget as of September 30th and are projected to be over budget $133.1k, 8.5% at year end due to an increase in the maximum taxable earnings cap which is higher than the assumption in the budget.

- Benefits were $229.7k, 9.0% under budget as of September 30th and are projected to be $410.0k, 12.1%, under budget at year end due to open positions, lower than budgeted renewal rates for employee health benefits and lower than budgeted relocation expense. Education benefits were over budget $43.1k through September 30th, and are projected to be equal budget at year end. Workers compensation expense is projected to be $11.6k over budget at year end based upon the final audit of the July 1, 2013 through June 30th.

- Retirement costs were $364.9k, 17.2%, under budget as of September 30th and are projected to be $332.0k, 11.5%, under budget at year end due to having fewer FTEs on staff, delayed eligibility related to timing of hiring and attrition and due to forfeiture of unvested employer contributions.

Meetings, Travel, and Conferencing expenses were collectively under budget $126.8k, 4.5%, through September 30th due to lower than budgeted travel and meeting expenses, offset by higher than budgeted conferencing expenses. Meetings and workshop expenses were $18.9k, 2.6%, under budget due to lower than budgeted workshop expenses related to the elimination of NERC funding of NASPI workshops, offset by higher than budgeted meeting expenses for the CIP V5 and physical security standards. Travel expenses were $112.1k, 6.2%, under budget through September 30th, and are projected to be $307.1k, 12.7%, under budget at year end based upon the current spend trend compared to the actual monthly spending trend in 2013.

Consultant and Contract expenses were under budget $1.2M, 22.2%, through September 30th and are projected to be over budget $272.0k, 4.0%, at year end. As further explained below, contracts for a number of projects were executed late in the third quarter and work has begun, but invoices have not been received.

CONSULTANTS and CONTRACTS	As of September 30, 2014 Actual	Budget	Over(Under)	2014 Projection	2014 Annual Budget	Variance from Budget Over(Under)
REGIONAL ENTITY OVERSIGHT AND ASSURANCE	406,715	362,500	44,215	450,543	400,000	50,543
RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	278,686	513,564	(234,878)	793,767	638,085	155,682
RELIABILITY RISK MANAGEMENT	1,230,403	1,081,640	148,764	1,550,228	1,289,108	261,120
CRITICAL INFRASTRUCTURE DEPARTMENT	98,904	142,501	(43,597)	249,612	190,000	59,612
ES-ISAC	334,087	671,050	(336,963)	681,300	786,450	(105,150)
CRISP	-	-	-	-	-	-
TRAINING, EDUCATION and OPERATOR CERTIFICATION	241,711	662,498	(420,786)	558,745	848,830	(290,085)
GENERAL and ADMINISTRATIVE	-	-	-	80,000	-	80,000
POLICY and EXTERNAL AFFAIRS	8,890	56,250	(47,360)	15,000	75,000	(60,000)
INFORMATION TECHNOLOGY	1,309,203	1,458,033	(148,830)	2,174,143	1,944,000	230,143
HUMAN RESOURCES	210,566	198,500	12,066	322,000	257,500	64,500
FINANCE and ACCOUNTING	107,559	285,000	(177,441)	225,647	400,000	(174,353)
TOTAL CONTRACTS and CONSULTANTS	**4,226,724**	**5,431,535**	**(1,204,811)**	**7,100,985**	**6,828,973**	**272,012**

- Regional Entity Oversight and Assurance – Over budget $44.2k through September 30th and projected to be $50.5k over budget at year end for consulting support to review RAI pilot programs and development of associated internal control evaluation and testing processes.
- Reliability Assessments and Performance Analysis – Under budget $234.9 through September 30th due to delays in execution of the contracts for FAC 3 vegetation management project and to study the reliability effects of GMD. The $155.7k over budget 2014 year end projection is primarily related to the FAC 3 vegetation management project. The contract for FAC 3 was executed in August and was identified as a use of Known Contingency Reserves in the 2014 Business Plan and Budget.
- Reliability Risk Management – $148.8k over budget primarily due to higher than budgeted expenses for NERCnet, offset by lower than budgeted expenses for SAFNR, which is due to timing of actual expenses versus the allocation of the budget for the project. The $261.1k year end over budget projection is due to higher than budgeted expenses for NERCnet and higher than budgeted expenses for the current secure alert system which is still being used pending transition to a new system.
- Critical Infrastructure Department – Under budget $43.6k through September 30th due to timing. The $59.6k over budget year end projection is for contract support to begin the planning process in 2014 for GridEx III, which will take place in 2015.
- Training, Education and Operator Certification – Under budget $420.8k through September 30th and projected to be $290.1k under budget at year end due to: (i) timing and projected lower than budgeted expenses related to the system operator database improvement project and examination development project; (ii) lower than budgeted system operator testing expenses due to a new vendor contract that was negotiated after the 2014 budget was developed; and (iii) lower than budgeted costs for industry and staff training.

- General and Administrative – The $80k over budget projection is related to the survey to assess the effectiveness of the ERO.
- Policy and External Affairs – Under budget $47.4k through September 30th and projected to be $60.0k under budget at year end due to a reduction in the need for outside consulting to support external affairs as a result of these duties being managed by NERC staff.
- Information Technology – Under budget $148.8k through September 30th and projected to be $230.1k over budget at year end. The plan developed by the IT department for completion or initiation of ERO Enterprise projects during the remainder of 2014 and included in the year end projection includes consulting support for: (i) $209.0k for review and development of IT architecture and enterprise application development strategy; (ii) $120.0k for development of an enterprise reporting tool for GADS/TADS/DADS data; and (iii) $88.6k for applications support for BESnet, SBS and the ERO portal with a new vendor. The spend plan for the remainder of 2014 for NERC infrastructure projects includes contract and consulting expenses for: (i) $208.0k for implementation of a document management system; and (ii) $45.0k for disaster recovery hardware and software, installation of new microphones in the Atlanta office large conference rooms and installation of new wireless network equipment. The projected over budget variance will be offset by lower than budgeted fixed asset costs for infrastructure equipment.
- Human Resources – Over budget $12.1k through September 30th and projected to be $64.5k over budget at year end due primarily to higher than budgeted expenses for executive training and development.
- Finance and Accounting – Under budget $177.4k through September 30th and projected to be $174.4k under budget at year end due to lower than budgeted consulting support for internal controls and risk management.

Rent expense is projected to be $103.0k, 3.9%, over budget at year end due to an approximate reduction of $24.5k in sublease revenue from NERC's former Washington, DC office in connection with negotiation and execution of a sublease amendment as a result of the subtenant's bankruptcy reorganization and due to an $80.0k increase in property taxes in Atlanta as a result of an increase in the tax assessment on the building by Fulton County based on a recent property tax revaluation. With respect to the sublease agreement, the company received an upfront payment in connection with the execution of its current lease space in Washington, D.C. to offset potential liabilities associated with the sublease. This upfront payment is included in the company's working capital reserves and is being amortized over the term of the lease and is sufficient to offset the reduction in sublease revenue resulting from the subtenant bankruptcy

Office Costs, Professional Services and Miscellaneous were collectively $60.2k, 1.4%, over budget through September 30th, and are projected to be $72.2k, 1.2%, under budget at year end.

- Office costs were $98.9k, 3.8%, under budget through September 30th and are projected to be $64.3k, 1.8%, under budget at year end primarily due to lower than budgeted costs for maintenance and service agreements.
- Professional services expenses were $179.0k, 10.7%, over budget through September 30th due to: (i) higher outside legal fees related to closing on the capital financing loan and preparation of the special assessment filing with FERC on behalf of Peak Reliability; (ii) higher trustee search fees, which were budgeted to occur in the fourth quarter, but were incurred in the third quarter; and (iii) higher than budgeted accounting and auditing fees related to review of NERC's retirement plans. Professional services are projected to be approximately equal to budget at year end. $171.6k in outside legal expense incurred to date related to development of CRISP contracts is not included in 2014 YTD Actual or the 2014 Projection for Office Costs, Professional Services and Miscellaneous since these costs will be funded by CRISP participants.
- Miscellaneous expenses were $19.9k, 72.8%, under budget as of September 30th and are projected to be approximately equal to budget at year end.

Other Non-Operating Expenses were under budget $23.2k, 21.5%, through September 30th due to lower than budgeted interest expense associated with the capital financing loan. Interest expense is lower than budget due to a lower than budgeted interest rate and a delay in closing the capital financing program loan. The actual interest rate on the loan, which closed in January, 2014 instead of fourth quarter, 2013, is 2.9%. The 2014 budget was developed using an interest rate of 3.5%. Other non-operating expenses are projected to be $48.9k, 34.0%, under budget at year end due to the reduction in interest expense.

Fixed Asset Purchases, which excludes the credit for depreciation, were $1.9M, 80.3%, under budget as of September 30th and are projected to be $1.3M, 42.1%, under budget at year end. $209.0k in fixed asset purchases are being used to offset the use of operating reserves to fund Enterprise IT strategy and application consulting support noted above. The plan developed by the IT department for completion or initiation of ERO Enterprise projects during the remainder of 2014 and included in the year end projection includes: (i) $162.5k completion of the Standards Balloting System; (ii) $87.6k to begin the RADS and Event Analysis projects; and (iii) $549.4k for hardware and software licenses for implementation of the xRM Platform. The spend plan for the remainder of 2014 for NERC infrastructure projects includes $350k for disaster recovery hardware and software, $100k for a new microphone system for the Atlanta conference rooms, and approximately $150k for other network infrastructure requirements.

In addition to the forgoing, management is recommending that certain improvements be undertaken to the Atlanta office space to better accommodate current budgeted staffing levels, as well as allow personnel within each department to be located in close proximity to their co-workers. An architect was retained to prepare drawings and estimate of the costs to undertake these improvements. The estimate is approximately $285k and management is separately requesting the committee's authorization to proceed with these improvements.

OPERATING RESERVE ANALYSIS

As of September 30, 2014, the available balance in working capital and operating reserves was $4.75M, after the adjustment of reserves for future liabilities. The total balance in working capital and operating reserves, including the reserves for future liabilities was $8.2M[1]. The current balances in the Known Contingency Reserve, Unknown Contingency Reserve and the System Operator Reserves as of September 30, 2014, were $1.0M, $2.35M, and $1.4M, respectively. After taking into consideration the use of reserves which are restricted for future liabilities associated with NERC's lease obligations, the balance in available operating reserves was approximately $2.6M higher than budget.

OPERATING RESERVE ANALYSIS - as of September 30, 2014

				2014 Current Reserve Balances			
	2014 Actual	2014 Budget*	Variance - Actual to Budget	Known Contingency Reserves	Unknown Contingency Reserves	System Operator Reserves	CRISP
WORKING CAPITAL and OPERATING RESERVES							
Balance as of 01/01/2014	6,264,672	8,217,862	(1,953,190)				
Less: Adjustment for future liabilities	(3,817,478)	(3,788,645)	(28,833)				
Beginning Available Operating Reserves	**2,447,194**	**4,429,217**	**(1,982,023)**	**1,000,000**	**(69,672)**	**1,516,866**	**-**
Proceeds from Financing Activities (non-current portion only)	562,222		562,222		562,222		
Change in Reserves from Current Year Operations	1,741,545	(2,320,011)	4,061,558	-	1,857,482	(115,937)	
Other adjustments to reserves**	2,648		2,648		2,648		
Available Reserve Balance	**4,753,609**	**2,109,206**	**2,644,405**	**1,000,000**	**2,352,680**	**1,400,929**	**-**

*The 2014 budget includes a $1.2M reduction in Known and Unknown reserves and a $438.3k planned reduction in the System Operator Reserves, for a total budgeted reduction in reserves of $1,660,724.

**Represents transactions recorded only on the Statement of Financial Position (balance sheet) and do not impact the Statement of Activities (income statement)

As of September 30th, the projected use of Unknown Contingency Reserves was $894.0k: (i) $48.5k for RAI contract support to develop the internal control evaluation and testing processes; (ii) $48.6k for data modeling and change orders related to generation databases; (iii) $25.1k for preliminary work on the development of E-GAR, which is a replacement for pcGAR; (iv) $59.6k for a cyber asset survey and to begin preparations for GridEx III in 2015; (v) $64.5k for executive coaching and HR administrative support; (vi) $80.0k for ERO effectiveness assessment; and (vii) $567.7k for IT architecture and strategy consulting, compliance database maintenance, and various IT infrastructure projects, including disaster recovery and network simplification, as explained above. Management projects to use $150k of Known Contingency Reserves for the FAC3 vegetation research project.

Based upon the revised 2014 spend plan for ERO Enterprise applications and NERC IT infrastructure projects included in the 2014 year end projection, the projected 2014 draw on the capital financing loan

[1] Refer to the Statement of Financial Position on page 10.

in 2014 for completed projects has been reduced from the budgeted amount of $1.416M to $1.28M. The $1.28M includes $379.2k for completion of Standards Balloting System, $549.4k for hardware and software to implement the xRM platform, and $350.0k for disaster recovery hardware. With this revision to the draw on the capital financing loan and based upon the current 2014 projection, the projected year end balances in the Known Contingency Reserve, Unknown Contingency Reserve and the System Operator Reserves are $850.0k, $1.37M, and $1.14M, respectively, for a total of approximately $3.4M, which is approximately $1.36M more than assumed for purposes of NERC's 2015 business plan and budget before taking into account any expenditure of reserves for the Atlanta office space improvements noted above. The projected 2014 year end balances in NERC's 2015 Business Plan and Budget in the Known Contingency Reserve, Unknown Contingency Reserve and the System Operator Reserves were $850.0k, $159.1k, and $996.4k, respectively, for a total of approximately $2.0M.

OPERATING RESERVE ANALYSIS - as of September 30, 2014

	2014 Projection as of 9/30/2014	2014 Budget*	Variance - Projection to Budget	2014 Projected Year End Reserve Balances: Known Contingency Reserves	Unknown Contingency Reserves	System Operator Reserves
WORKING CAPITAL and OPERATING RESERVES						
Balance as of 01/01/2014	6,264,672	8,217,862	(1,953,190)			
Less: Adjustment for future liabilities	(3,817,478)	(3,788,645)	(28,833)			
Beginning Available Operating Reserves	**2,447,194**	**4,429,217**	**(1,982,023)**	**1,000,000**	**(69,672)**	**1,516,866**
Proceeds from Financing Activities (non-current portion only)	1,309,406	943,993	365,412		1,309,406	
Change in Reserves from Current Year Operations	(395,641)	(2,654,714)	2,259,073	(150,000)	133,131	(378,773)
Other adjustments to reserves**		49,999	(49,999)		-	
Available Reserve Balance	**3,360,958**	**2,768,494**	**592,463**	**850,000**	**1,372,865**	**1,138,093**

*The 2014 budget includes a $1.2M reduction in Known and Unknown reserves and a $438.3k planned reduction in the System Operator Reserves, for a total budgeted reduction in reserves of $1,660,724.

**Represents transactions recorded only on the Statement of Financial Position (balance sheet) and do not impact the Statement of Activities (income statement)

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Statement of Activities, Fixed Assets and Change in Working Capital
(Unaudited, without CRISP)
For the period ended 09/30/2014

	2014 YTD Actual	2014 YTD Budget	2014 YTD Variance Over(Under)	%	2014 Projection	2014 Annual Budget	2014 Projected Variance from Budget Over(Under)	%
Funding								
Assessments	38,551,036	38,551,037	(0)		51,401,382	51,401,382	-	
Penalties	290,000	290,000	(0)		290,000	290,000	-	
Third-Party Funding (CRISP)	-	-	-		-	-	-	
Testing	1,214,814	1,215,000	(186)		1,620,000	1,620,000	-	
Services & Software	55,000	37,500	17,500		75,000	50,000	25,000	
Workshop Fees	196,852	218,250	(21,398)		197,837	354,000	(156,163)	
Interest	1,773	15,000	(13,227)		2,500	20,000	(17,500)	
Miscellaneous	58	-	58		100	-	100	
Total Funding	40,309,534	40,326,786	(17,253)	0.0%	53,586,819	53,735,382	(148,563)	-0.3%
Expenses								
Personnel Expenses								
Salaries	19,287,903	19,663,933	(376,030)		25,742,797	26,218,572	(475,775)	
Payroll Taxes	1,399,434	1,349,816	49,619		1,704,050	1,570,954	133,096	
Employee Benefits	2,309,779	2,539,431	(229,652)		2,975,925	3,385,917	(409,992)	
Savings & Retirement	1,757,088	2,122,009	(364,920)		2,552,226	2,884,212	(331,986)	
Total Personnel Expenses	24,754,205	25,675,186	(920,983)	-3.6%	32,974,998	34,059,655	(1,084,657)	-3.2%
Meeting Expenses								
Meetings	720,955	739,864	(18,909)		1,104,035	1,052,150	51,885	
Travel	1,702,576	1,814,644	(112,068)		2,112,400	2,419,525	(307,125)	
Conference Calls	242,525	238,387	4,138		308,494	317,850	(9,356)	
Total Meeting Expenses	2,666,057	2,792,895	(126,839)	-4.5%	3,524,929	3,789,525	(264,596)	-7.0%
Operating Expenses								
Consultants and Contracts	4,226,724	5,431,535	(1,204,811)		7,100,985	6,828,973	272,012	
Rent & Improvements	1,978,560	1,962,974	15,586		2,720,299	2,617,299	103,000	
Office Costs	2,535,167	2,634,022	(98,855)		3,441,736	3,506,074	(64,338)	
Professional Services	1,855,425	1,676,468	178,957		2,284,745	2,290,280	(5,535)	
Miscellaneous	7,433	27,375	(19,942)		34,150	36,500	(2,350)	
Depreciation	1,367,172	1,749,755	(382,583)		1,790,700	2,333,007	(542,307)	
Total Operating Expenses	11,970,482	13,482,129	(1,511,647)	-11.2%	17,372,615	17,612,133	(239,518)	-1.4%
Other Non-Operating Expenses	84,770	108,000	(23,230)	-21.5%	95,061	144,000	(48,939)	-34.0%
Total Expenses	39,475,514	42,058,210	(2,582,699)	-6.1%	53,967,602	55,605,313	(1,637,711)	-2.9%
Net Change in Assets	**834,020**	**(1,731,424)**	**2,565,446**	**-148.2%**	**(380,783)**	**(1,869,931)**	**1,489,148**	**-79.6%**
Fixed Assets								
Depreciation	(1,367,172)	(1,749,755)	382,583		(1,790,700)	(2,333,007)	542,307	
Computer & Software	293,020	2,178,593	(1,885,572)		1,522,674	2,904,790	(1,382,116)	
Furniture & Fixtures	-	-	-		-	-	-	
Equipment	166,627	159,750	6,877		282,884	213,000	69,884	
Leasehold Improvements	-	-	-		-	-	-	
Incr(Dec) in Fixed Assets	**(907,525)**	**588,587**	**(1,496,112)**	**-254.2%**	**14,858**	**784,783**	**(769,925)**	**-98.1%**
Total Budget (Expenses plus Incr(Dec) in Fixed Assets)	**38,567,989**	**42,646,800**	**(4,078,811)**	**-9.6%**	**53,982,460**	**56,390,096**	**(2,407,636)**	**-4.3%**
FTE's	**179.16**	**189.53**	**(10.37)**	**-5.5%**	**179.87**	**189.53**	**(9.66)**	**-5.1%**

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Statement of Financial Position
(Unaudited)
For the period ended 09/30/2014

			Available Operating Reserves	
	9/30/2014	12/31/2013	9/30/2014	12/31/2013
ASSETS				
Cash	35,262,617	26,182,060	35,262,617	26,182,060
Accounts receivable, net of allowance for uncollectible accounts of 0 and 62,573 in 2014 and 2013	14,884,169	3,353,895	14,884,169	3,353,895
Prepaid expenses and other current assets	884,384	869,876	884,384	869,876
Security deposit	99,136	99,136		
Cash value of insurance policies	-	-		
Employee Fiduciary - 457b	320,660	320,660		
Property and equipment	4,737,591	5,645,116		
Total Assets	56,188,557	36,470,743		
LIABILITIES AND NET ASSETS				
Liabilities				
Current Portion				
Accounts payable and accrued expenses (includes vacation accrual)	2,975,649	2,917,303	(2,975,649)	(2,917,303)
Accured incentive compensation	2,968,310	4,025,979	(2,968,310)	(4,025,979)
Deferred rent-current	231,501	182,421	(231,501)	(182,421)
Deferred compensation - current	14,257	20,386	(14,257)	(20,386)
Capital lease obligations - current	47,108	47,108	(47,108)	(47,108)
Accrued retirement liabilities	1,453,739	1,788,624	(1,453,739)	(1,788,624)
Debt service - current portion	421,667		(421,667)	-
Deferred income	12,917,692	5,287,044	(12,917,692)	(5,287,044)
Deferred revenue - penalties	0	-	(0)	-
Deferred revenue - other	14,000		(14,000)	-
Regional assessments	19,115,051	9,427,293	(19,115,051)	(9,427,293)
Total Current Portion	40,158,974	23,696,159		
Long-Term Portion				
Deferred compensation[1]	600,162	597,514		
Long-Term Debt	562,222			
Deferred Rent-non-current	3,635,209	3,817,478	(3,635,209)	(3,817,478)
Capital lease obligations - non-current	-	-		
Total Long-Term Portion	4,797,594	4,414,992		
Total Liabilities	44,956,567	28,111,151		
Net Assets - unrestricted	8,576,990	7,914,592		
Net Assets - restricted	2,655,000	445,000	(2,655,000)	(445,000)
Total Liabilities and Net Assets	56,188,557	36,470,743	4,581,986	2,447,194

[1]Includes 457b liability, life insurance for former executive, and retiree medical

Working Capital and Operating Reserves	**8,217,196**	**6,264,672**
Less: Restriction for future liabilities	(3,635,209)	(3,817,478)
Available Working Capital and Operating Reserves*	4,581,986	2,447,194

*The Available Working Capital and Operating Reserve balance as of September 30, 2014 per this report includes the expenditure of $172.6k in legal fees associated with CRISP that will be reimbursed by CRISP participants.

Financial Covenants	
1 - WC & OR Balance to Debt Service Ratio > 1.2 to 1.0 (Working Capital / Debt Service)	19.49
2 - Liquidity to Debt Service Ratio > 1.5 to 1.0 (= Cash - Regional Assessments - Restricted Net Assets)	32.00

CRISP

Significant progress has been made on CRISP. All legal documentation has been finalized. 2014 and 2015 budgets and funding mechanics have also been finalized with PNNL and participating utilities. NERC and an initial group of 15 utilities have signed the Master Agreement (MA) and associated statements of work and another 6 utilities have indicated an intent to sign in the future. Management expects this number may grow now that the program is officially launched.

A separate bank account has been established to segregate CRISP funds and track funding by utility participant. We are in the process of collecting 2014 funding requirements from participating utilities. 2015 funding will be in two installments, with the first installment due in early January, 2015. The second installment will be due within 30 days after NERC provides a reconciliation of actual to budgeted costs, which is anticipated to be on or about March 15, 2015.

The 2014 CRISP budget is sufficient to fund 100% of the 2014 CRISP program costs, inclusive of PNNL costs. An overall not to exceed budget, as well as a not to exceed budget by participating utility, has been agreed to with PNNL and each participating utility. Consistent with the NERC Board's authorizing resolution, 2014 utility funding was established in a sufficient amount to avoid the use of existing reserves.

The 2015 budget reflects final cost reduction negotiations with PNNL, as well as the allocation of direct funding of program startup costs by participating utility in 2014. The final 2015 budget, inclusive of PNNL costs and the MSA defense fund, has been reduced from approximately $9.8M to approximately $5.9M. This is in large part due to the inclusion of the funding of PNNL startup capital costs and certain other startup expenses in the 2014 budget, which are thus not required in the 2015 budget. The 2014 budget, covering the period from October 1, 2014 thru December 31, 2014, is approximately $4.9M. The aggregate direct utility funding for 2014 and 2015 will be approximately $10.3M. The final total 2014 and 2015 CRISP budgets are set forth in Attachment A. NERC's internal 2015 ES-ISAC department budget, which is exclusive of PNNL subcontract costs and other costs funded directly by utility participants, is consistent with the internal ES-ISAC budget included in the company's 2015 business plan and budget and utilized to determine the portion of the 2015 CRISP budget funded through assessments.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF AMENDMENTS TO REGIONAL RELIABILITY STANDARDS DEVELOPMENT PROCEDURE OF THE NORTHEAST POWER COORDINATING COUNCIL, INC.

Pursuant to § 215(e)(4) of the Federal Power Act ("FPA")[1] and 18 C.F.R. §§ 39.8 and 39.10, the North American Electric Reliability Corporation (NERC) requests Federal Energy Regulatory Commission (FERC or Commission) approval of the proposed Northeast Power Coordinating Council, Inc. (NPCC) Regional Standard Processes Manual (RSPM). The RSPM is contained in Exhibit C to the Amended and Restated Delegation Agreement between NERC and NPCC (NPCC Delegation Agreement). The proposed amendments to the NPCC Delegation Agreement consist of amendments to Exhibit C, the NPCC Regional Reliability Standards Development Procedure (RRSDP). The RRSDP is a "Regional Entity Rule" as defined in 18 C.F.R. § 39.1; thus, in accordance with 18 C.F.R. § 39.10, amendments to the RRSDP require Commission approval. By approving the proposed amendments to Exhibit C of the NPCC Delegation Agreement, the Commission will also be approving the amendments to the RRSDP as a "Regional Entity Rule."

Revisions to the RRSDP were executed by NPCC Staff and were posted for comment from May 21, 2013 until July 5, 2013. The comments received were reviewed by NPCC Staff and incorporated as necessary, and the document was posted for a second comment period between

[1] 16 U.S.C. §824o (2005).

September 5, 2013 and October 20, 2013. After this second review of the comments received, the NPCC Regional Standards Committee ("RSC") approved the document to be posted for a pre-ballot review from November 12, 2013 until December 12, 2013. The ballot period for document approval was December 13, 2013 until January 27, 2014. The amended RRSDP, renamed to the RSPM, was approved by the NPCC Board of Directors ("BOD") at its March 11, 2014 meeting. The approved package was forwarded to NERC for approval, and it was approved by the NERC Board of Trustees on August 14, 2014.

As described in greater detail in Section III of this Petition, the principal purposes of the amendments to the RRSDP are:

(1) to change the name of the RRSDP to the Northeast Power Coordinating Council, Inc. Regional Standard Processes Manual (RSPM),

(2) to provide organization and clarity to the RSPM by developing separate sections for:

(i) the withdrawal of a request for approval of a regional standard before it has been approved,

(ii) retirement of an approved NPCC regional standard,

(iii) requirements for approval of a process waiver, and

(iv) process for correcting errata;

(3) to incorporate NPCC's Cost Effectiveness Analysis Procedure (CEAP) into the RSPM;

(4) to further develop NPCC's clarification process for regional standards,

(5) to create new appendices for the newly revised RSPM, and

(6) to recognize the Reliability Standard Audit Worksheet (RSAW) as necessary to a regional standard developed by the NPCC Standard Drafting Team and the NPCC

Compliance Staff. The proposed revisions also implement various updates, corrections, and typographical and format changes.

Attachment 1 to this filing is a "Clean" version of the RSPM incorporating the proposed amendments. Attachment 2 is a "Redline" version of the RSPM, marked to show the proposed amendments. By approving the proposed amendments to the RSPM included in this filing, the Commission will also be approving the amendments for purposes of Exhibit C to the NPCC Delegation Agreement.[2]

[2] The complete currently effective NPCC RE Delegation Agreement is available at: http://www.nerc.com/AboutNERC/Pages/Regional-Entity-Delegation-Agreements.aspx. Upon approval by the Commission of the amended RRSDP, the RSPM will be inserted into Exhibit C of the posted version of the NPCC Delegation Agreement.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[3]

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 467-0474 – facsimile

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

[3] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2014), to allow the inclusion of more than two persons on the service list in this proceeding.

II. PROPOSED NPCC RSPM

The currently effective version of the NPCC Regional Reliability Standard Development Procedure ("NPCC RRSDP") is Version 0 adopted by FERC on March 21, 2008.[4] The proposed amendments to the NPCC RRSDP include numerous improvements. As a preliminary matter, the title of the document has been changed from Northeast Power Coordinating Council, Inc. Regional Reliability Standards Development Procedure to the Northeast Power Coordinating Council, Inc. Regional Standards Processes Manual ("RSPM") to achieve consistency with the names of similar documents in the Delegation Agreements of other Regional Entities and NERC. The other proposed amendments revise the RRSDP to accomplish a number of objectives, including:

- developing separate sections within the RRSDP (hereafter referred to as "RSPM") for (i) "Withdrawal of a Regional Standard Pending Approval," (ii) "Retirement of an Approved NPCC Regional Standard," (iii) "Discontinuance of Regional Standard Development," (iv) "Approval of Process Waiver," and (v) "Process for Correcting Errata."
- integrating NPCC's CEAP into the RSPM,
- further developing NPCC's interpretation process for regional standards by moving to a clarification process instead of an interpretation process to ensure all statutory requirements are met while maintaining an expedited process to produce clarifications for stakeholders,
- revising Appendix A: Regional Standard Authorization Request (RSAR)

[4] *The North American Electric Reliability Corporation*, 122 FERC ¶ 61,245 (March 21, 2008).

Completion Guidelines and Form and developing three new appendices for the RSPM, including (i) Appendix B: Selection of Drafting Team Members and Nomination Form, (ii) Appendix C: Maintenance of Regional Standards and Process and (iii) Appendix D: NPCC Clarification Request;

- identifying the Reliability Standard Audit Worksheet (RSAW) as a companion document to a regional standard that is collaboratively developed by the NPCC Standard Drafting Team and the NPCC Compliance Staff; and,
- implementing other corrections, clarifications and typographical, formatting, and minor language changes.

The discussions in the following subsections describe the proposed amendments to the RRSDP.

A. Table of Contents

The original Table of Contents is removed and replaced with a more expansive and inclusive Table of Contents to account for all of the additional requirements and information added to the RRSDP since the last filing. The revisions to the Table of Contents provide reference to each new section, including the various background information provided in the "Regional Standard Characteristics and Elements" section and the additional subsections added under the "Regional Standards Development Process" section. Further, the Table of Contents provides reference to the page numbers for each of the steps under Regional Standards Development Process as well as the Appendices A, B, C, and D.

B. Section I: Executive Summary

The Executive Summary is substantially revised to remove a majority of the

background information about NPCC and to add revision history of the RSPM. Of particular importance is a section describing the close work of the NPCC Reliability Standards Staff in concert with the RSC to complete the revisions to the RSPM that are the subject matter of this filing. Several lines are inserted in this section which describe "Key changes" that were approved by the BOD including, among other changes, the incorporation of process improvements, provision of greater clarity, inclusion of the new CEAP, development of the RSAW, and the creation of three new appendices.

C. Section II: Introduction

New subsections for the Introduction section organize the subject matter further into "Purpose" and "Background" subsections.

The "Purpose" subsection describes the purpose and scope of regional standards and of the RSPM. The revisions to the subsection also list numerous guiding principles describing the development of standards as well as the proper procedure for regulatory approval following both industry and NPCC approval of proposed regional reliability standards.

The "Background" subsection describes the responsibilities of NPCC for "promoting and improving the reliability of the international, interconnected, Bulk Electric System in Northeastern North America." It also provides a description of NPCC's delegated authority to develop reliability standards, and it describes the legal and historical background for the creation of NPCC, the mission of NPCC, the statutory authority for the delegation of power to NPCC, the legal framework for the ERO and Regional Entity model, and the relationship of NPCC to NERC.

D. Section III: Regional Standard Characteristics and Elements

Under the "Characteristic Attributes" subsection, text is amended to describe the key

characteristics of the regional standards development process, including: (i) fair due process, (ii) openness, (iii) inclusive, (iv) balanced, (v) transparent, and (vi) without undue delay. The subsection is also augmented to account for objectives of the regional standards development process, including: (i) No Adverse Impact on Reliability of the Interconnection, (ii) Justifiable Difference, (iii) Uniformity, and (iv) No Undue Adverse Impact on Commerce. Each of these characteristics and objectives include appropriate explanations of their purpose, scope, and application to the NPCC regional standards development process.

Under the "Elements of a Regional Standard" subsection, minor revisions were made to improve the text and style of language as well as to correct grammatical inconsistencies. Also, Table 1 and Table 2 were removed from this subsection. Table 1 and Table 2 were removed to improve the readability of this section of the RSPM.

The "Types of Reliability Requirements" subsection is added to describe the variety of requirements that should be represented in the Drafting Team's portfolio of requirements to achieve an effective defense-in-depth strategy. The Types of Reliability Requirements are Performance-based, Risk-based, and Capability-based; for each of those types, a brief definition is added.

The "Elements of a Regional Standard" subsection is added to describe the necessary components of a reliability standard. As is developed further in that subsection, the standard should, at a minimum, include: (1) Applicability, (2) Requirements, and (3) the Effective Dates. Additional components are included for informational purposes, but they are not mandatory and enforceable. A description of each of the possible elements for a reliability standard is added to this subsection to provide additional information for the development of regional standards. A description of "Compliance Elements," or "elements to aid in the administration of compliance

monitoring and enforcement responsibilities" is also added to provide explanations for various compliance elements, including (i) Measure, (ii) Violation Risk Factors and Violation Severity Levels, (iii) Version History, (iv) Variance, (v) Compliance Enforcement Authority (CEA), and (vi) Reliability Standard Audit Worksheets (RSAWs). A description of "Informational Elements: Elements to aid in the implementation of the regional standard" is also added to provide explanations for various informational elements, including (i) Application Guidelines and (ii) Procedures. The information in the "Terms and Functions" subsection is relocated to Section IV. Regional Standards Development Process.

E. Section IV: Regional Standards Development Process

The Regional Standards Development Process section is added to encompass the entire process for the development of a regional standard. Within this section, subsections are added to provide clarity to the process, including the addition of subsections for (i) Roles in the NPCC Regional Standards Process, (ii) Standard Development Process Steps, (iii) Standard Clarification Process Steps, (iv) Discontinuance Of Regional Standard Development, (v) Withdrawal of a Regional Standard Pending Approval, (vi) Retirement Of An Approved NPCC Regional Standard, (vii) Approval Of Process Waiver, (viii) Process For Correcting Errata, and (ix) Appeals (process broken down into two levels).

"Roles in the NPCC Regional Standards Process" is a subsection added to provide rules for Nomination, Revision, Interpretation, or Retirement of a Standard and to provide information on Process Roles and Responsibilities for various NPCC regional standard development participants. Full descriptions of each of the Process Roles and Responsibilities are added to this subsection, including descriptions for: Board of Directors, Drafting Team, Manager of Reliability Standards, NPCC Members, Non-NPCC Members, NPCC Standards Staff, NPCC

Committees, Task Forces and Working Groups, Regional Standards Committee (RSC), Reliability Coordinating Committee (RCC), Requester, and Quality Review Team.

"Standard Development Process Steps" is a subsection added to provide individual process steps for the development of a regional standard. Step 2.1 is created to describe a Regional Standard Authorization Request (RSAR), the first step in the development, modification or retirement of a standard. Steps 2.1.A, 2.1.B, and 2.1.C are created to describe different actions to be taken by Requesters, NPCC Manager of Reliability Standards, and the RSC for submission of the RSAR. Step 2.2 is added for the purpose of describing the timeline and process for responding to the RSAR, and also the creation of a Drafting Team for a new or revised standard. Step 2.3 is added to describe the actual development process of the standard and associated documents, including all of the work product expected from the Drafting Team. Steps 2.4.A and 2.4.B are created to provide information for posting for comment and the resolution of those comments during a final comment period, respectively. Step 2.5 "Posting for Ballot Period in the Open Process" is created to describe the posting, quorum, and voting requirements. Steps 2.5.A, 2.5.B, 2.5.B.1, and 2.5.B.2 are added to provide situational responses based on the number of votes received. Step 2.6 is added to direct the BOD to either approve, approve with the stipulation that non-substantive comments be incorporated, or remand a standard presented to them upon the affirmative vote of the NPCC Members, and Step 2.7 provides direction for submission of the new or revised standard to NERC for filing with FERC. Finally, Step 2.8 is created to provide the process for the implementation of a regional standard upon recognition and approval of the standard by the Applicable Governmental Authority.

"Standard Clarification Process Steps" is a subsection that is added to provide individual process steps for requests for standard clarifications. Step 3.1 is added to allow any Member of

NPCC or group within the NPCC region to submit a Clarification Request (CR). As this Step explains, a valid CR is one that seeks additional clarity about one or more requirements in an approved regional standard, but does not request approval as to how to comply with any requirements of the standard. Step 3.1 also provides that a request may alternatively seek a Request for Interpretation and explains that an interpretation will be initiated under the NERC process for developing an interpretation. Step 3.2, Review and Validation of Clarification Request (CR) is added so that the NPCC Manager of Reliability Standards may determine the validity of a CR. Step 3.3 is added to explain the Regional Standards Committee (RSC) Actions and its role in accepting or rejecting the CR jointly with the NPCC Manager of Reliability Standards. Step 3.4, Formation of a Drafting Team for the Response to CR, and Step 3.5 are created to provide guidance on the process for developing a response to the CR. Step 3.6 is added to explain the procedure for posting the CR for a comment period and resolution of said comments. Step 3.7 is added to explain the actions to be taken by the RSC upon receipt of the CR from the NPCC Manager of Reliability Standards. Finally, Step 3.8 is added to direct the BOD to take an action on the CR once it has been endorsed by the RSC.

"Discontinuance of Regional Standard Development" is a subsection added to define the term "discontinuance" as used in the RSPM, and refers to the termination of the standard development process after RSAR approval but prior to posting for industry ballot.

"Withdrawal of a Regional Standard Pending Approval" is a subsection added to define the term "withdrawal" as used in the RSPM. This process allows the requester to revoke a request for approval of a regional standard, variance, clarification, or definition that has already "been approved by the NPCC Board of Directors and has not been filed with Applicable Governmental Authorities or has been filed but not yet approved by Applicable Governmental

Authorities".

"Figure 5" of the RSPM, the "Flowchart Regional Standards Development Procedure (Open Process)," is removed from the RRSDP because its content is included in Figure 1 Flowchart of Regional Standards Development Process Overview.

"Retirement of an Approved NPCC Regional Standard" is a subsection added to define the term "retirement" as used in the RSPM, and to explain the discontinuance of a regional standard, variance, clarification, or definition that has been approved by the Applicable Governmental Authority.

"Approval of Process Waiver" is a subsection added to give NPCC the authority to develop a new or modified regional standard, implementation plan, variance, clarification, or definition when extenuating circumstances arise. As is explained in that subsection, the RSC may override the requirements for standard development in the RSPM if good cause exists, limited to extenuating circumstances. That subsection also allows any individual to submit a waiver request to the RSC, and it requires certain notice to be provided before the waiver request may be considered.

"Process for Correcting Errata" is a subsection added to give the RSC the ability to make minor errata changes after final ballot approval by the NPCC ballot body. More detailed directions for submitting these errata changes are also added to this subsection.

The "Appeals" section is edited to account for non-substantive grammatical errors, updated terms, style, and improved text, and it is not amended substantively from the original RRSDP.

F. Appendix A: RSAR Completion Guidelines

Appendix A: RSAR Completion Guidelines is added to provide guidance that results in a streamlined, efficient process for submitting an RSAR to the NPCC Manager of Reliability Standards. Also included in this Appendix is a revised version of the RSAR with some minor stylistic changes and limited typographical and grammatical revisions. Substantively, the RSAR is updated to reflect the requirements for RSARs in the RSPM, including revisions to the following fields in the RSAR, which are edited to become a "Required Field" for purposes of submission to NPCC: (i) information for the standard and of the RSAR requester, (ii) detailed description of the "Purpose" of the proposed standard, (iii) the technical justification for "Industry Need," (iv) a "Brief Description" of the proposed standard, (v) identification of "Reliability Functions," (vi) a "Detailed Description" of the standard, (vii) "Related Standards," and (viii) "Related SARs or RSARs."

G. Appendix B: Selection of Drafting Team Members

Appendix B: Selection of Drafting Team Members is added to explain the process by which Drafting Team Members are selected. Precise criteria for each member and for the selection process are added to this Appendix. Also included in this Appendix is the newly created Nomination Form for NPCC [Name of Drafting Team] Drafting Team, used to allow parties to nominate candidates to the Drafting Teams.

H. Appendix C: Maintenance of Regional Standards and Process

Appendix C: Maintenance of Regional Standards and Process is added to provide for periodic review and revision to NPCC regional standards and to the RSPM so that those documents remain current and viable. To provide clarity, Appendix C is further separated into two

subsections: Maintenance of Regional Standards and Maintenance of Regional Standards Process. These two subsections provide a timeline for review of these documents and the requirements for the review process.

I. Appendix D: NPCC Clarification Request

Appendix D: NPCC Clarification Request is added to provide a standard form for submitting a clarification request.

III. CONCLUSION

The North American Electric Reliability Corporation respectfully requests that the Commission approve the proposed amendments to NERC's Delegation Agreement with NPCC which includes the currently effective RRSDP, shown in **Attachment 1** to this Petition, including approving the amendments to the RRSDP and renaming the RRSDP to RSPM (included in Exhibit C to the NPCC Delegation Agreement) as amendments to Regional Entity Rules.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 467-0474 – facsimile

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

Counsel for the North American Electric Reliability Corporation

Date: September 15, 2014

Attachment 1 (Clean)

NPCC, Inc.

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

Northeast Power Coordinating Council, Inc.

Regional Standard Processes Manual (RSPM)



Adopted by FERC: XXXX XX, 20XX

Approved by NERC Board of Trustees: August 14, 2014

Approved by NPCC Board of Directors: March 11, 2014

Revision History

Version	NPCC Board of Directors Approval	NERC Board of Trustees Approval	FERC Approval
0	9/19/07	10/23/07	3/21/08
1	3/11/14	8/14/14	xx/xx/xx

NPCC REGIONAL RELIABILITY STANDARDS PROCESS MANUAL

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 3
II. INTRODUCTION 4
PURPOSE 4
BACKGROUND 4
III. REGIONAL STANDARD CHARACTERISTICS AND ELEMENTS 5
1. CHARACTERISTIC ATTRIBUTES 5
2. ELEMENTS OF A REGIONAL STANDARD 6
TYPES OF RELIABILITY REQUIREMENTS 6
ELEMENTS OF A REGIONAL STANDARD 7
IV. REGIONAL STANDARDS DEVELOPMENT PROCESS 9
1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS 9
NOMINATION, REVISION, CLARIFICATION, OR RETIREMENT OF A STANDARD: 9
PROCESS ROLES AND RESPONSIBILITIES 9
2. STANDARD DEVELOPMENT PROCESS STEPS 11
STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE 11
STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD 12
STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS 13
STEP 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 14
STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS 16
STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL 17
STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL 18
STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD 18
3. STANDARD CLARIFICATION PROCESS STEPS 19
STEP 3.1: REGIONAL STANDARDS CLARIFICATION REQUEST (CR) 19
STEP 3.2: REVIEW AND VALIDATION OF CLARIFICATION REQUEST (CR) 19
STEP 3.3: NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS 20
STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO CR 20
STEP 3.5: DEVELOPMENT OF RESPONSE TO CR 20
STEP 3.6: POSTING CR FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 21
STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF CR 21
STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF CR 21
4. DISCONTINUANCE OF REGIONAL STANDARD DEVELOPMENT 22
5. WITHDRAWAL OF A REGIONAL STANDARD PENDING APPROVAL 23
6. RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD 23
7. APPROVAL OF PROCESS WAIVER 23
8. PROCESS FOR CORRECTING ERRATA 24
9. APPEALS 24
LEVEL 1 APPEAL 25
LEVEL 2 APPEAL 25
APPENDIX A: RSAR COMPLETION GUIDELINES A1
APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS B1
APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS ... C1
MAINTENANCE OF REGIONAL STANDARDS C1
MAINTENANCE OF THE REGIONAL STANDARDS PROCESS C1
APPENDIX D: NPCC CLARIFICATION REQUEST D1

I. EXECUTIVE SUMMARY

The NPCC Bylaws state "NPCC shall develop a Regional Reliability Standards Development Procedure that provides the design-basis approach to a consensus building process by which NPCC may develop Regional Reliability Standards and Regional Variances to be proposed to the ERO for adoption, under delegated authority by the FERC and the Canadian Provincial regulatory and/or governmental authorities."

The NPCC Regional Reliability Standards Development Procedure was originally adopted by the NPCC Board of Directors on September 19, 2007. The NPCC Reliability Standards Staff in concert with the NPCC Regional Standards Committee (RSC) has completed a revision to the NPCC Regional Reliability Standards Process Manual to incorporate process improvements, provide greater clarity and reflect the new NPCC Cost Effectiveness Analysis Procedure (CEAP).

Key changes addressed in this revision include:

- Replacing interpretation with clarification and expanding the Clarification Section narrative into process steps and including an associated flowchart
- Creating separate sections for: 1) Withdrawal of a Regional Standard Pending Approval; 2) Retirement of an Approved NPCC Regional Standard; and 3) Approval of Process Waiver; 4) Process for Correcting Errata
- Recognizing the new NPCC Cost Effectiveness Analysis Procedure (CEAP)
- Identifying the Reliability Standard Audit Worksheet (RSAW) as a companion document to a regional standard that needs to be collaboratively developed by the drafting team and NPCC Compliance Staff
- Creating three new appendices: 1) Appendix A: Regional Standard Authorization Request (RSAR) Completion Guidelines and Form; 2) Appendix B: Selection of drafting team Members and Nomination Form; and 3) Appendix C: Maintenance of Regional Standards and Process

In addressing areas for improvement in the NPCC Regional Reliability Standards Development Procedure, recent improvements made to the NERC Standards Process Manual (e.g., Standards Process Input Group (SPIG) recommendations) as well as the manuals of other Regional Entities were benchmarked to identify best practices for inclusion in this manual.

The process improvements and clarity captured in this revision to the NPCC Regional Reliability Standards Development Procedure, will result in a more timely and efficient manner to address the development of regional standards to ensure the reliability of the Bulk Electric System within the NPCC geographical area.

II. INTRODUCTION

PURPOSE

This manual defines the characteristics of a Northeast Power Coordinating Council, Inc. (NPCC) regional Reliability Standard (hereinafter referred to as "regional standard") and establishes the process by which NPCC regional standards are developed, approved, revised, clarified and retired. The NPCC regional standards process is a stakeholder process that is approved by the NPCC members to ensure a transparent standard development process that is "open, fair, and inclusive."

NPCC regional standards address the reliability of the international and interconnected Bulk Electric System in Northeast North America. NPCC regional standards shall enable or support one or more NERC/ERO reliability principles[1] and will, in all cases, not be inconsistent with or less stringent than any requirements of the North American Electric Reliability Council/Electric Reliability Organization (NERC/ERO) continent-wide Reliability Standards.

The development of NPCC regional standards is performed according to the following principles using the process contained in this manual:

- Developed in a fair and open process that provides an opportunity for all interested parties to participate;
- Does not have an adverse impact on commerce that is not necessary for reliability;
- Provides a level of Bulk Electric System reliability that is adequate to protect public health, safety, welfare, and national security and would not have a significant adverse impact on reliability; and
- Based on a justifiable difference between Regions or between sub-Regions within the Regional geographic area.

Following industry approval, NPCC regional standards process and NPCC regional standards require approval by the NPCC Board of Directors, NERC as the Electric Reliability Organization (ERO) and the applicable regulatory authorities in the United States (FERC) and Canada.

BACKGROUND

Northeast Power Coordinating Council, Inc. (NPCC) is responsible for promoting and improving the reliability of the international, interconnected Bulk Electric System in Northeastern North America. NPCC carries out its mission through (i) the development of regional standards and compliance assessment and enforcement of continent-wide and regional standards, coordination of system planning, design and operations, and assessment of reliability, (collectively, "Regional Entity activities"), and (ii) the establishment of regionally-specific criteria, and monitoring and enforcement of compliance with such criteria (collectively, "criteria services activities").

The Energy Policy Act (EPA) of 2005 (Section 1211) amended the Federal Power Act (FPA) by adding Section 215, Electric Reliability. Specifically regarding standards development and pursuant with Section 215(e)(4) of the FPA, NPCC as a Regional Entity with delegated authority from NERC may propose regional standards to NERC for eventual enforcement within the NPCC region.

[1] Reliability Principles are available on the NERC website as amended from time to time

As a condition of NPCC membership, NPCC General and Full Members[2] agree to adhere to NERC Reliability Standards. NERC Reliability Standards are comprised of both continent-wide and regional standards. The NPCC regional standards apply only to that part of the Eastern Interconnection within the NPCC geographical area.

III. REGIONAL STANDARD CHARACTERISTICS AND ELEMENTS

1. CHARACTERISTIC ATTRIBUTES

The NPCC regional standards development process has the following key characteristics:

- **Fair due process** — The NPCC regional standards development process provides 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. Upon approval by the NPCC Members, the NPCC Board of Directors then votes to approve submittal of the regional standard to NERC for ERO approval, followed by submission to FERC and Canadian Authorities for their approvals.
- **Openness** — Participation in the NPCC regional standards development process is open to all persons and organizations that are directly and materially affected by the reliability of the NPCC's Bulk Electric System. There is no undue financial burden to participation. Participation shall not be conditioned upon membership in the ERO, NPCC or any organization, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements.
- **Inclusive** — Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the reliability of NPCC's Bulk Electric System has the right to participate by: (a) expressing an opinion and its basis; (b) having their position considered, and (c) having the right to appeal a response through an established appeal process.
- **Balanced** — The NPCC regional standards development process strives to have an appropriate balance of interest and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter. Pursuant with the NPCC By-Laws[3] there are seven (7) stakeholder voting sectors and the votes for each sector are weighted to achieve an appropriate balance.
- **Transparent** — All actions material to the development of NPCC regional standards are transparent and information regarding the progress of a standard's development action is made available to the public through postings on the NPCC website as well as through E-mail lists.
- **Without undue delay** — The NPCC regional standards development process shall be performed within a reasonable time.

In as much as NPCC is one of six Regional Entities within the Eastern Interconnection of North America, there will be no presumption of validity by the ERO for any NPCC regional standard.

[2] As defined in the NPCC By-Laws – available on the NPCC website
[3] NPCC By-Laws are available on the NPCC website

In order to receive the approval of the ERO, the NPCC regional standards development process must also achieve the following objectives:

- **No Adverse Impact on Reliability of the Interconnection** — A NPCC regional standard provides an Adequate Level of Reliability[4] as defined by NERC.
- **Justifiable Difference** — A NPCC regional standard addresses a justifiable difference within the NPCC geographical area that results from a physical difference[5] or operating difference in the Northeast's Bulk Electric System. Although a justifiable difference allows for a unique regional standard, a NPCC regional standard shall be no less stringent than a continent-wide standard.
- **Uniformity** — To the extent possible, the NPCC regional standards provides uniformity with Reliability Standards across the interconnected Bulk Electric System of North America.
- **No Undue Adverse Impact on Commerce** — A NPCC regional standard will not cause any undue adverse impact on business activities that are not necessary for reliability of the Region and its interconnected Regions. All regional standards shall be consistent with NERC's market principles[6].

2. ELEMENTS OF A REGIONAL STANDARD

To ensure uniformity of regional standards and avoid inconsistency with NERC continent-wide standards, a NPCC regional standard shall be consistent with the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of regional standards. The application of a systematic discipline is necessary for achieving regional standards that are measurable, enforceable, and consistent as well as results oriented[7], i.e.:

- Performance-based,
- Risk-based, and
- Capability-based.

TYPES OF RELIABILITY REQUIREMENTS

Regional reliability standards should be viewed as a portfolio of requirements designed to achieve an effective defense-in-depth strategy. Each requirement should identify a clear and measurable expected outcome, such as: a) a stated level of reliability performance, b) a reduction in a specified reliability risk, or c) a necessary competency.

a) **Performance-based** - defines a specific reliability objective or outcome that has a direct, observable effect on the reliability of the Bulk Electric System, i.e. an effect that can be measured using power system data or trends.

---

[4] Adequate Level of Reliability is available on the NERC website as amended from time to time

[5] The meaning of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

[6] Market Principles are available on the NERC website as amended from time to time

[7] Results-based Standards see http://www.nerc.com/pa/Stand/Resources/Documents/ResultsBasedStandardGuidance.pdf

b) **Risk-based** - defines actions of entities that reduce a stated risk to the reliability of the Bulk Electric System and can be measured by evaluating a particular product or outcome resulting from the required actions.

c) **Capability-based** - defines capabilities needed to perform reliability functions and can be measured by demonstrating that the capability exists as required.

Each regional standard shall enable or support one or more of the reliability principles[8] as identified in the most recent set posted on the NERC website. Each regional standard shall also be consistent with all of the reliability principles. The intent of the set of NPCC regional standards is to deliver an Adequate Level of Reliability[9] as defined by NERC.

Recognizing that Bulk Electric System reliability and electricity markets are inseparable and mutually interdependent, all regional standards shall be consistent with the most recent set of Market Principles[10] as posted on the NERC website. Consideration of the Market Principles is intended to ensure that regional standards are written such that they achieve their reliability objective without placing undue restrictions or causing adverse impacts on competitive electricity markets.

ELEMENTS OF A REGIONAL STANDARD

A regional standard includes several components designed to work collectively to identify what entities must do to meet their reliability-related obligations as an owner, operator or user of the Bulk Electric System. The components of a NPCC regional standard identified below are based on the NERC Standard Processes Manual (SPM) that was approved by the NERC Board of Trustees at its February 2013 meeting. Future revisions of the NERC SPM will be used at the time of development of a NPCC regional standard if different from the elements listed below.

The only mandatory and enforceable components of a regional standard are the: (1) Applicability, (2) Requirements, and (3) the Effective Dates. The additional components are included in the regional standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to functional entities concerning how compliance will be assessed by the Compliance Enforcement Authority.

The components of a regional standard may include the following:

Title:	A brief, descriptive phrase identifying the topic of the regional standard.
Number:	A unique identification number assigned in accordance with a published classification system to facilitate tracking and reference to the regional standards.
Purpose:	The reliability outcome achieved through compliance with the requirements of the regional standard.
Applicability:	Identifies which entities are assigned reliability requirements; i.e., the specific functional entities and facilities to which the regional standard applies.
Effective Dates:	Identification of the date or pre-conditions determining when each Requirement becomes effective in each jurisdiction.

[8] Reliability Principles are available on the NERC website as amended from time to time
[9] Adequate Level of Reliability is available on the NERC website as amended from time to time
[10] Market Principles are available on the NERC website as amended from time to time

Requirement: An explicit statement that identifies the functional entity responsible, the action or outcome that must be achieved, any conditions achieving the action or outcome, and the reliability-related benefit of the action or outcome. Each requirement shall be a statement for which compliance is mandatory.

Compliance Elements: Elements to aid in the administration of compliance monitoring and enforcement responsibilities.

Measure: Provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.

Violation Risk Factors and Violation Severity Levels: Violation risk factors (VRFs) and violation severity levels (VSLs) are used as factors when determining the size of a penalty or sanction associated with the violation of a requirement in an approved Reliability Standard. Each requirement in each Reliability Standard has an associated VRF and a set of VSLs. VRFs and VSLs are developed by the drafting team, working with NPCC Standards Staff and Compliance Staff, at the same time as the associated Reliability Standard, but are not part of the Reliability Standard. The Board of Directors is responsible for approving VRFs and VSLs.

- Violation Risk Factors
  VRFs identify the potential reliability significance of noncompliance with each requirement. Each requirement is assigned a VRF in accordance with the latest approved set of VRF criteria.
- Violation Severity Levels
  VSLs define the degree to which compliance with a requirement was not achieved. Each requirement shall have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs. Each requirement is assigned one or more VSLs in accordance with the latest approved set of VSL criteria.

Version History: The version history is provided for informational purposes and lists information regarding prior versions of the regional standard.

Variance: As applied to a NPCC regional standard is a Requirement (to be applied in the place of the NPCC region-wide Requirement) that is applicable to a specific geographic area or to a specific set of Registered Entities.

Compliance Enforcement Authority (CEA): The entity that is responsible for assessing performance or outcomes to determine if an entity is compliant with the associated regional standard. The Compliance Enforcement Authority will be NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the ERO regional standards.

Reliability Standard Audit Worksheets (RSAWs)[11] Reliability Standard Audit Worksheets (RSAWs) are developed as companion documents to regional and continent-wide Reliability Standards to facilitate the CEA assessment of a registered entity's compliance with a standard.

[11] While RSAWs are not part of the regional standard, they are developed through collaboration of the drafting team and NPCC Compliance Staff.

Informational Elements: Elements to aid in the implementation of the regional standard.

Application Guidelines:	Guidelines or reference documents to support the implementation of the associated regional standard.
Procedures:	Procedures to support implementation of the associated regional standard.

IV. REGIONAL STANDARDS DEVELOPMENT PROCESS

1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS

NOMINATION, REVISION, CLARIFICATION, OR RETIREMENT OF A STANDARD:

Any member of NPCC or group within the NPCC region shall be allowed to request that a NPCC regional standard be developed, modified, clarified, or retired. Additionally, any person (organization, company, government agency, individual, etc.) who is directly and materially affected by the reliability of the NPCC Bulk Electric System shall be allowed to request that a NPCC regional standard be developed, modified, clarified, or retired. The following section identifies the process roles in the NPCC regional standards process. Refer to Step 2 STANDARD DEVELOPMENT PROCESS STEPS and FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS OVERVIEW for the regional standards development process steps and associated flowchart. Refer to Step 3 STANDARD CLARIFICATION PROCESS STEPS and FIGURE 2: FLOWCHART OF REGIONAL STANDARDS CLARIFICATION PROCESS OVERVIEW for the regional standards clarification process steps and associated flowchart.

PROCESS ROLES AND RESPONSIBILITIES

BOARD OF DIRECTORS

The NPCC Board of Directors (Board) shall consider for adoption regional standards, definitions, variances and clarifications and associated implementation plans that have been processed according to the processes identified in this manual.

DRAFTING TEAM

The drafting team (DT) should strive to achieve a portfolio of performance, risk, and capability-based mandatory reliability requirements that support an effective defense-in-depth strategy. The drafting team develops standards-related regional products as directed by the NPCC RSC and within the scope of an approved Regional Standard Authorization Request (RSAR) or a Clarification Request (CR). The product that is developed is typically a new or revised regional standard, but could also be a definition, a reference document, a set of Violation Risk Factors, a set of Violation Severity levels, or the team could be appointed to assist an author in refining a Regional Standard Authorization Request (RSAR). The drafting team also works collaboratively with NPCC Compliance Staff to develop Reliability Standard Audit Worksheets (RSAWs) at the same time regional standards are developed. The drafting team shall remain in place until such time as the NERC Board of Trustees adopts the regional standard.

MANAGER OF RELIABILITY STANDARDS

The NPCC Manager of Reliability Standards has the overall responsibility for managing the NPCC regional standards processes in accordance with this manual. As used herein, the NPCC Manager of Reliability Standards will be the NPCC Manager of Reliability Standards or his/her designee.

NPCC MEMBERS

NPCC members may participate in the comment and ballot periods associated with the development and industry approval of regional standards. The ballot body is comprised of all

entities or individuals that qualify for one of the stakeholder sectors within NPCC as stated in the most recently approved NPCC Bylaws. All General and Full Members of NPCC can participate in the balloting of regional standards. Any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards.

NON-NPCC MEMBERS

Any entity or person that is neither a General nor Full Member of NPCC is not eligible to participate in the ballot body voting on a regional standard. However, any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards. Subject Matter Experts (SMEs), regardless of NPCC membership status, are encouraged to participate in comment periods for regional standards.

NPCC STANDARDS STAFF

The Standards Staff is responsible for assisting the NPCC Manager of Reliability Standards and the RSC in administering the NPCC regional standards processes in accordance with this manual.

NPCC COMMITTEES, TASK FORCES AND WORKING GROUPS

The Committees, Task Forces and Working Groups within NPCC serve an active role in the standards process. Activities performed by these groups include, but are not limited to, the following:

- Identify the need for new or modified regional standards
- Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs)
- Develop comments (views and objections) to standards actions
- Participate in NPCC Standard drafting
- Dispensation of Clarification Requests (CRs)
- Provide technical oversight in response to changing industry conditions and ERO Requirements
- Conduct Field Tests, as required

REGIONAL STANDARDS COMMITTEE (RSC)

The NPCC Regional Standards Committee (RSC), a committee of the NPCC Board of Directors, is charged with oversight of all drafting team activities and managing the NPCC regional standards development process in accordance with this manual.

The RSC is responsible for maintenance of the Regional Standard Processes Manual (RSPM), including the endorsement of RSPM revisions for NPCC Board review and approval.

RELIABILITY COORDINATING COMMITTEE (RCC)

The Reliability Coordinating Committee (RCC) supports the standards development process through the assignment of NPCC Task Forces to serve as technical resources for: (1) staffing drafting teams, and (2) performing a technical advisory role in the regional standards process through comments, recommendations and technical justifications.

REQUESTER

Any individual representing an organization (entity, company, government agency, etc.) that is directly and materially affected by the reliability of the Bulk Electric System within the NPCC

geographical area may request a regional standard be developed or an existing regional standard be modified, clarified, or deleted.

QUALITY REVIEW TEAM

The NPCC Standards Staff shall coordinate a quality review of the "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, whether the regional standard is clear and enforceable as written and the VRFs and VSLs are developed according to NERC and FERC guidelines. The Quality Review Team may be comprised of legal and compliance representatives, a technical writer, and NPCC Standards Staff. It will not involve individuals who participated on the drafting team of the standard undergoing the Quality Review.

2. STANDARD DEVELOPMENT PROCESS STEPS

STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE

A Regional Standard Authorization Request[12] (RSAR) is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified regional standards or the benefit of retiring one or more approved regional standards.

A RSAR shall be used to seek approval and initiate the development, modification or retirement of a NPCC regional standard. A RSAR is not used to seek a Clarification Request (CR) of a NPCC regional standard. The initiation and handling of a CR is covered in Step 3 STANDARD CLARIFICATION PROCESS STEPS, of this manual.

Any individual representing an organization which is directly or materially impacted by the operation of the Bulk Electric System within the geographical footprint of NPCC may request, via a submittal of a RSAR to the NPCC Manager of Reliability Standards, the development, modification, or deletion of a NPCC regional standard. The individual completing the form is referred to herein as the Requester.

STEP 2.1.A. REQUESTER ACTIONS

> *Note: The NPCC Manager of Reliability Standards will assist the Requester, as necessary, to ensure all required information is submitted on the RSAR.*

The Requester shall complete a RSAR form in accordance with the guidance provided in APPENDIX A: RSAR COMPLETION GUIDELINES.

The Requester shall submit the completed RSAR to the NPCC Manager of Reliability Standards, via npccstandard@npcc.org, for processing.

STEP 2.1.B. NPCC MANAGER OF RELIABILITY STANDARDS ACTIONS

The NPCC Manager of Reliability Standards shall review the submitted RSAR and verify that the submitted form has been adequately completed. Within fifteen (15) calendar days[13] of receipt of the submitted RSAR, the NPCC Manager of Reliability Standards will electronically acknowledge

[12] The RSAR is located on the NPCC website under Standards – Regional Standards General

[13] Time periods specified in this manual may be extended as deemed appropriate by NPCC Staff. When business days are specified, this provision could be used to take into account differing Canadian and US holiday schedules. When calendar days are specified, this provision could be used to take into account due dates that fall on a weekend.

receipt of the RSAR. If, at that time, the NPCC Manager of Reliability Standards finds the RSAR to be deficient, the Requester will be contacted to determine how to proceed.

Within ten (10) calendar days of the receipt of an adequately completed RSAR, the NPCC Manager of Reliability Standards shall forward the properly completed RSAR to the NPCC Regional Standards Committee (RSC) for its review and processing. Included in the transmittal of the RSAR to the RSC, the NPCC Manager of Reliability Standards shall include a statement indicating the applicability of the NPCC Cost Effectiveness Analysis Procedure (CEAP) for the proposed change.

STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS

Note:	*The RSC shall meet to review all pending RSARs. The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for RSC action more than 60 calendar days from the date of receipt by the RSC.*

The RSC shall review the RSAR and take one of the following actions:

- Remand the RSAR back to the NPCC Manager of Reliability Standards for additional work. In this case, the NPCC Manager of Reliability Standards shall work with the Requester to provide additional information or clarification for the RSAR as specified by the RSC.
- Reject the RSAR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the Requester within ten (10) calendar days of the rejection decision.

Note:	*Before the RSC can accept a RSAR for a new or modified standard the applicable CEAP process steps shall be completed.*

- Accept the RSAR.
  - If a new or modified standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to develop or modify a regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR.
  - If the retirement of an existing regional standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to retire an existing regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR. The process to retire an existing regional standard is included in Step 6 RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD.

STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD

A RSAR that has been accepted by the RSC shall, within ten (10) calendar days of the acceptance of the RSAR, be submitted by the NPCC Manager of Reliability Standards to the NPCC Reliability Coordinating Committee (RCC). The RCC shall, within sixty (60) calendar days, assign the development of the regional standard to a NPCC Task Force, and notify the NPCC Manager of Reliability Standards of its decision within ten (10) calendar days.

After receipt of the notification of drafting team assignment, the NPCC Manager of Reliability Standards shall oversee solicitation and recommendation of a list of additional qualified[14] candidates over and above the appropriate NPCC Task Force members, for appointment to the drafting team. The Requester and a NPCC Compliance Staff person will be included on the drafting team. Within sixty (60) calendar days of the drafting team assignment notification from the RCC, the NPCC Manager of Reliability Standards shall submit the list of the entire drafting team membership to the RSC for acceptance. The RSC may accept the recommendations of the NPCC Manager of Reliability Standards as presented or revise the recommendations as necessary.

Upon acceptance of the drafting team slate, the RSC shall provide a target date on which the drafting team is expected to have ready a completed draft regional standard and associated supporting documentation available for consideration by the NPCC membership. Additionally, the RSC shall provide the drafting team with any preliminary development products including, but not limited to, a draft standard, comments, and related white papers.

The RSC shall designate one of its members to actively monitor and assist NPCC staff in the oversight of drafting team milestones and deadlines, and extend or expedite milestones and deadlines, as appropriate, acting as a liaison between the drafting team and the RSC to help resolving any issues.

STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS

Prior to beginning work on the development of a new or revised regional standard and the associated supporting documentation, the drafting team should develop a work plan for completing the regional standard development work, including the establishment of milestones for completing critical elements of the work in sufficient detail to ensure that the drafting team will meet the target date established by the RSC, or the drafting team shall propose an alternative date. This work plan must be submitted to the RSC for its concurrence. When a drafting team begins its work, it shall regularly (at least quarterly) report progress against that aforementioned work plan to the NPCC Manager of Reliability Standards for presentation to the RSC.

> *Note: During the regional standards development, the drafting team will deliberate on whether the requirements in the regional standard are developed enough to begin the Cost Effectiveness Analysis (CEA) of the NPCC Cost Effectiveness Analysis Procedure (CEAP). When appropriate, the drafting team shall request that the RSC initiate the second phase (CEA) of the CEAP process.*

The drafting team shall create and manage its work structure (e.g., sub-teams) and meeting schedule (face-to-face as well as electronic meetings), as necessary, to meet the milestone dates and project deliverables outlined in the work plan.

The work products of the drafting team should consist of the following

- A draft regional standard consistent with the RSAR on which it was based
- An implementation plan, including the nature, extent and duration of field-testing, if any
- Identification of any existing regional standard and NPCC criteria that will be deleted, in part or whole, or otherwise impacted by the implementation of the draft regional standard

[14] Refer to Appendix B: Selection of Drafting Team Members

- Technical reports, white papers and/or work papers that provide technical justification for the draft regional standard under consideration
- Reliability Standard Audit Worksheet (RSAW) collaboratively developed by the drafting team and NPCC Compliance Staff

Any proposed changes to definitions in existing regional standards should be sent to the appropriate Task Force (TF) for consideration of the impact to the standard. If necessary, the TF can produce a RSAR.

NPCC Standards Staff can assist in the drafting of the regional standard including compliance measures, process and elements. The drafting of measures and compliance administration aspects of the standard will be coordinated with the NPCC Compliance Staff.

The drafting team shall submit the initial and subsequent interim drafts of the regional standard and associated documents to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post documents for comment.

STEP 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS

Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.

STEP 2.4.A. COMMENT PERIOD

Note: For Final Comment Period skip this step and proceed to STEP 2.4.B. FINAL COMMENT PERIOD.

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the draft of the regional standard on the NPCC website, along with a draft implementation plan and available supporting documents, for a forty-five (45) calendar day comment period. The NPCC Manager of Reliability Standards shall also notify NERC to process the draft document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the draft regional standard and associated documents and provide all comments to the drafting team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the drafting team shall convene and consider changes to the draft Standard, the implementation plan and/or supporting technical documents based upon comments received. All submitted comments shall be addressed, and each commenter shall be advised of the disposition, with reasons, of their comments. The NPCC Manager of Reliability Standards shall publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

Based on the comments received, the drafting team may elect to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the draft regional standard, the implementation plan and/or supporting technical documents.
- Recommend that the RSC authorize Field Testing of the draft regional standard. Upon completion of the Field Test, return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD

AND ASSOCIATED DOCUMENTS to revise the draft regional standard based on insights learned during the Field Test.

- Obtain RSC concurrence to post documents for Final Comment Period and request that the RSC initiate the second phase (CEA) of the CEAP process

STEP 2.4.B. FINAL COMMENT PERIOD

The NPCC Standards Staff shall coordinate a Quality Review of "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, whether the regional standard is clear and enforceable as written and the VRFs and VSLs are developed according to NERC and FERC guidelines. Upon Completion of the Quality Review, including resolution of comments, the drafting team shall submit the regional standard to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post these documents for comment.

As authorized by the RSC, the NPCC Standards Staff shall post the "final draft" of the regional standard on the NPCC website, along with the implementation plan, supporting documents and the Cost Effectiveness Analysis (CEA) survey[15] for a forty-five (45) calendar day comment period. NPCC Standards Staff shall also notify NERC to process the proposed final document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard and associated documents and provide all comments to the drafting team for consideration.

In addition, the RSC, pursuant with the requirements of the Cost Effectiveness Analysis Procedure (CEAP), will use the responses to the posted CEA survey to develop a recommendation based on the cost effectiveness of the proposed regional standard.

The NPCC Task Forces (TFs) or Working Groups (WGs) may develop recommendations for submittal to the RSC. Following the RSC deliberations to determine a course of action, the RSC will communicate to the drafting team to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the Standard to address the results of the CEAP
- Accept the Standard "as is" to move forward through the remainder of the process
- Hold the Standard in abeyance until such time as additional guidance can be provided regarding whether or how to continue
- Decide not to pursue the development of certain requirements or the entire Standard due to cost effectiveness considerations

Upon Completion of the final comment period the drafting team shall submit the proposed regional standard, along with any supporting materials, consideration of comments and field test results, to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post the regional standard for ballot and concurrently provide an information copy to the RCC.

[15] In accordance to the Cost Effectiveness Analysis Procedure (CEAP) the Cost Effectiveness Analysis (CEA) survey may be assigned directly to NPCC Task Forces (TFs) or Working Groups (WGs) in addition to the posting process.

The NPCC Manager of Reliability Standards shall also publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS

> *Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.*

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed regional standard on the NPCC website, along with supporting documentation [16] (e.g., implementation plan, consideration of comments, technical reports, white papers and any field test results), for a thirty (30) day pre-ballot review period and a subsequent ten (10) day ballot period. The ten (10) day ballot period will commence immediately following the pre-ballot review period. In the event that a quorum exists for purposes of an electronic vote but the ballot purpose has not been resolved, NPCC may continue to solicit additional responses in order to resolve the matter by electronic voting. In the event that quorum has not been achieved for purposes of an electronic vote, NPCC may continue to solicit electronic ballots, including abstentions, to obtain quorum and resolve the matter.

At the time the regional standard is posted for ballot, the NPCC Manager of Reliability Standards shall also notify NERC to process the proposed regional standard in accordance with NERC's regional standards review procedure, as applicable.

During the ballot period, the NPCC Members of the ballot body can cast their vote as follows:

- Affirmative, with or without comments
- Negative with comments
- Abstain

In accordance with the NPCC Bylaws, a quorum and receipt of a two-thirds (2/3) affirmative majority of the weighted sector votes is required for a ballot to pass.

The NPCC Manager of Reliability Standards shall post the final outcome of the ballot process on the NPCC website.

STEP 2.5.A. BALLOT DOES NOT RECEIVE 2/3 AFFIRMATIVE VOTE

If a ballot fails to achieve the 2/3 majority vote the NPCC Manager of Reliability Standards may:

- Direct the drafting team to respond to ballot comments and return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard. The consideration of comments from prior ballot will be included with the re-posting.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.
- Pursue the discontinuance of the regional standard development by soliciting the Requester to withdraw the RSAR or by soliciting the RSC to reject the RSAR pursuant with STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS. The NPCC Manager of

[16] The ballot posting is for the regional standard, definition, variance or clarification. Supporting documentation is included for information only and is not balloted.

Reliability Standards, in the event of a discontinuance of the development of a regional standard, shall post a notice of the discontinuance and will post and archive all comments submitted during the process for future consideration, if required. The NPCC Manager of Reliability Standards will also notify NERC to process the proposed regional standard in accordance with NERC's regional standards review procedure, as applicable.

STEP 2.5.B. BALLOT RECEIVES ≥ TWO-THIRDS (2/3) AFFIRMATIVE VOTE

A ballot that achieved two-thirds or greater affirmative vote has successfully passed. However, negative votes with comments should still be reconciled. If there is at least one negative vote with comments proceed to STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT". If there was not any negative vote with comments proceed to STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT".

STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT"

Following the conclusion of the NPCC ballot period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard and provide all comments to the drafting team for consideration. The drafting team shall review all negative votes with comments and elect to:

- Recommend to the RSC to accept the regional standard "as is" and seek RSC endorsement to move forward through the remainder of the process. Upon receiving RSC endorsement to proceed, the regional standard and associated documents, approved by the NPCC ballot body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval. If comments that were received during balloting should be considered in future revisions to the regional standard then the NPCC Manager of Reliability Standards should log comments in an issues database.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.
- Respond to ballot comments and recommend to the RSC endorse the return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard. The NPCC Manager of Reliability Standards should include the consideration of comments from the prior ballot with the re-posting.

STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT"

Regional standard and associated documents, approved by the NPCC ballot body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval.

STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL

Following approval by the NPCC Members, regional standards require review and approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the regional standard as presented.
- Approve the regional standard with comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive revisions to the standard.]
- Remand the regional standard back to the RSC and the drafting team to address their concerns. The RSC / drafting team can address the BOD comments and re-submit for BOD

approval or return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.

STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL

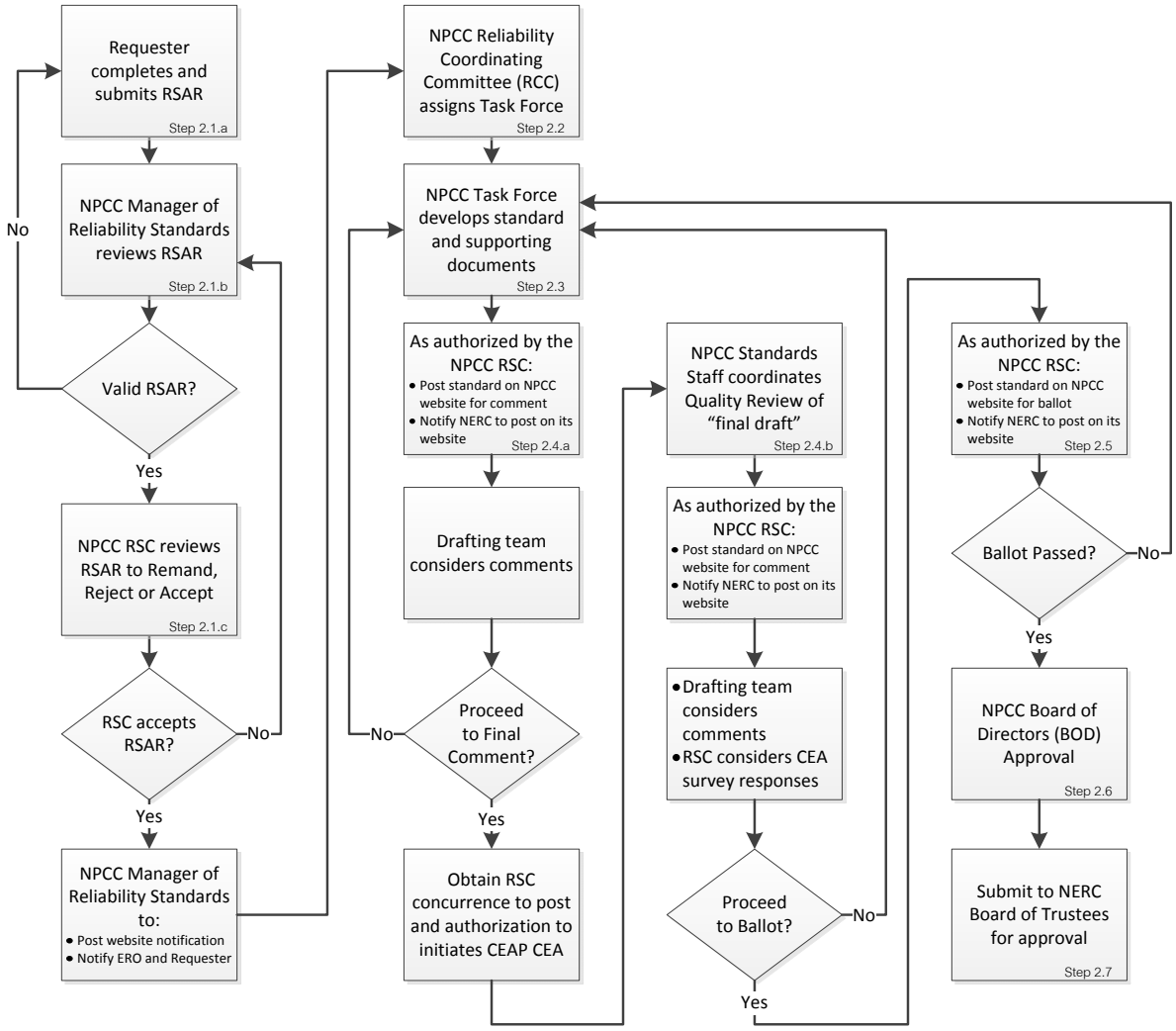
Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the regional standard to NERC, as the Electric Reliability Organization, for approval and subsequent filing with FERC and the applicable Canadian Provincial regulatory and/or governmental authorities for adoption.

STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD

Following the approval of a NPCC regional standard by FERC and the applicable Canadian Provincial regulatory and/or governmental authorities, all users, owners, and operators of the Bulk Electric System in the NPCC geographic area are required to comply with the standard as of its enforcement date.

ERO approved Reliability Standards (both continent-wide and regional) are included in both the NERC and NPCC Compliance Monitoring and Enforcement Programs (CMEPs).

FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS OVERVIEW



3. STANDARD CLARIFICATION PROCESS STEPS

This section applies to NPCC regional standards that have been approved[17] and are currently enforceable or have a future enforcement date. A clarification request is not permitted for regional standards under development. For regional standards under development, an explanation of a requirement or its meaning can be sought during a comment period. Refer to Step 2, STANDARD DEVELOPMENT PROCESS STEPS of this manual for details on the comment process for a standard under development.

STEP 3.1: REGIONAL STANDARDS CLARIFICATION REQUEST (CR)

Any member of NPCC or group within the NPCC region shall be allowed to submit a Clarification Request (CR) for a NPCC regional standard.

Additionally, any person (organization, company, government agency, individual, etc.) who is directly and materially affected by the reliability of the NPCC Bulk Electric System shall be allowed to submit a Clarification Request (CR) for a NPCC regional standard.

> *Note: A valid Clarification Request is one that seeks additional clarity about one or more requirements in an approved regional standard, but does not request approval as to how to comply with any requirements of the standard.*

The Requester should submit a Clarification Request[18] (CR) for a NPCC regional standard directly to the NPCC Manager of Reliability Standards, via npccstandard@npcc.org, for processing. Alternatively, the Requester can submit a Request for Interpretation (RFI) of a NPCC regional standard under the NERC process for developing an interpretation[19] to the NERC Reliability Standards Staff explaining the clarification required, the specific circumstances surrounding the request, and the impact of not having the clarification provided. A copy of the completed RFI form should also be sent to the NPCC Manager of Reliability Standards.

NERC Reliability Standards Staff will refer the RFI to NPCC and delegate its resolution to NPCC. NPCC will process the NERC delegation pursuant with the NPCC Clarification Request (CR) process described herein.

STEP 3.2: REVIEW AND VALIDATION OF CLARIFICATION REQUEST (CR)

Upon receipt of a Clarification Request (CR) for a NPCC regional standard, the NPCC Manager of Reliability Standards shall review the CR to determine whether:

- It meets the requirements for a valid Clarification Request
- A compliance process or approach could be used in lieu of a clarification

The NPCC Manager of Reliability Standards will utilize, as necessary, the NPCC Standards Staff, NPCC Compliance and Legal Staffs when determining the validity of the CR. Based on this review, the NPCC Manager of Reliability Standards will recommend to the RSC whether to accept or reject the CR. The recommendation to the RSC should be made within thirty (30) calendar days of the receipt of the CR.

[17] Approval is granted by FERC and the Canadian Provincial regulatory and/or governmental authorities, as applicable.
[18] The NPCC Clarification Request form is included as Appendix D
[19] The *Request for Interpretation* form is posted under Resource Documents on the NERC Standards webpage.

The following examples identify situations that may warrant a recommendation from the NPCC Manager of Reliability Standards to reject the CR:

- Requests approval of a particular compliance approach
- Identifies a gap or perceived weakness in the approved regional standard (Requester should be redirected to initiate a RSAR rather than a CR)
- Where an issue can be addressed by an active (regional or continent-wide) standard drafting team
- Where an issue can be better addressed by a compliance process or approach
- Where it requests clarification of any element of a regional standard other than a requirement
- Where a question has already been addressed in the record
- Where the clarification identifies an issue and proposes the development of a new or modified regional or continent-wide standard (such issues should be addressed via submission of a RSAR or SAR)
- Where a clarification seeks to expand the scope of a regional standard
- Where the requirement of the regional standard is clear

STEP 3.3: NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS

The RSC shall review the CR along with the recommendation from the NPCC Manager of Reliability Standards and take one of the following actions:

- Reject the CR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the CR to the entity requesting the clarification within ten (10) calendar days of the decision to reject.
- Accept the CR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then: 1) post notification on the NPCC website of the intent to develop a clarification; 2) notify the NPCC Reliability Coordinating Committee (RCC) of the need to assign the resolution of the CR to one or more Task Forces (if more than one Task Force is assigned, one of them shall be assigned the lead role); and 3) notify the Requester of the acceptance of the CR. The notifications shall be made within ten (10) calendar days of the acceptance of the CR.

STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO CR

A CR that has been accepted by the RSC shall be assigned by the RCC to the responsible NPCC Task Force to make up the clarification drafting team (CDT) and develop the CR response.

STEP 3.5: DEVELOPMENT OF RESPONSE TO CR

> *Note: A valid clarification response provides additional clarity about one or more requirements, but does not expand on any requirement and does not explain how to comply with any requirement.*

Within sixty (60) calendar days from the receipt of being assigned to respond to a CR, the CDT shall submit a proposed clarification response to the NPCC Manager of Reliability Standards. Upon receipt of the proposed clarification response from the CDT, the NPCC Manager of

Reliability Standards shall present the response to the RSC to obtain concurrence to post the proposed response for comment.

Along with the proposed clarification response, the drafting team shall also develop and submit a set of questions to be included in the comment form, for approval by the RSC.

If the RSC concurrence is not received, the drafting team will continue to refine the clarification response.

Note: There are no limits to the number of public comment periods that can be conducted to result in a clear and concise clarification of a regional standard requirement.

STEP 3.6: POSTING CR FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed clarification response on the NPCC website for a forty-five (45) calendar day comment period.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the proposed clarification response and provide all comments to the drafting team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the drafting team shall convene and consider changes to the proposed clarification response based upon comments received. All submitted comments shall be addressed, which may be in the form of a summary response addressing each of the issues raised in comments received. The NPCC Manager of Reliability Standards shall publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

Based on the comments received, the drafting team may elect to:

- Return to STEP 3.5: DEVELOPMENT OF RESPONSE TO CR to revise the proposed clarification response.
- Accept the proposed clarification response "as is" to move forward through the remainder of the process.

Upon acceptance of the proposed clarification response "as is," the drafting team shall submit the proposed clarification response to the NPCC Manager of Reliability Standards to obtain RSC endorsement to the submitted CR response.

STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF CR

Upon receipt of the CR response from the NPCC Manager of Reliability Standards, the RSC shall elect to:

- Endorse the proposed clarification response and direct the NPCC Assistant Vice President Standards to forward the CR to the NPCC Board of Directors for final Regional approval; or
- Direct the drafting team to return to STEP 3.5: DEVELOPMENT OF RESPONSE TO CR to revise the proposed clarification response

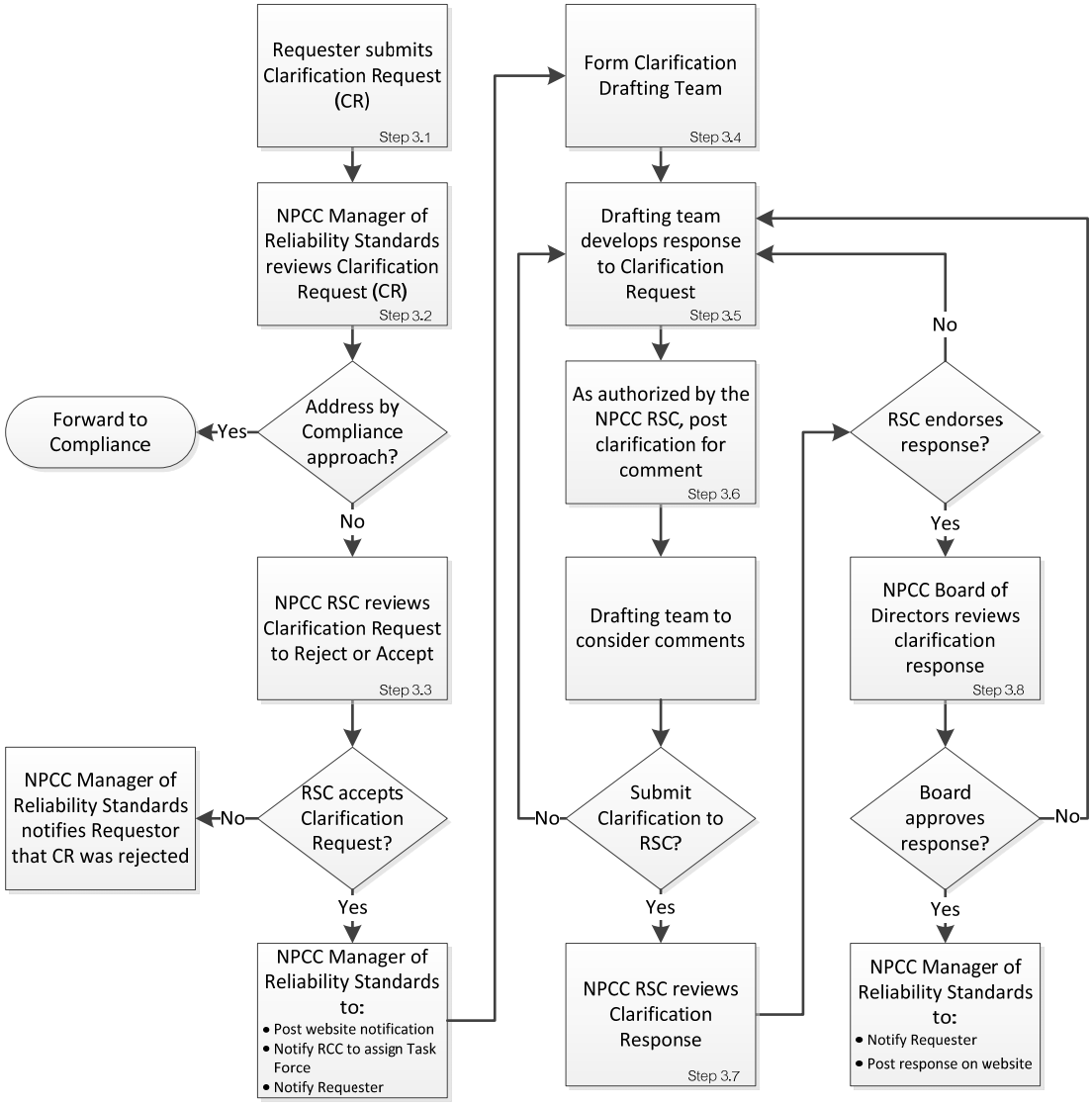
STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF CR

Following endorsement by the RSC, clarification responses require review and approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the clarification response as presented
- Approve the clarification response with comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive revisions to the clarification response.]
- Remand the clarification response back to the RSC and the drafting team to address their concerns

Upon receipt of Board approval, the NPCC Manager of Reliability Standards shall notify the Requestor and post the approved clarification on the NPCC website.

FIGURE 2: FLOWCHART OF REGIONAL STANDARDS CLARIFICATION PROCESS OVERVIEW



4. DISCONTINUANCE OF REGIONAL STANDARD DEVELOPMENT

The term "discontinuance" as used herein refers to terminating the standard development process after RSAR approval but prior to posting a regional standard for industry ballot. From time to time the need or rationale for a regional standard may change thereby necessitating the curtailment

of the regional standard development. Upon notification or determination that a regional standard under development should be considered for discontinuance due to a perceived change in the need for the standard, the NPCC Manager of Reliability Standards will submit the recommendation for discontinuance to the RSC for approval.

5. WITHDRAWAL OF A REGIONAL STANDARD PENDING APPROVAL

The term "withdrawal" as used herein, refers to the revocation of a request for approval of a regional standard, variance, clarification or definition that has been approved by the NPCC Board of Directors and has not been filed with Applicable Governmental Authorities or has been filed but not yet approved by Applicable Governmental Authorities. The RSC may withdraw a regional standard, variance, clarification or definition for good cause subject to approval by the NPCC Board of Directors. Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards will notify NERC Staff to petition the Applicable Governmental Authorities, as necessary, to allow for withdrawal in the case that the regional standard has been filed.

6. RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD

The term "retirement" refers to the discontinuation of a regional standard in whole, certain requirements within a regional standard, a variance, clarification or definition that: 1) has been approved by Applicable Governmental Authorities and 2) is not being superseded by or merged into a new or revised regional standard, clarification or definition.

Upon identification of a need for retirement, a RSAR containing the proposal of the retirement will be handled in accordance with the STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE. The proposal shall include the rationale for the retirement and a statement regarding the impact of retirement on the reliability of the Bulk Electric System. Upon approval by the NPCC Members and the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the request for retirement to NERC, as the Electric Reliability Organization, for approval and to subsequently petition the Applicable Governmental Authorities to allow for retirement.

7. APPROVAL OF PROCESS WAIVER

While it is NPCC's intent to adhere to this manual under normal circumstances, NPCC may need to develop a new or modified regional standard, implementation plan, variance, clarification or definition under extenuating circumstances. Extenuating circumstances may include, but not be limited to, specific time constraint imposed by a regulatory body and urgent reliability issue that requires expedited handling outside of the normal regional Reliability Standards process.

The RSC, by two-thirds (2/3) majority vote, may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:

- Where necessary to meet regulatory deadlines
- Where necessary to address an urgent reliability issue identified by regulatory and/or governmental authorities, including response to national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber-attack on the Bulk Electric System
- Where necessary to meet deadlines imposed by the NPCC Board of Directors

- Where the RSC determines that a revision to a proposed regional standard, implementation plan, variance, clarification or definition has already been vetted by the industry through the standards development process or is so insubstantial that developing the revision through the processes contained in this manual will add significant time delay without any corresponding benefit.

In no circumstances shall this provision be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

A waiver request may be submitted to the RSC by any entity or individual, including NPCC committees or subgroups and NPCC Standards Staff. Prior to consideration of any waiver request, the NPCC Manager of Reliability Standards must provide notification to stakeholders at least five (5) business days prior to RSC consideration and action. Posting the waiver request on the NPCC website satisfies the notification provision.

Action on the waiver request will be included in the minutes of the RSC. Following the approval of the RSC to waive any provision of the regional Reliability Standards process, the Assistant Vice President Standards shall report the exercise of this waiver provision to the NPCC Board of Directors prior to adoption of the related Reliability Standard, clarification, definition or variance. Actions taken pursuant to an approved waiver request will be posted on the NPCC Standards webpage.

8. PROCESS FOR CORRECTING ERRATA

From time to time, an error may be discovered in a regional standard after it has received final ballot approval by the NPCC ballot body. Such errors may be corrected by the RSC without re-balloting if the RSC agrees that the correction of the error does not change the scope or intent of the associated regional standard, and agrees that the correction has no material impact on the end users of the regional standard.

If the regional standard containing errata is pending approval by the NPCC Board of Directors, the corrected regional standard shall be presented to the NPCC Board for approval in lieu of the regional standard approved by the NPCC ballot body.

If a regional standard containing errata had received prior approval by the NPCC Board of Directors, the corrected regional standard shall be presented to the NPCC Board for approval. Upon approval by the Board, the corrected regional standard will be filed for approval by NERC.

The NPCC Board of Directors has resolved to concurrently approve any errata approved by the RSC associated with a regional standard that has received prior approval by the NPCC Board.

9. APPEALS

Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the approval, revision, reaffirmation, or withdrawal of a regional standard (appellant) shall have the right to appeal. This appeals process applies only to the regional standards process as defined in this manual.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within thirty (30) calendar days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

LEVEL 1 APPEAL

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the NPCC Manager of Reliability Standards that describes the substantive or procedural action or inaction associated with a Reliability Standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary NPCC Standards Staff and Committee resources, the NPCC Manager of Reliability Standards shall prepare a written response addressed to the appellant as soon as practical, but not more than forty-five (45) calendar days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response will be made a part of the public record associated with the standard and posted with the standard.

LEVEL 2 APPEAL

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the NPCC Manager of Reliability Standards, the NPCC Board of Directors shall appoint a five member panel to serve as a Level 2 Appeals Panel.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The NPCC Manager of Reliability Standards shall post the complaint and other relevant materials and provide at least a thirty (30) calendar day notice of the meeting of the Level 2 Appeals Panel.

In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC with a statement of the issues and facts in regard to which unfair and/or inequitable action was taken, or which fair and/or equitable action was not taken. The panel may find for or against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise, approve, disapprove, or adopt a Reliability Standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the NPCC Board of Directors for consideration at the time the Board decides whether to adopt a particular Reliability Standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than thirty (30) calendar days after the announcement of the vote on the standard in question.

APPENDIX A: RSAR COMPLETION GUIDELINES

The Requester shall complete a RSAR form in accordance with the guidance provided below.

The RSAR, at a minimum, shall contain information in the required fields in order to be qualified for consideration. The NPCC Manager of Reliability Standards will assist the Requester to ensure all required information is submitted on the RSAR.

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC Manager of Reliability Standards, at npccstandard@npcc.org. The NPCC Manager of Reliability Standards shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:	***[Required Field]***
Request Date:	***[Required Field]***

RSAR Requester Information

Name:	***[Required Field]***	**RSAR Type (Check box for one of these selections.)**	
Company:	***[Required Field]***	☐	New Standard
Telephone:	***[Required Field]***	☐	Revision to Existing Standard
Fax:		☐	Withdrawal of Existing Standard
Email:	***[Required Field]***	☐	Urgent Action

Purpose: (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.) ***[Required Field]***
Industry Need: (Provide a detailed statement justifying the need for the proposed standard, along with a technical justification and any supporting documentation.) ***[Required Field -- must include technical justification (relevant studies, documentation, etc.) for a new standard or revision to an existing standard.]***

Brief Description: (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.)

[Required Field]

Reliability Functions *[Required Field]*

The Standard will Apply to the Following Functions (Check all applicable boxes.)		
☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission Operator	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.

☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected Bulk Electric System 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 System 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 System 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 System 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 System.
☐	6. Personnel responsible for planning and operating interconnected Bulk Electric System shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected Bulk Electric System shall be assessed, monitored, and maintained on a wide-area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
Recognizing that reliability is an Common Attribute of a robust North American economy:	
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	

4. A reliability 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 a standard based on this description.) ***[Required Field – Provide: 1) Necessary information to assist the drafting team (which is to include relevant study results and documentation), to the extent feasible, to allow them to draft the standard, 2) Any existing known cross references to NPCC or NERC documents and 3) Technical background for the RSAR to properly address the need for the standard.]***

Related Standards *[Required Field, to extent known]*

Standard No.	Explanation

Related SARs or RSARs *[Required Field, to extent known]*

SAR ID	Explanation

APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS

A regional standard drafting team shall be comprised of Subject Matter Experts (SMEs) from NPCC Task Forces and Working Groups as determined by the RCC, and from industry. The guidelines provided herein primarily address overall team requirements and more specifically those of a SME.

Formal membership on a drafting team should be reserved only for those individuals who intend to work consistently, diligently, and professionally on what is required to be done for a regional standard. Drafting team members are expected to contribute meaningfully to the ongoing development of the standard.

Drafting Team members must be:

- Committed to participating in scheduled drafting team meetings, teleconferences, as well as industry outreach (e.g., workshops and webinars)
- Willing to lead teams / sub-teams, as necessary
- Champions for standard development and promoters of the approval of the standard
- Open to consider the comments of others and provide constructive feedback

Subject Matter Experts should possess the necessary expertise and knowledge regarding the topic of the standard. The SMEs should represent a cross section of the registered entities applicable to the standard under development as well as geographical areas within the NPCC footprint.

Industry stakeholders may nominate themselves for consideration by the NPCC Regional Standards Committee (RSC) for the specific drafting team vacancies by completing the following drafting team Self Nomination form and submitting it to NPCC Manager of Reliability Standards, at npccstandard@npcc.org.

Nomination Form for NPCC [Name of drafting team] Drafting Team

Please return this form as soon as possible. If you have any questions, please contact the NPCC Standards Staff at npccstandard@npcc.org.

By submitting the following information you are indicating your willingness and agreement to actively participate in the drafting team meetings if appointed to the drafting team by the NPCC Regional Standards Committee (RSC). This means that if you are appointed to the DT you are expected to attend all (or at least the vast majority) of the face-to-face DT meetings as well as participate in all the DT meetings held via conference calls. Failure to do so shall result in your removal from the DT.

Name:	
Organization:	
Address:	
Telephone:	

E-mail:	

Please briefly describe your experience and qualifications to serve on the requested drafting team.

If you are currently a member of any NERC or Regional drafting teams, please list each team here.

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any drafting team please identify the team(s).

☐ No prior NERC or Regional SAR or standard drafting team experience.

☐ Prior experience on the following team(s):

Select each NERC Region that you represent:	Select each Industry Segment that you represent:	
☐ ERCOT ☐ FRCC ☐ MRO ☐ NPCC ☐ RFC ☐ SERC ☐ SPP ☐ WECC ☐ NA – Not Applicable	☐	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, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities
	☐	NA – Not Applicable

Select each Function[20] in which you have current or prior expertise:

☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

[20] These functions are defined in the NERC Functional Model, which is downloadable from the NERC website.

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group.			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS

NPCC regional standards and the Regional Standard Processes Manual are living documents that will be updated periodically to remain current and viable (e.g., respond to changing conditions, as well as to incorporate lessons learned and process improvements).

MAINTENANCE OF REGIONAL STANDARDS

NPCC regional standards will be posted for open process review by the RSC for possible revision at least once every five (5) years[21] after the first regulatory approval and follow the same process as in the case of a new standard. If no changes are warranted, the Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or retire a regional standard, a Regional Standard Authorization Request shall be prepared by the RSC and submitted in accordance with the NPCC regional standards process. The existing, approved standard subject to revision will remain in effect until such time as the revised version has received FERC or applicable Provincial Governmental Authorities approvals, as appropriate, at which time it will be retired in accordance with any applicable implementation plan associated with the newly approved regional standard.

MAINTENANCE OF THE REGIONAL STANDARDS PROCESS

This NPCC Regional Standards Process will be reviewed for possible revision at least once every five (5) years, or more frequently if needed, and subject to the same procedure as applies to the development of a Regional Standard. All such revisions shall be subject to approval by the NPCC Board of Directors, NERC Board of Trustees, FERC, and may be subject to approval, if required, by Applicable Governmental Authorities in Canada.

[21] More frequent reviews of NPCC regional standards may be required to promptly evaluate new or revised NERC reliability standards to ensure NPCC regional standards remain consistent and more stringent than continent-wide reliability standards.

APPENDIX D: NPCC CLARIFICATION REQUEST

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

Note: A valid clarification request is one that requests additional clarity about one or more requirements in approved NPCC regional standards, but does not request approval as to how to comply with one or more requirements.

When completed, email this form to:
npccstandard@npcc.org
For questions about this form or for assistance in completing the form, call Lee Pedowicz at 212-840-1070.

Request for an Clarification of a Regional Standard	
Date submitted:	
Contact information for person requesting the clarification:	
Name:	
Organization:	
Telephone:	E-mail:
Identify the standard that needs clarification:	
Standard Number (include version number, e.g. PRC-006-NPCC-1):	
Standard Title:	
Identify specifically what requirement needs clarification:	
Requirement Number and Text of Requirement:	
Identify the nature of clarification that is requested: (Check as many as applicable)	
☐ Clarify the required performance ☐ Clarify the conditions under which the performance is required ☐ Clarify which functional entity is responsible for performing an action in a requirement ☐ Clarify the reliability outcome the requirement is intended to produce Please explain the clarification needed:	
Identify the material impact associated with this clarification:	

Identify the material impact to your organization or others, if known, caused by the lack of clarity or an incorrect clarification of this standard.

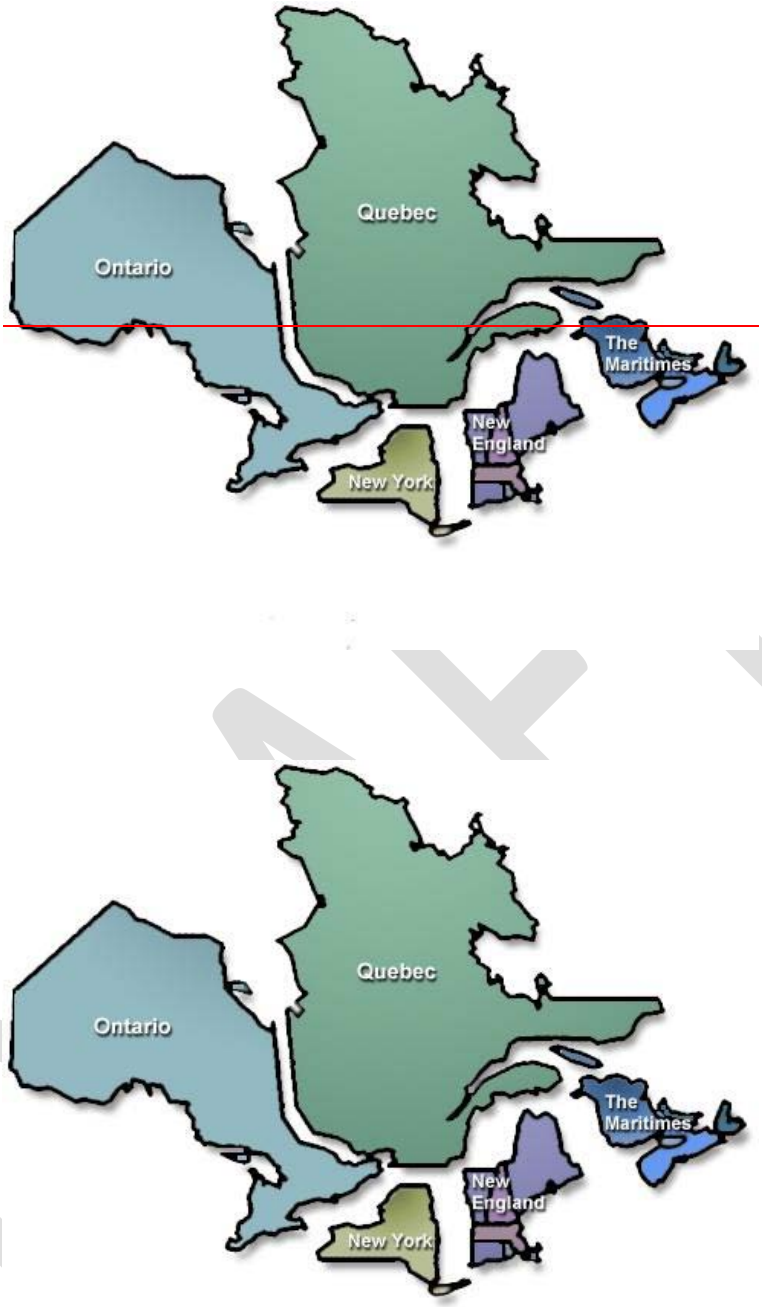
Attachment 2 (Redline)

NPCC, Inc.
NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Northeast Power Coordinating Council, Inc.

Regional ~~Reliability~~ Standards Process Manual (RSPM)

~~Development Procedure~~



Adopted by FERC: XXXX XX, 20XX

Approved by NERC Board of Trustees: XXXX XX, 20XX

Approved by NPCC Board of Directors: XXXX XX, 20XX

~~**September 19, 2007**~~
~~**Approved by NERC BOT October 23, 2007**~~
~~**Adopted by FERC March 21, 2008**~~

DRAFT

~~NPCC~~

DRAFT

Revision History

Version	NPCC Board Of Directors Approval	NERC Board Of Trustees Approval	FERC Approval
0	9/19/07	10/23/07	3/21/08
1	xx/xx/xx	xx/xx/xx	xx/xx/xx

DRAFT

NPCC REGIONAL RELIABILITY STANDARDS PROCESS MANUAL

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 6
II. INTRODUCTION 9
PURPOSE 9
BACKGROUND 9
III. REGIONAL STANDARD CHARACTERISTICS AND ELEMENTS 10
1. CHARACTERISTIC ATTRIBUTES 10
2. ELEMENTS OF A REGIONAL STANDARD 12
TYPES OF RELIABILITY REQUIREMENTS 14
ELEMENTS OF A REGIONAL STANDARD 15
IV. REGIONAL STANDARDS DEVELOPMENT PROCESS 19
1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS 20
NOMINATION, REVISION, INTERPRETATION, OR RETIREMENT OF A STANDARD: 20
PROCESS ROLES AND RESPONSIBILITIES 21
2. STANDARD DEVELOPMENT PROCESS STEPS 24
STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE 24
STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD 26
STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS 26
STEP 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 27
STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS 31
STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL 33
STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL 33
STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD 33
3. STANDARD INTERPRETATION PROCESS STEPS 33
STEP 3.1: REGIONAL STANDARDS REQUEST FOR INTERPRETATION (RFI) 34
STEP 3.2: REVIEW AND VALIDATION OF REQUEST FOR INTERPRETATION (RFI) 34
STEP 3.3: NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS 35
STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO RFI 35
STEP 3.5: DEVELOPMENT OF RESPONSE TO RFI 36
STEP 3.6: POSTING RFI FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 36
STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF RFI 36
STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF RFI 37
4. WITHDRAWAL OF A REGIONAL STANDARD PENDING APPROVAL 37
5. RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD 37
6. APPROVAL OF PROCESS WAIVER 41
7. PROCESS FOR CORRECTING ERRATA 42
8. APPEALS 42
LEVEL 1 APPEAL 42
LEVEL 2 APPEAL 43
APPENDIX A: RSAR COMPLETION GUIDELINES A1
APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS B1
APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS ... C1
MAINTENANCE OF REGIONAL STANDARDS C1
MAINTENANCE OF THE REGIONAL STANDARDS PROCESS C1

DRAFT

I. EXECUTIVE SUMMARY

The NPCC Bylaws state "NPCC shall develop a Regional Reliability Standards Development Procedure

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. REGIONAL RELIABILITY STANDARD DEVELOPMENT PROCEDURE

1. CHARACTERISTIC ATTRIBUTES 2
2. ELEMENTS OF A REGIONAL STANDARD 5
3. TERMS AND FUNCTIONS 8
4. PROCEDURE DESCRIPTION 10
5. FLOWCHART 15
6. ERO AND REGULATORY APPROVALS 16
7. APPEALS 16

III. APPENDIX

A) RSAR FORM 19

DRAFT

~~I. EXECUTIVE SUMMARY~~

~~The purpose of the Northeast Power Coordinating Council, Inc. ("NPCC"), is to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of more stringent and specific regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards pursuant to the execution and implementation of a Regional Delegation Agreement with the Electric Reliability Organization ("ERO") and applicable Canadian Memoranda of Understanding~~ that ~~are backstopped by the Federal Energy Regulatory Commission ("FERC") and~~ provides the design-basis approach to a consensus building process by which NPCC may develop Regional Reliability Standards and Regional Variances to be proposed to the ERO for adoption, under delegated authority by the FERC and the Canadian Provincial regulatory and/or governmental authorities~~. In the development and enforcement of Regional Reliability Standards, NPCC, to the extent possible, facilitates attainment of fair, effective, efficient, and competitive electric markets.~~

~~General Membership in NPCC is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the ERO that has an interest in the reliable operation of the Northeastern North American bulk power system.~~."

The NPCC Regional Reliability Standards Development Procedure ~~describes~~was originally adopted by the ~~procedures, policies~~NPCC Board of Directors on September 19, 2007. The NPCC Reliability Standards Staff in concert with the NPCC Regional Standards Committee (RSC) has completed a revision to the NPCC Regional Reliability Standards Process Manual to incorporate process improvements, provide greater clarity and reflect the new NPCC Cost Effectiveness Analysis Procedure (CEAP).

Key changes addressed in this revision include:

- Expanding the interpretation Section narrative into process steps and including an associated flowchart
- Creating separate sections for: 1) Withdrawal Of A Regional Standard Pending Approval; 2) Retirement Of An Approved NPCC Regional Standard; and 3) Approval Of Process Waiver; 4) Process For Correcting Errata
- Recognizing the new NPCC Cost Effectiveness Analysis Procedure (CEAP)
- Identifying the Reliability Standard Audit Worksheet (RSAW) as a companion document to a regional standard that needs to be collaboratively developed by the Drafting Team and NPCC Compliance Staff
- Creating three new appendices: 1) Appendix A: Regional Standard Authorization Request (RSAR) Completion Guidelines and Form; 2) Appendix B: Selection Of Drafting Team Members and Nomination Form; and 3) Appendix C: Maintenance Of Regional Standards and Process

In addressing areas for improvement in the NPCC Regional Reliability Standards Development Procedure, recent improvements made to the NERC Standards Process Manual (e.g., Standards Process Input Group (SPIG) recommendations) as well as the manuals of other Regional Entities were benchmarked to identify best practices ~~implemented~~for inclusion in this manual.

DRAFT

The process improvements and clarity captured in this revision to the NPCC Regional Reliability Standards Development Procedure, will result in a more timely and efficient manner to address the development of regional standards to ensure the reliability of the Bulk Electric System within the NPCC geographical area.

DRAFT

II. INTRODUCTION

PURPOSE~~an~~

This manual defines the characteristics of a Northeast Power Coordinating Council, Inc. (NPCC) regional Reliability Standard (hereinafter referred to as "regional standard") and establishes the process by which NPCC regional standards are developed, approved, revised, formally interpreted and retired. The NPCC regional standards process is a stakeholder process that is approved by the NPCC members to ensure a transparent standard development process that is "open, fair, and inclusive"~~ process for the transparent initiation, development, implementation and revision of NPCC Regional Reliability Standards necessary for the reliable operation~~."

NPCC regional standards address the reliability of the international and interconnected ~~bulk power system~~Bulk Electric System in Northeast North America. ~~These Standards~~NPCC regional standards shall enable or support one or more NERC/ERO reliability principles[1] and will, in all cases, not be inconsistent with or less stringent than any requirements of the North American Electric Reliability Council/Electric Reliability Organization (NERC/ERO) ~~Reliability Standards. The procedure will not unnecessarily delay the development of the proposed reliability standards. Each regional reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of pertinent reliability principles and criteria, thereby ensuring that no standard undermines reliability through an unintended consequence~~continent-wide Reliability Standards.

~~II.~~ The development of NPCC regional standards is performed according to the following principles using the process contained in this manual:

- Developed in a fair and open process that provides an opportunity for all interested parties to participate;
- Does not have an adverse impact on commerce that is not necessary for reliability;
- Provides a level of Bulk Electric System reliability that is adequate to protect public health, safety, welfare, and national security and would not have a significant adverse impact on reliability; and
- Based on a justifiable difference between Regions or between sub-Regions within the Regional geographic area.

Following industry approval, NPCC regional standards process and NPCC regional standards require approval by the NPCC Board of Directors, NERC as the Electric Reliability Organization (ERO) and the applicable regulatory authorities in the United States (FERC) and Canada.

BACKGROUND

Northeast Power Coordinating Council, Inc. (NPCC) is responsible for promoting and improving the reliability of the international, interconnected Bulk Electric System in Northeastern North America. NPCC carries out its mission through (i) the development of regional standards and compliance assessment and enforcement of continent-wide and regional standards, coordination of system planning, design and operations, and assessment of reliability, (collectively, "Regional

[1] Available on the NERC website: Reliability Principles

Entity activities"), and (ii) the establishment of regionally-specific criteria, and monitoring and enforcement of compliance with such criteria (collectively, "criteria services activities").

The Energy Policy Act (EPA) of 2005 (Section 1211) amended the Federal Power Act (FPA) by adding Section 215, Electric Reliability. Specifically regarding standards development and pursuant with Section 215(e)(4) of the FPA, NPCC as a Regional Entity with delegated authority from NERC may propose regional standards to NERC for eventual enforcement within the NPCC region.

As a condition of NPCC membership, NPCC General and Full Members[2] agree to adhere to NERC Reliability Standards. NERC Reliability Standards are comprised of both continent-wide and regional standards. The NPCC regional standards apply only to that part of the Eastern Interconnection within the NPCC geographical area.

III. REGIONAL STANDARD ~~DEVELOPMENT PROCEDURE~~CHARACTERISTICS AND ELEMENTS

1. ~~1.~~ CHARACTERISTIC ATTRIBUTES

~~The NPCC Regional Reliability Standards Development Procedure is:~~

~~**Open** — The NPCC Regional Reliability Standards Development Procedure provides any person the ability to participate in the development of~~ The NPCC regional standards development process has the following key characteristics:

- **Fair due process** — The NPCC regional standards development process provides for reasonable notice and opportunity for public comment. At a minimum, the procedure shall include public notice of the intent to develop a standard~~. Any entity~~, a public comment period on the proposed standard, due consideration of those public comments, and a ballot of interested stakeholders. Upon approval by the NPCC Members, the NPCC Board of Directors then votes to approve submittal of the regional standard to NERC for ERO approval, followed by submission to FERC and Canadian Authorities for their approvals.

- **Openness** — Participation in the NPCC regional standards development process is open to all persons and organizations that ~~is~~are directly and materially affected by the reliability of the NPCC's ~~bulk power system has the ability to participate in the development and approval of reliability standards~~Bulk Electric System. There ~~are~~is no undue financial ~~barriers~~burden to participation. Participation ~~in the open comment process is~~shall not ~~conditional~~be conditioned upon membership in the ERO, NPCC or any organization, and ~~participation is~~shall not be unreasonably restricted on the basis of technical qualifications or other such requirements. ~~NPCC utilizes a website to accomplish this. Online posting and review of standards and the real time sharing of comments uploaded to the website allow complete transparency.~~

- **Inclusive** — ~~The NPCC Regional Reliability Standards Development Procedure provides any person~~Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the reliability of NPCC's Bulk Electric System has the right to participate by: (a) expressing an opinion and its basis~~, have that~~; (b) having their

[2] As defined in the NPCC By-Laws – available on the NPCC website

position considered, and ~~appealed~~(c) having the right to appeal a response through an established ~~appeals~~appeal process ~~if adversely affected.~~.

- ~~**Balanced** — The NPCC Regional Reliability Standards Development Procedure has a balance of interests and all those entities that are directly and materially affected by the reliability of the NPCC's bulk power system are welcome to participate~~**Balanced** — The NPCC regional standards development process strives to have an appropriate balance of interest and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter. ~~This will be accomplished through~~Pursuant with the NPCC ~~Bylaws defining eight~~By-Laws[3] there are seven (7) stakeholder voting sectors ~~(categories)~~and the votes for ~~voting.~~each sector are weighted to achieve an appropriate balance.

  - ~~**Fair Due Process** — The NPCC Regional Reliability Standards Development Procedure provides for reasonable notice and opportunity for public comment. The procedure includes public notice of the intent to develop a standard, a 45 calendar day public comment period on the proposed standard request, or standard with due consideration of those public comments, and responses to those comments will be posted on the NPCC website. A final draft will be posted for a 30 calendar day pre-balloting period, and then a ballot of NPCC Members will be conducted. Upon approval by the NPCC Members, the NPCC Board then votes to approve submittal of the Regional Standard to NERC.~~

- **Transparent** — All actions material to the development of ~~Regional Reliability Standards~~NPCC regional standards are transparent and information regarding the progress ~~is posted~~of a standard's development action is made available to the public through postings on the NPCC website as well as through ~~extensive email~~E-mail lists.

- **Without undue delay** — The NPCC regional standards development process shall be performed within a reasonable time.

In as much as NPCC is one of ~~several regional entities~~six Regional Entities within the Eastern Interconnection of North America, there will be no presumption of validity by the ERO for any NPCC ~~Regional Reliability Standard.~~regional standard. In order to receive the approval of the ERO, the NPCC ~~Reliability Standards Development Process~~regional standards development process must also achieve the following objectives:

- **No Adverse Impact on Reliability of the Interconnection** —~~An~~ A NPCC ~~Regional Reliability Standard~~regional standard provides a level of ~~bulk power system~~Bulk Electric System reliability that is necessary and adequate to protect public health, safety, welfare, and North American security and will not have an adverse impact on the reliability of the Interconnection or other Regions within the Interconnection.

  - ~~**Justifiable Difference** — An NPCC Regional Reliability Standard is based on justifiable differences between Regions, such as different electrical systems or~~

[3] NPCC By-Laws are available on the NPCC website

~~facilities, sensitivity of load to disruptions, sensitivity of generation to disruptions, frequency and voltage sensitivity, system operating limit development and facilities ratings process, electrical system interactions, etc.~~

- ~~**Uniformity** - NPCC Regional Reliability Standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk power system of the North American continent. A NPCC Reliability Standard shall be more stringent than a continent-wide reliability standard, may include a regional variation that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the northeast's bulk power system, where the interpretation of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.~~

- **Justifiable Difference** — A NPCC regional standard addresses a justifiable difference within the NPCC geographical area that results from a physical difference[4] or operating difference in the Northeast's Bulk Electric System. Although a justifiable difference allows for a unique regional standard, a NPCC regional standard shall be no less stringent than a continent-wide standard.
- **Uniformity** — To the extent possible, the NPCC regional standards provides uniformity with Reliability Standards across the interconnected Bulk Electric System of North America.
- **No Undue Adverse Impact on Commerce** — ~~An~~A NPCC ~~Regional Reliability Standard~~regional standard will not cause any undue adverse impact on business activities that are not necessary for reliability of the Region and its interconnected Regions. All regional ~~reliability~~ standards shall be consistent with NERC's market principles[5].

~~**Other Attributes of the NPCC Regional Reliability Standards Development Procedure include;**~~

- ~~**Maintenance of Regional Reliability Standards** - NPCC Regional Standards will be reviewed for possible revision at least every three years and follow the same process as a new standard. The old standard will remain in place until such time as the revised version has passed through the entire process, at which point the old standard will be retired in accordance with any applicable new implementation plan associated with the approved revised standard. The review process shall be conducted by soliciting comments from the stakeholders and through open posting on the NPCC website. If no changes are warranted, Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review~~

[4] The interpretation of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

[5] Available on the NERC website: www.nerc.com

~~indicates a need to revise or withdraw a standard, a regional standard authorization request shall be prepared by the RSC and submitted in accordance with the standards development process contained in this procedure.~~

- ~~**Maintenance of Regional Reliability Standards Development Procedure** This NPCC Regional Reliability Standards Development Procedure will be reviewed for possible revision at least once every five years or more frequently if needed and subject to the same procedure as that of the development of a standard. All such revisions shall be subject to approval by the NPCC Board, NERC, FERC, and could be subject to approval, if required, by applicable authorities in Canada. The NPCC RSC has the authority to make non-substantive changes to this procedure and subsequently notify the NPCC Board for their concurrence at their next scheduled meeting.~~

- ~~**Interpretation of Standards** All persons who are directly and materially affected by the NPCC's bulk power system reliability shall be permitted to request an interpretation of a standard. The person requesting an interpretation will send an email request to the Regional Standards Process Manager (RSPM), as noted on the NPCC website, explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard. The RSPM along with guidance from the RSC will forward the request to the originating Task Force which acted as the drafting team for that regional reliability standard. The Task Force will address, through a written response, the request for clarification as soon as practical, but not more than 45 business days from its receipt by the Task Force. This written interpretation will be posted along with the final approved and adopted standard and will stand until such time as the standard is revised through the normal RSAR process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.~~

2. ELEMENTS OF A ~~RELIABILITY~~REGIONAL STANDARD

- ~~**Elements of a Regional Reliability Standard**~~

To ensure uniformity of regional ~~reliability~~standards and avoid inconsistency with NERC continent-wide standards, a NPCC regional ~~reliability~~ standard shall ~~consist of~~be consistent with the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of regional standards. ~~This~~The application of a systematic discipline is necessary ~~to~~for achieving regional standards that are measurable, enforceable, and consistent~~.~~ as well as results oriented[6], i.e.:

[6] Results-based Standards see http:www.nerc.com/filez/standards/Project2010-06_Results-based_Reliability_Standards.html

~~All mandatory requirements of a regional reliability standard shall be within the standard document. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself.~~

~~The most current version of the approved NERC Reliability Standard template and its associated elements as or if applicable, will be used at the time of the development of the NPCC Regional Reliability Standard to ensure all essential elements are contained therein to achieve consistency and uniformity and meet all statutory requirements. A sample of the elements contained in the standard appears in Table 1 below, however the latest ERO Board approved Standard template, that may be found on the NERC website, will supersede the list below at the time the regional standard is developed.~~

~~Table 1- Elements of a Regional Reliability Standard~~

- Performance-based,
- Risk-based, and
- Capability-based.

TYPES OF RELIABILITY REQUIREMENTS

The Drafting Team (DT) should strive to achieve a portfolio of performance, risk, and capability-based mandatory reliability requirements that support an effective defense-in-depth strategy. Each requirement should identify a clear and measurable expected outcome, such as: a) a stated level of reliability performance, b) a reduction in a specified reliability risk, or c) a necessary competency.

a) **Performance-based** - defines a specific reliability objective or outcome that has a direct, observable effect on the reliability of the Bulk Electric System, i.e. an effect that can be measured using power system data or trends.

b) **Risk-based** - defines actions of entities that reduce a stated risk to the reliability of the Bulk Electric System and can be measured by evaluating a particular product or outcome resulting from the required actions.

c) **Capability-based** - defines capabilities needed to perform reliability functions and can be measured by demonstrating that the capability exists as required.

Each regional standard shall enable or support one or more of the reliability principles[7] as identified in the most recent set posted on the NERC website. Each regional standard shall also be consistent with all of the reliability principles. The intent of the set of NPCC regional standards is to deliver an Adequate Level of Reliability[8] as defined by NERC.

Recognizing that Bulk Electric System reliability and electricity markets are inseparable and mutually interdependent, all regional standards shall be consistent with the most recent set of Market Principles[9] as posted on the NERC website. Consideration of the Market Principles is intended to ensure that regional standards are written such that they achieve their reliability

[7] Available on the NERC website: Reliability Principles
[8] Available on the NERC website: Adequate Level of Reliability
[9] Available on the NERC website: Market Principles

objective without placing undue restrictions or causing adverse impacts on competitive electricity markets.

ELEMENTS OF A REGIONAL STANDARD

A regional standard includes several components designed to work collectively to identify what entities must do to meet their reliability-related obligations as an owner, operator or user of the Bulk Electric System. The components of a NPCC regional standard identified below are based on the NERC Standard Processes Manual (SPM) that was approved by the NERC Board of Trustees at its February 2013 meeting. Future revisions of the NERC SPM will be used at the time of development of a NPCC regional standard if different from the elements listed below.

The only mandatory and enforceable components of a regional standard are the: (1) Applicability, (2) Requirements, and (3) the Effective Dates. The additional components are included in the regional standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to functional entities concerning how compliance will be assessed by the Compliance Enforcement Authority.

The components of a regional standard may include the following:

Title:	A brief, descriptive phrase identifying the topic of the regional standard.
~~***Identification Number:***~~	A unique identification number assigned in accordance with ~~an administrative~~a published classification system to facilitate tracking and reference~~. (i.e. "NPCC-BAL-002-0-Date" which refers~~ to ~~NPCC Regional Standard, referencing NERC BAL-002 Version 0, with NPCC Effective Date-final adoption by all Regional Authorities)~~the regional standards.
~~***Title*** ***Purpose:***~~	~~A brief, descriptive phrase identifying~~The reliability outcome achieved through compliance with the ~~topic~~requirements of the regional standard.
Applicability:	~~Clear identification of~~Identifies which entities are assigned reliability requirements; i.e., the specific functional ~~classes of~~ entities ~~responsible for complying with~~and facilities to which the regional standard~~, noting any specific additions or exceptions.~~ ~~The standard will be applicable to the Bulk Power System unless otherwise noted~~ applies.
Effective ~~**Date and Status**~~ ***Dates:***	~~The effective date of the standard or, prior to approval of the standard, the proposed effective date.~~Identification of the date or pre-conditions determining when each Requirement becomes effective in each jurisdiction.

~~**Purpose**~~	~~The purpose of the standard. The purpose shall explicitly state what outcome will be achieved or is expected by this standard.~~
~~**Requirement(s)**~~	~~Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Each statement in the requirements section shall be a statement for which compliance is mandatory.~~

DRAFT

~~**Risk Factor(s)**~~ ***Requirement:***	~~The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below:~~ ~~A High Risk Factor requirement (a) is one that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, 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, or could hinder restoration to a normal condition.~~ ~~A Medium Risk Factor requirement (a) is a requirement that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk power system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.~~ ~~A Lower Risk Factor 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.~~An explicit statement that identifies the functional entity responsible, the action or outcome that must be achieved, any conditions achieving the action or outcome, and the reliability-related benefit of the action or outcome. Each requirement shall be a statement for which compliance is mandatory.
~~**Measure(s)**~~	~~Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to~~

DRAFT

	~~realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.~~

~~**Table 2 —**~~ Compliance Elements: Elements to aid in the administration of ~~**a Regional Reliability Standard**~~compliance monitoring and enforcement responsibilities.

Measure: Provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.

~~**Compliance Monitoring Process**~~***Violation Risk Factors and Violation Severity Levels:***

~~Defines for each measure:~~

- ~~The specific data or information that is required to measure performance or outcomes.~~
- ~~The entity that is responsible for providing the data or information for measuring performance or outcomes.~~
- ~~The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes.~~
- ~~The entity that is responsible for evaluating data or information to assess performance or outcomes.~~
- ~~The time period in which performance or outcomes is measured, evaluated, and then reset.~~
- ~~Measurement data retention requirements and assignment of responsibility for data archiving.~~

~~Violation severity levels.~~Violation risk factors (VRFs) and violation severity levels (VSLs) are used as factors when determining the size of a penalty or sanction associated with the violation of a requirement in an approved Reliability Standard. Each requirement in each Reliability Standard has an associated VRF and a set of VSLs. VRFs and VSLs are developed by the Drafting Team, working with NPCC Standards Staff, at the same time as the associated Reliability Standard, but are not part of the Reliability Standard. The Board of Directors is responsible for approving VRFs and VSLs.

- Violation Risk Factors
  VRFs identify the potential reliability significance of noncompliance with each requirement. Each requirement is assigned a VRF in accordance with the latest approved set of VRF criteria.
- Violation Severity Levels
  - VSLs define the degree to which compliance with a requirement was not achieved. Each requirement shall have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs. Each requirement is assigned one or more VSLs in accordance with the latest approved set of VSL criteria.

DRAFT

Version History:	The version history is provided for informational purposes and lists information regarding prior versions of the regional standard.
Variance:	As applied to a NPCC regional standard is a Requirement (to be applied in the place of the NPCC region-wide Requirement) that is applicable to a specific geographic area or to a specific set of Registered Entities.
Compliance Enforcement Authority (CEA):	The entity that is responsible for assessing performance or outcomes to determine if an entity is compliant with the associated regional standard. The Compliance Enforcement Authority will be NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the ERO regional standards.
Reliability Standard Audit Worksheets (RSAWs)[10]	Reliability Standard Audit Worksheets (RSAWs) are developed as companion documents to regional and continent-wide Reliability Standards to facilitate the CEA assessment of a registered entity's compliance with a standard.

~~*Supporting Information Elements*~~

Informational Elements: Elements to aid in the implementation of the regional standard.

~~Interpretation~~	~~Any interpretation of regional reliability standard that is developed and approved in accordance with the "Interpretation of Standards" section of Appendix A of this procedure, to expound on the application of the standard for unusual or unique situations or to provide clarifications.~~

~~Implementation Plan~~*Application Guidelines:*	~~Each regional reliability standard shall have an associated implementation plan describing the effective date of the standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the standard in the compliance program and other considerations in the initial use of the standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and is approved as part of the ballot of the standard.~~Guidelines to support the implementation of the associated regional standard.

[10] While RSAWs are not part of the regional standard, they are developed through collaboration of the Drafting Team and NPCC Compliance Staff.

~~Supporting References~~*Procedures:* ~~This section references related documents that~~ Procedures to support ~~reasons for, or otherwise provide additional information related to~~ implementation of the associated regional ~~reliability~~ standard. ~~Examples include, but are not limited to:~~

- ~~Glossary of terms~~
- ~~Developmental history of the standard and prior versions~~
- ~~Notes pertaining to implementation or compliance~~
- ~~Standard references~~
- ~~Standard supplements~~
- ~~Procedures~~
- ~~Practices~~
- ~~Training references~~
- ~~Technical references~~
- ~~White papers~~
- ~~Internet links to related information~~

~~3. Terms And Functions~~

- ~~**Regional Standards Committee (RSC)** – An NPCC committee charged with management of the NPCC Standards Procedure under a sector based voting structure as described in the NPCC Bylaws. The NPCC RSC will consider requests for new or revised standards and be available for advisement to the NPCC Board on the standards.~~

  ~~The RSC may not itself modify the standard without issuing a new notice to stakeholders regarding a vote of the modified standard. Any RSC action will only be activated in the event of a minor correction of a standard such as errata.~~

  ~~The RSC is an open and balanced stakeholder committee inclusive of all stakeholder interests that provide for or are materially impacted by the reliability of the bulk power system.~~

  ~~The RSC disposition regarding the regional standard authorization request, which will in all cases be within 60 calendar days of receipt of a completed standard request, shall include:~~

  - ~~Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The RSC may, at its discretion, expand or narrow the scope of the standard request under consideration. The RSC shall prioritize the development of standards in relation to other proposed standards, as may be required based on the volume of requests and resources.~~

DRAFT

- ~~Reject the standard request. If the RSC rejects a standard request, a written explanation for rejection will be delivered to the requester within 30 calendar days of the decision.~~
- ~~Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the RSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the RSC.~~

IV. ~~The NPCC~~ REGIONAL STANDARDS DEVELOPMENT PROCESS

1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS ~~responsibilities of the RSC will include:~~

- ~~Review of NPCC Draft Standards for such factors as completeness, sufficient detail, rational result, and compatibility with existing standards; clarifying standard development issues not specified in this procedure. Under no circumstance will the RSC change the substance of a draft standard.~~
- ~~Due consideration to the work of the drafting team as well as the comments of stakeholders and minority objections, in approving a proposed regional reliability standard to go to ballot.~~
- ~~Approve standards for pre-ballot posting under a sector based voting structure as described later in the NPCC Inc. Bylaws or~~
- ~~Remand the standard back to the Task Force acting as the drafting team for further work or recommend a change in those participating in the drafting team (i.e. a new drafting team).~~

- ~~**Regional Standards Process Manager (RSPM)** - The Regional Reliability Standards Procedure shall be administered by a NPCC staff Regional Standards Process Manager. The RSPM is responsible for ensuring that the development and revision of standards is in accordance with this manual. The RSPM works to ensure the integrity of the process, format, consistency of quality, and completeness of the reliability standards. The RSPM facilitates all steps in the process.~~

- ~~**RELIABILITY COORDINATING COMMITTEE (RCC)** - The RCC, will support the standards development process through the assignment of NPCC Task Forces. They will also provide a technical advisory role in the Regional Reliability Standards development procedure through recommendations.~~

~~REQUESTER~~ ~~**A Requester is any individual or an entity**~~ NOMINATION, REVISION, INTERPRETATION, OR RETIREMENT OF A STANDARD:

Any member of NPCC or group within the NPCC region shall be allowed to request that a NPCC regional standard be developed, modified, interpreted, or retired. Additionally, any person (organization, company, government ~~authority~~agency, individual, etc.) ~~that submits a complete~~

~~request for development, revision, or withdrawal of a standard. Any person or an entity that~~ who is directly and materially affected by ~~an existing standard or the need for a new standard may submit a~~ the reliability of the NPCC Bulk Electric System shall be allowed to request ~~for a new standard or revision to a standard. The Requester is assisted by the RSAR drafting team (if one is appointed by the RSC) to respond to comments and to decide if and when the RSAR is forwarded to the RSC with a request to draft a standard. The Requester is responsible for the RSAR, assisted by the RSAR drafting team and Regional Standards~~ that a NPCC regional standard be developed, modified, interpreted, or retired. The following section identifies the process roles in the NPCC regional standards process. Refer to Step 2 STANDARD DEVELOPMENT PROCESS STEPS and FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS for the regional standards development process steps and associated flowchart.

PROCESS ~~**Manager, until such time the RSC authorizes**~~ ROLES AND RESPONSIBILITIES

BOARD OF DIRECTORS

The NPCC Board of Directors (Board) shall consider for adoption regional standards, definitions, variances and interpretations and associated implementation plans that have been processed according to the processes identified in this manual. Once the Board adopts a regional standard, definition, variance or interpretation, the Board shall direct NPCC Standards Staff to submit the document(s) for approval to the NERC Board of Trustees.

COMPLIANCE COMMITTEE (CC)

The NPCC Compliance Committee, a committee of the NPCC Board of Directors, manages the NPCC Compliance Monitoring and Enforcement Program (CMEP). The CMEP is used to monitor, assess and enforce mandatory compliance with both NERC continent-wide and NPCC regional standards. The CC aides in the regional standards development, as necessary, by: (1) performing compliance reviews of technical requirements, (2) assisting the Drafting Team with the development of ~~the standard. The Requester has the option at any time to allow the RSAR drafting team to assume full~~Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), Reliability Standard Audit Work Sheets (RSAWs) and (3) participating on quality review teams.

DRAFTING TEAM

The Drafting Team develops standards-related regional products as directed by the NPCC RSC and within the scope of an approved Regional Standard Authorization Request (RSAR) or a formal Request for Interpretation (RFI). The product that is developed is typically a new or revised regional standard, but could also be a definition, a reference document, a set of Violation Risk Factors, a set of Violation Severity levels, or the team could be appointed to assist an author in refining a Regional Standard Authorization Request (RSAR). The Drafting Team also works collaboratively with NPCC Compliance Staff to develop Reliability Standard Audit Worksheets (RSAWs) at the same time regional standards are developed. The Drafting Team shall remain in place until such time as the NERC Board of Trustees adopts the regional standard.

MANAGER OF RELIABILITY STANDARDS

The NPCC Manager of Reliability Standards has the overall responsibility for ~~the RSAR. The Requester may chose to~~managing the NPCC regional standards processes in accordance with this manual. As used herein, the NPCC Manager of Reliability Standards will be the NPCC Manager of Reliability Standards or his/her designee.

DRAFT

NPCC MEMBERS

NPCC members may participate in the comment and ballot periods associated with the development and industry approval of regional standards. The ballot body is comprised of all entities or individuals that qualify for one of the stakeholder sectors within NPCC as stated in the most recently approved NPCC Bylaws. All General and Full Members of NPCC can participate in ~~subsequent standard drafting efforts related to the RSAR.~~the balloting of regional standards. Any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards.

NON-NPCC MEMBERS

Any entity or person that is neither a General nor Full Members of NPCC is not eligible to participate in the ballot body voting on a regional standard. However, any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards. Subject Matter Experts (SMEs), regardless of NPCC membership status, are encouraged to participate in comment periods for regional standards.

NPCC STANDARDS STAFF

The Standards Staff is responsible for assisting the NPCC Manager of Reliability Standards and the RSC in administering the NPCC regional standards processes in accordance with this manual.

NPCC COMMITTEES, TASK FORCES AND WORKING GROUPS

The Committees, Task Forces and Working Groups~~. The committees, task forces and working groups~~ within NPCC~~,~~ serve an active role in the standards process. Activities performed by these groups include, but are not limited to, the following:

- Identify the need for new or modified regional standards~~ Identify the need for new or modified regional standards.~~
- ~~•~~
- Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs~~).~~)
- ~~•~~ Develop comments (views and objections) to standards actions~~.~~
- ~~•~~ Participate in NPCC Standard drafting~~.~~
- ~~•~~ Provide technical oversight in response to changing industry conditions ~~—~~and ERO Requirements~~.~~
- ~~•~~ Conduct Field Tests, as required

REGIONAL STANDARDS COMMITTEE (RSC)

The NPCC Regional Standards Committee (RSC), a committee of the NPCC Board of Directors, is charged with oversight of all Drafting Team activities and managing the NPCC regional standards development process in accordance with this manual.

The RSC is responsible for maintenance of the Regional Standards Process Manual (RSPM), including the endorsement of RSPM revisions for NPCC Board review and approval.

DRAFT

RELIABILITY COORDINATING COMMITTEE (RCC)

The Reliability Coordinating Committee (RCC) supports the standards development process through the assignment of NPCC Task Forces to serve as technical resources for: (1) staffing Drafting Teams, and (2) performing a technical advisory role in the regional standards process through comments, recommendations and technical justifications.

REQUESTER

~~**4. PROCEDURE DESCRIPTION**~~

~~***STEPS 1 AND 2: REQUEST TO DEVELOP A NEW REGIONAL STANDARD***~~

~~Requests to develop a new Regional Reliability Standard shall be submitted to the RSPM by completing a **Regional Standard Authorization Request** (RSAR) ***(see Appendix A)***. The RSAR is a description of the new or revised standard in sufficient detail to clearly define the scope, purpose, and importance of the Regional Standard, impacted parties or other relevant information. A "needs" statement will provide the justification for the development of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard. The RSPM shall maintain the RSAR form and make it available electronically on the NPCC website.~~

~~Any person or entity ("Requester") directly or materially affected by an existing standard or the need for a new or revised standard may initiate a RSAR.~~

~~The Requester will submit the RSAR to the RSPM electronically and the RSPM will acknowledge receipt of the RSAR immediately, through electronic receipt. The RSAR, as a minimum, needs to contain the following information in order to be qualified for consideration. The NPCC RSPM will assist the Requester to ensure all the following information is submitted (on the RSAR) in a form appearing in Appendix A:~~

~~1. Proposed Title and Date of New RSAR~~
~~2. Requester's Name and Contact Information~~

Any individual representing an organization (entity, company, government agency, etc.) that is directly and materially affected by the reliability of the Bulk Electric System within the NPCC geographical area may request a regional standard be developed or an existing regional standard be modified, interpreted, or deleted.

QUALITY REVIEW TEAM

The NPCC Standards Staff shall coordinate a quality review of the "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, and whether the regional standard is clear and enforceable as written. The Quality Review Team may be comprised of legal and compliance representatives, a technical writer, and NPCC Standards Staff. It will not involve individuals who participated on the Drafting Team of the standard undergoing the Quality Review.

DRAFT

2. Standard Development Process Steps

Step 2.1: Regional Standards Authorization Request to Develop, Modify or Retire

A Regional Standard Authorization Request[11] (RSAR) is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified regional standards or the benefit of retiring one or more approved regional standards.

A RSAR shall be used to seek approval and initiate the development, modification or retirement of a NPCC regional standard. A RSAR is not used to seek a formal Request for Interpretation (RFI) of a NPCC regional standard. The initiation and handling of a RFI is covered in Step 3 Standard Interpretation Process Steps, of this manual.

Any individual representing an organization which is directly or materially impacted by the operation of the Bulk Electric System within the geographical footprint of NPCC may request, via a submittal of a RSAR to the NPCC Manager of Reliability Standards, the development, modification, or deletion of a NPCC regional standard. The individual completing the form is referred to herein as the Requester.

Step 2.1.a. Requester Actions

> *Note: The NPCC Manager of Reliability Standards will assist the Requester, as necessary, to ensure all required information is submitted on the RSAR.*

The Requester shall complete a RSAR form in accordance with the guidance provided in Appendix A: RSAR Completion Guidelines.

The Requester shall submit the completed RSAR to the NPCC Manager of Reliability Standards, via npccstandard@npcc.org, for processing.

Step 2.1.b. NPCC Manager of Reliability Standards Actions

The NPCC Manager of Reliability Standards shall review the submitted RSAR and verify that the submitted form has been adequately completed. Within fifteen (15) calendar days[12] of receipt of the submitted RSAR, the NPCC Manager of Reliability Standards will electronically acknowledge receipt of the RSAR. If, at that time, the NPCC Manager of Reliability Standards finds the RSAR to be deficient, the Requester will be contacted to decide on how to proceed.

~~3.~~ Within ten (10) calendar days of the receipt of an adequately completed RSAR, the NPCC Manager of Reliability Standards **~~Purpose~~** ~~of the Regional Standard~~

~~4. Description of Industry Need~~

~~5. Provide a Brief Description of the Standard~~

~~6. Identification of the Entities in the Functional Model as being responsible to adhere to the standard.~~

~~7. Necessary information to assist the drafting the team, to the extent feasible, to allow them to draft the standard.~~

~~8. A cross references to existing NPCC or NERC documents~~

[11] The RSAR is located on the NPCC website under Standards – Regional Standards General

[12] Time periods specified in this manual may be extended as deemed appropriate by NPCC Staff. When business days are specified, this provision could be used to take into account differing Canadian and US holiday schedules. When calendar days are specified, this provision could be used to take into account due dates that fall on a weekend.

~~The RSPM~~ shall forward ~~all~~the properly completed ~~RSARs to the RSC. The RSC shall meet at established intervals to review all pending RSARs. The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for~~ RSAR to the NPCC Regional Standards Committee (RSC) for its review and processing. Included in the transmittal of the RSAR to the RSC, the NPCC Manager of Reliability Standards shall include a statement indicating the applicability of the NPCC Cost Effectiveness Analysis Procedure (CEAP) for the proposed change.

STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC~~ action more than 60 calendar days from the date of receipt. The RSC may~~) ACTIONS

Note: The RSC shall meet to review all pending RSARs. The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for RSC action more than 60 calendar days from the date of receipt by the RSC.

The RSC shall review the RSAR and take one of the following actions:

- ~~•~~ Remand the RSAR back to the ~~RSPM~~NPCC Manager of Reliability Standards for additional work. In this case, the ~~RSPM~~NPCC Manager of Reliability Standards may request additional information or clarification for the RSAR from the Requester.

  ~~•~~ ~~Accept~~Reject the RSAR ~~as a candidate for a new or revised standard~~. In this case, the RSC will ~~forward the RSAR to the RCC to assign a NPCC Task Force to provide technical support and analysis of comments for that RSAR, and assist the Requester and the RSPM in the remaining steps of the process. The RSPM shall post notification of intent to develop a standard on both NPCC and ERO websites within 30 calendar days of acceptance.~~
- ~~• Reject the RSAR. In this case, the RSC will~~provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the Requester within ~~30~~ten (10) calendar days of the rejection decision.

~~STEPS 3, 4, AND 5: RSC ACCEPTS RSAR AND RCC ASSIGNS TF TO DRAFT NEW OR REVISED STANDARD~~

Note: Before the RSC can accept a RSAR for a new or modified standard the applicable CEAP process steps shall be completed.

- Accept the RSAR.
  - If a new or modified standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to develop or modify a regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR.
    - If the retirement of an existing regional standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to retire an existing regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR.

DRAFT

The process to retire an existing regional standard is included in Step 5 RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD.

STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD

A RSAR that ~~is~~has been accepted by the RSC ~~will~~shall, within ten (10) calendar days of the acceptance of the RSAR, be submitted by the NPCC Manager of Reliability Standards to the NPCC Reliability Coordinating Committee (RCC~~. Within 60 calendar days the~~). The RCC shall, within sixty (60) calendar days, assign the development of the regional standard to a NPCC Task Force, and notify the NPCC Manager of Reliability Standards of its decision within ten (10) calendar days.

After receipt of the notification of Drafting Team~~. The RSPM shall solicit and recommend~~ assignment, the NPCC Manager of Reliability Standards shall oversee solicitation and recommendation of a list of additional qualified[13] candidates over and above the appropriate NPCC Task Force members, for appointment to the ~~team and~~Drafting Team. The Requester and a NPCC Compliance Staff person will be included on the Drafting Team. Within sixty (60) calendar days of the Drafting Team assignment notification from the RCC, the NPCC Manager of Reliability Standards shall submit the list ~~to the RSC.~~of the entire Drafting Team membership to the RSC for acceptance. The RSC may accept the recommendations of the NPCC Manager of Reliability Standards as presented or revise the recommendations as necessary.

Upon acceptance of the Drafting Team slate, the RSC shall provide a target date on which the Drafting Team is expected to have ready a completed draft regional standard and associated supporting documentation available for consideration by the NPCC membership. Additionally, the RSC shall provide the Drafting Team with any preliminary development products including, but not limited to, a draft standard, comments, and related white papers.

STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS

Prior to beginning work on the development of a new or revised regional standard and the associated supporting documentation, the Drafting Team should develop a work plan for completing the regional standard development work, including the establishment of milestones for completing critical elements of the work in sufficient detail to ensure that the Drafting Team will meet the target date established by the RSC, or the Drafting Team shall propose an alternative date. This ~~list shall include the Requester. The RSC may select other individuals to serve, with the Task Force to draft the Standard. This team shall~~work plan must be submitted to the RSC for its concurrence. When a Drafting Team begins its work, it shall regularly (at least quarterly) report progress against that aforementioned work plan to the NPCC Manager of Reliability Standards for presentation to the RSC.

[13] Refer to Appendix B: Selection of Drafting Team Members

DRAFT

Note: During the regional standards development, the Drafting Team will deliberate on whether the requirements in the regional standard are developed enough to begin the Cost Effectiveness Analysis (CEA) of the NPCC Cost Effectiveness Analysis Procedure (CEAP). When appropriate, the Drafting Team shall request that the RSC initiate the second phase (CEA) of the CEAP process.

The Drafting Team shall create and manage its work structure (e.g., sub-teams) and meeting schedule (face-to face as well as electronic meetings), as necessary, to meet the milestone dates and project deliverables outlined in the work plan.

The work products of the Drafting Team should consist of ~~a small group of people who collectively have the necessary technical expertise and work process skills.~~ the following

- ~~The RSPM shall assign~~A draft regional standard consistent with the RSAR on which it was based
- An implementation plan, including the nature, extent and duration of field-testing, if any
- Identification of any existing regional standard and NPCC ~~staff personnel to~~criteria that will be deleted, in part or whole, or otherwise impacted by the implementation of the draft regional standard
- Technical reports, white papers and/or work papers that provide technical justification for the draft regional standard under consideration
- Reliability Standard Audit Worksheet (RSAW) collaboratively developed by the Drafting Team and NPCC Compliance Staff

NPCC Standards Staff can assist in the drafting of the regional standard including compliance ~~measure~~measures, process and elements. The drafting of measures and compliance administration aspects of the standard will be coordinated with the NPCC Compliance ~~Program.~~Staff.

The Drafting Team shall submit the initial and subsequent interim drafts of the regional standard and associated documents to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post documents for comment.

STEP ~~*6: SOLICIT PUBLIC*~~ 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS ~~*ON DRAFT STANDARD*~~

~~Once a draft standard has been verified by the RSC to be within the scope and purpose of the RSAR, the RSPM will post the draft standard for the purpose of soliciting public comments. The posting of the draft standard will be linked to the RSAR for reference. In addition to the standard, an implementation plan shall be posted to provide additional details to the public and aid in their commenting and decision process. Comments on the draft standard will be accepted for a 45 calendar day period from the public notice of posting. Comments will be accepted on-line using the NPCC Open Process web-based application.~~

~~Final draft standards will be concurrently posted on the ERO website for comments.~~

~~*STEPS 7, 8, AND 9: OPEN PROCESS POSTING AND ANALYSIS OF THE COMMENTS*~~

~~The RSPM~~

Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.

STEP 2.4.A. COMMENT PERIOD

Note: For Final Comment Period skip this step and proceed to STEP 2.4.B. FINAL COMMENT PERIOD.

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the draft of the regional standard on the NPCC website, along with a draft implementation plan and available supporting documents, for a forty-five (45) calendar day comment period. The NPCC Manager of Reliability Standards shall also notify NERC to process the draft document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the ~~new~~ draft regional standard and ~~distribute those~~associated documents and provide all comments to the Drafting Team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the Drafting Team shall convene and consider changes to the draft Standard, the implementation plan and/or supporting technical documents based upon comments received. All submitted comments ~~to the Task Force acting as the standard drafting team. The Task Force shall give prompt consideration to the written views and comments of all participants. An effort to address all expressed comments shall be made~~shall be addressed, and each commenter shall be advised of the disposition ~~of the comment and the reasons therefore, in addition to public posting of the responses.~~, with reasons, of their comments. The NPCC Manager of Reliability Standards shall publicly post all of the Drafting Team's responses to stakeholder comments on the NPCC website.

~~The Task Force acting as the Standard Drafting Team shall take one of the following actions:~~

- ~~Submit the draft standard for RCC endorsement as it stands, along with the comments received and responses to the comments. Based on the comments received, the Task Force acting as the standard drafting team may include revisions that are not substantive. A substantive change is one that directly and materially affects the application of the standard, including, for example: changing "shall" to "should," changing "should" to "shall"; adding, deleting, or revising requirements; or adding, deleting, or revising measures for which compliance is mandatory.~~

- ~~Make substantive revisions to the draft standard and reposts it for further open review and comment.~~

- ~~Task Force recommends Field Test if necessary to RSC.~~

~~Requester also may withdraw the request for a standard.~~

~~RCC submits proposed RRS to the RSC along with its recommendation based on comments, Task Force statements and any field test results.~~

~~STEPS 10 AND 11: RSC APPROVES OF THE NEW OR REVISED STANDARD FOR POSTING~~

If the RSC, acting with consideration of any recommendations by the RCC and utilizing the composite sector voting structure, as outlined in the NPCC, votes to post the draft standard for approval, the draft standard, all comments received, and the responses to those comments shall be posted electronically for the NPCC Members, by the RSPM and made public through the NPCC Website (www.npcc.org) for a 30 calendar day "pre-ballot review" and request for balloting. If the RSC decides more work is needed, the draft standard will be remanded back to the drafting Task Force. All actions of the RCC, Task Forces acting as drafting teams and the Regional Standards Committee will be recorded in regular minutes of the group(s) and posted on the NPCC website. Once the notice for a ballot has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued

STEPS 12, 13 AND 14: BALLOT OF STANDARD

Upon notification of a ballot, the Members of NPCC's registered ballot body will cast their vote consistent with the NPCC Bylaws. This ballot shall commence no sooner than 15 calendar days and no later than 30 calendar days following the notification of ballot. All members of the NPCC are eligible to participate in the voting on proposed, standard revisions or deletions of regional standards. The ballot period will typically begin immediately following the 30 calendar day pre-ballot posting and will last at least 10 business days.

The NPCC registered ballot body comprises all entities or individuals that qualify for one of the eight NPCC stakeholder sectors and are registered with NPCC as potential ballot participants in the voting on standards. Each member of the NPCC registered ballot body is eligible to vote on standards.

In order for a NPCC Regional Standard to be approved;

- A quorum must be established by at least 50% of the NPCC Members of at least 60% of the Voting Sectors on the roster of Members maintained by NPCC.
- A two-thirds majority of the total weighted sector votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions, and non-responses. Weighted sector vote will be calculated as follows;
  - Affirmative votes cast in each sector will be divided by the sum of affirmative and negative votes cast, in that same sector, to determine the fractional affirmative vote for each sector. Abstentions and non-responses will not be counted for the purposes of determining the fractional affirmative vote for a sector.
  - The sum of the fractional affirmative votes from all sectors divided by the number of sectors voting will be used to determine if a two-thirds majority has been achieved. (A sector will be considered as "voting" if any member of the sector in the ballot pool casts either an affirmative or a negative vote.)
  - A standard will be approved if the sum of fractional affirmative votes from all sectors divided by the number of voting sectors is at least 2/3.

Ballots will be cast electronically and alternatives are as follows;

- Affirmative
- Affirmative with Comments

DRAFT

Based on the comments received, the Drafting Team may elect to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the draft regional standard, the implementation plan and/or supporting technical documents.
- Recommend that the RSC authorize Field Testing of the draft regional standard. Upon completion of the Field Test, return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the draft regional standard based on insights learned during the Field Test.
- Obtain RSC concurrence to post documents for Final Comment Period and request that the RSC initiate the second phase (CEA) of the CEAP process

STEP 2.4.B. FINAL COMMENT PERIOD

The NPCC Standards Staff shall coordinate a Quality Review of "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, and whether the regional standard is clear and enforceable as written. Upon Completion of the Quality Review, including resolution of comments, the Drafting Team shall submit the regional standard to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post these documents for comment.

As authorized by the RSC, the NPCC Standards Staff shall post the "final draft" of the regional standard on the NPCC website, along with the implementation plan, supporting documents and the Cost Effectiveness Analysis (CEA) survey[14] for a forty-five (45) calendar day comment period. NPCC Standards Staff shall also notify NERC to process the proposed final document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard and associated documents and provide all comments to the Drafting Team for consideration.

In addition, the RSC, pursuant with the requirements of the Cost Effectiveness Analysis Procedure (CEAP), will use the responses to the posted CEA survey to develop a recommendation based on the cost effectiveness of the proposed regional standard.

The NPCC Task Forces (TFs) or Working Groups (WGs) may develop recommendations for submittal to the RSC. Following the RSC deliberations to determine a course of action, the RSC will communicate to the Drafting Team to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the Standard to address the results of the CEAP
- Accept the Standard "as is" to move forward through the remainder of the process
- Hold the Standard in abeyance until such time as additional guidance can be provided regarding whether or how to continue

[14] In accordance to the Cost Effectiveness Analysis Procedure (CEAP) the Cost Effectiveness Analysis (CEA) survey may be assigned directly to NPCC Task Forces (TFs) or Working Groups (WGs) in addition to the posting process.

- Decide not to pursue the development of certain requirements or the entire Standard due to cost effectiveness considerations

Upon Completion of the final comment period the Drafting Team shall submit the proposed regional standard, along with any supporting materials, consideration of comments and field test results, to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post the regional standard and implementation plan for ballot and concurrently provide an information copy to the RCC.

The NPCC Manager of Reliability Standards shall also publicly post all of the Drafting Team's responses to stakeholder comments on the NPCC website.

STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS

Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed regional standard on the NPCC website, along with supporting documentation [15] (e.g., implementation plan, consideration of comments, technical reports, white papers and any field test results), for a thirty (30) day pre-ballot review period and a subsequent ten (10) day ballot period. The ten (10) day ballot period will commence immediately following the pre-ballot review period. In the event that a quorum exists for purposes of an electronic vote but the ballot purpose has not been resolved, NPCC may continue to solicit additional responses in order to resolve the matter by electronic voting. In the event that quorum has not been achieved for purposes of an electronic vote, NPCC may continue to solicit electronic ballots, including abstentions, to obtain quorum and resolve the matter.

At the time the regional standard is posted for ballot, the NPCC Manager of Reliability Standards shall also notify NERC to process the proposed regional standard in accordance with NERC's regional standards review procedure, as applicable.

During the ballot period, the NPCC Members of the ballot body can cast their vote as follows:

- Affirmative, with or without comments
- Negative with comments
  - ~~Negative with Comments~~
- Abstain

In accordance with the NPCC Bylaws, a quorum and receipt of a two-thirds (2/3) affirmative majority of the weighted sector votes is required for a ballot to pass.

The ~~RSPM~~ NPCC Manager of Reliability Standards shall post the final outcome of the ballot process~~.~~ on the NPCC website.

[15] The ballot posting is for the regional standard, definition, variance or interpretation. Supporting documentation is included for information only and is not balloted.

STEP 2.5.A. BALLOT DOES NOT RECEIVE 2/3 AFFIRMATIVE VOTE

If ~~the~~ a ballot fails to achieve the 2/3 majority vote the NPCC Manager of Reliability Standards may:

- Direct the Drafting Team to respond to ballot comments and return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard ~~is rejected, it may be withdrawn~~. The consideration of comments from prior ballot will be included with the re-posting.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.
- Pursue the curtailment of the regional standard development by ~~either~~soliciting the ~~RCC or the original~~ Requester~~, or the standard may be remanded~~ to withdraw the RSAR or by soliciting the RSC ~~back to the Task Force acting as the drafting team to address the issues. All~~ to reject the RSAR pursuant with STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS. The NPCC Manager of Reliability Standards, in the event of a curtailment of the development of a regional standard, shall post a notice of the curtailment and will post and archive all comments submitted during the process ~~will be posted and archived~~ for future consideration ~~when redrafting~~, if required. The NPCC Manager of Reliability Standards will also notify NERC to process the proposed regional standard ~~upon~~in accordance with NERC's regional standards review~~.~~ procedure, as applicable.

~~The~~ STEP 2.5.B. BALLOT RECEIVES ≥ TWO-THIRDS (2/3) AFFIRMATIVE VOTE

A ballot that achieved two-thirds or greater affirmative vote has successfully passed. However, negative votes with comments should still be reconciled. If there is at least one negative vote with comments proceed to STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT". If there was not any negative vote with comments proceed to STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT".

STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT"

Following the conclusion of the NPCC ballot period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard~~, once~~ and provide all comments to the Drafting Team for consideration. The Drafting Team shall review all negative votes with comments and elect to:

- Recommend to the RSC to accept the regional standard "as is" and seek RSC endorsement to move forward through the remainder of the process. Upon receiving RSC endorsement to proceed, the regional standard and associated documents, approved by the NPCC ballot~~, and a recommendation will~~ body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval. If comments that were received during balloting should be considered in future revisions to the regional standard then the NPCC Manager of Reliability Standards should log comments in an issues database.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.

DRAFT

- Respond to ballot comments and recommend to the RSC endorse the return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard. The NPCC Manager of Reliability Standards should include the consideration of comments from the prior ballot with the re-posting.

STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT"

Regional standard and associated documents, approved by the NPCC ballot body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval.

STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL

Following approval by the NPCC Members, regional standards require review and approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the regional standard as presented.
- Approve the regional standard with comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive ~~modifications~~revisions to the standard~~. If~~.]
- Remand the ~~Board does not approve the~~ regional standard ~~for transmittal~~back to the RSC and the Drafting Team to address their concerns.

STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL

Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the regional standard to NERC, as the Electric Reliability Organization, for approval and subsequent filing with FERC and the applicable Canadian Provincial regulatory and/or governmental authorities for adoption.

STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD

Following the approval of a NPCC regional standard by FERC and the applicable Canadian Provincial regulatory and/or governmental authorities, all users, owners, planners, and operators of the Bulk Electric System in the NPCC geographic area are required to comply with the standard as of its enforcement date.

ERO approved Reliability Standards (both continent-wide and regional) are included in both the NERC and NPCC Compliance Monitoring and Enforcement Programs (CMEPs).

FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS

Placeholder for flowchart

3. STANDARD INTERPRETATION PROCESS STEPS

This section applies to NPCC regional standards that have been approved[16] and are currently enforceable or have a future enforcement date. A request for interpretation is not permitted for regional standards under development. For regional standards under development, clarification

[16] Approval is granted by FERC and the Canadian Provincial regulatory and/or governmental authorities, as applicable.

can be sought during a comment period. Refer to Step 2, STANDARD DEVELOPMENT PROCESS STEPS of this manual for details on the comment process for a standard under development.

STEP 3.1: REGIONAL STANDARDS REQUEST FOR INTERPRETATION (RFI)

Any member of NPCC or group within the NPCC region shall be allowed to submit a formal Request for Interpretation (RFI) of a NPCC regional standard.

Additionally, any person (organization, company, government agency, individual, etc.) who is directly and materially affected by the reliability of the NPCC Bulk Electric System shall be allowed to submit a formal Request for Interpretation (RFI) of a NPCC regional standard.

> *Note: A valid interpretation request is one that seeks additional clarity about one or more requirements in an approved regional standard, but does not request approval as to how to comply with any requirements of the standard.*

Request for Interpretation of a NPCC regional standard shall be initiated under the NERC process for developing an interpretation. The entity requesting the interpretation shall submit a Request for Interpretation form[17] to the NERC Reliability Standards Staff explaining the clarification required, the specific circumstances surrounding the request, and the impact of not having the interpretation provided. A copy of the completed RFI form should also be sent to the NPCC Manager of Reliability Standards.

Upon receipt of a RFI for a requirement of a NPCC regional standard, NERC Reliability Standards Staff shall forward the RFI to the NPCC Manager of Reliability Standards and in doing so shall delegate the validation of and response to the RFI to NPCC.

STEP 3.2: REVIEW AND VALIDATION OF REQUEST FOR INTERPRETATION (RFI)

Upon receipt of the NERC delegation to NPCC to validate and respond to a RFI for a requirement of a NPCC regional standard, the NPCC Manager of Reliability Standards shall review the RFI to determine whether:

- It meets the requirements for a valid interpretation
- A compliance process or approach could be used in lieu of an interpretation

The NPCC Manager of Reliability Standards will utilize, as necessary, the NPCC Standards Staff, NPCC Compliance and Legal Staffs when determining the validity of the RFI. Based on this review, the NPCC Manager of Reliability Standards will recommend to the RSC whether to accept or reject the RFI. The recommendation to the RSC should be made within thirty (30) calendar days of the receipt of the RFI from NERC.

The following examples identify situations that may warrant a recommendation from the NPCC Manager of Reliability Standards to reject the RFI:

- Requests approval of a particular compliance approach
- Identifies a gap or perceived weakness in the approved regional standard (Requester should be redirected to initiate an RSAR rather than a RFI)

[17] The *Request for Interpretation* form is posted under Resource Documents on the NERC Standards webpage.

- Where an issue can be addressed by an active (regional or continent-wide) standard Drafting Team
- Where an issue can be better addressed by a compliance process or approach
- Where it ~~will be remanded back to the RSC.~~requests clarification of any element of a regional standard other than a requirement

- ~~If~~Where a question has already been addressed in the record
- Where the interpretation identifies an issue and proposes the development of a new or modified regional or continent-wide standard ~~is approved, the standard will~~(such issues should be ~~submitted to the NERC/ERO Board of Trustees for approval.~~addressed via submission of a RSAR or SAR)

- ~~**STEPS 15, 16 AND 17: IMPLEMENTATION OF**~~ Where an interpretation seeks to expand the scope of a regional standard
- Where the requirement of the regional standard is clear

STEP 3.3: NPCC REGIONAL ~~STANDARD~~STANDARDS COMMITTEE (RSC) ACTIONS

~~Upon approval within the NPCC , the standard will be~~The RSC shall review the RFI along with the recommendation from the NPCC Manager of Reliability Standards and take one of the following actions:

- Reject the RFI. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the RFI to the entity requesting the interpretation within ten (10) calendar days of the decision to reject.
- Accept the RFI. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then: 1) post notification on the NPCC website of the intent to develop an interpretation; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RFI.

STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO RFI

A RFI that has been accepted by the RSC shall, within ten (10) calendar days of the acceptance of the RFI, be assigned by the NPCC Manager of Reliability Standards to the responsible NPCC Task Force to make up the interpretation Drafting Team and develop the RFI response.

DRAFT

STEP 3.5: DEVELOPMENT OF RESPONSE TO RFI

Note: A valid interpretation response provides additional clarity about one or more requirements, but does not expand on any requirement and does not explain how to comply with any requirement.

The Drafting Team shall submit a proposed interpretation response within forty-five (45) calendar days, from the receipt of the RFI, to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post the proposed response for comment.

If the RSC concurrence is not received, the Drafting Team will continue to refine the interpretation response.

Note: There are no limits to the number of public comment periods that can be conducted to result in a clear and concise interpretation of a regional standard requirement.

STEP 3.6: POSTING RFI FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed interpretation response on the NPCC website for a forty-five (45) calendar day comment period. NPCC Manager of Reliability Standards shall also notify NERC for processing in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the proposed interpretation response and provide all comments to the Drafting Team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the Drafting Team shall convene and consider changes to the proposed interpretation response based upon comments received. All submitted comments shall be addressed, and each commenter shall be advised of the disposition, with reasons, of their comments. The NPCC Manager of Reliability Standards shall publicly post all of the Drafting Team's responses to stakeholder comments on the NPCC website.

Based on the comments received, the Drafting Team may elect to:

- Return to STEP 3.5: DEVELOPMENT OF RESPONSE TO RFI to revise the proposed interpretation response.
- Accept the proposed interpretation response "as is" to move forward through the remainder of the process.

Upon Completion of the final comment period the Drafting Team shall submit the proposed interpretation response to the NPCC Manager of Reliability Standards to obtain RSC concurrence to submitted ~~to~~ proposed interpretation response.

The NPCC Manager of Reliability Standards shall also publicly post all of the ~~NERC/ERO~~Drafting Team's responses to stakeholder comments on the NPCC website.

STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF RFI

Upon receipt of the RFI response from the NPCC Manager of Reliability Standards, the RSC shall elect to:

- Endorse the proposed interpretation response

- Direct the Drafting Team to return to STEP 3.5: DEVELOPMENT OF RESPONSE TO RFI to revise the proposed interpretation response
- Direct the Assistant Vice President Standards to forward the RFI to the NPCC Board of Directors for final Regional approval~~(s)~~

STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF RFI

Following endorsement by the RSC, interpretation responses require review and ~~filing~~approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the interpretation response as presented
- Approve the interpretation response with ~~FERC~~comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive revisions to the interpretation response.]
- Remand the interpretation response back to the RSC and the Drafting Team to address their concerns

Upon receipt of Board approval, the NPCC Manager of Reliability Standards shall notify NERC of the approved interpretation for processing in accordance with NERC procedures, as applicable ~~Canadian~~.

FIGURE 2: FLOWCHART OF REGIONAL STANDARDS INTERPRETATION PROCESS

Placeholder for flowchart

4. WITHDRAWAL OF A REGIONAL STANDARD PENDING APPROVAL

The term "withdrawal" as used herein, refers to the revocation of a request for approval of a regional standard, variance, interpretation or definition that has been approved by the NPCC Board of Directors and has not been filed with Applicable Governmental ~~and/or Regulatory~~ Authorities ~~for adoption.~~or has been filed but not yet approved by Applicable Governmental Authorities. The RSC may withdraw a regional standard, variance, interpretation or definition for good cause upon approval by the NPCC Board of Directors. Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards will notify NERC Staff to petition the Applicable Governmental Authorities, as necessary, to allow for withdrawal.

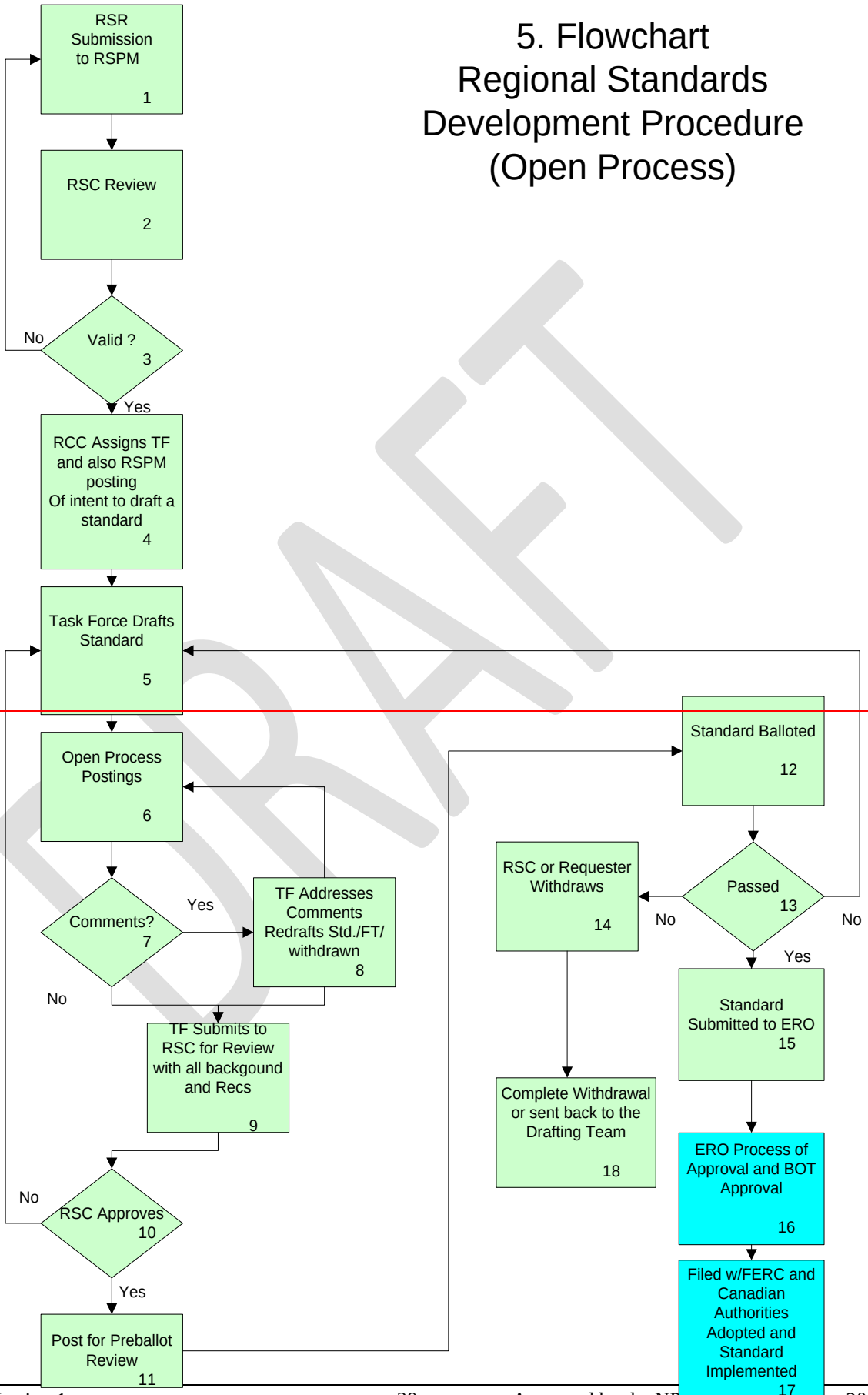
~~Once a reliability standard is adopted and made effective, all users, owners, planners, and operators of the Bulk Power System in the NPCC geographic area of the Northeast are required to comply with the standard. The NERC/ERO Board of Trustees has established a separate compliance program, also administered in the Northeast by NPCC , to measure compliance with the standards and administer sanctions as appropriate. After adoption of a NPCC Regional Standard, the standard will be forwarded to the compliance program for compliance monitoring and enforcement.~~

~~**STEP 18: WITHDRAWAL OF STANDARD**~~

~~Upon rejection of a proposed standard, the RCC or the requester may withdraw the standard completely or remand it back to the Task Force acting as the standard drafting team for further work.~~

DRAFT

5. Flowchart Regional Standards Development Procedure (Open Process)



DRAFT

~~**6. ERO and Regulatory Process and Approvals**~~

- ~~**NERC/ERO Comment Period** – NERC/ERO shall publicly notice and request comment on the NPCC Regional Reliability Standard, allowing a minimum of 45 calendar days for comment on NERC's website and actively notify all adjoining Regions. Concurrent with this regional posting, final drafts will be forwarded to NERC for posting on the NERC website to ensure full industry awareness of the standard and expedite and coordinate all commenting. All comments will be responded to electronically through a posted response on the NPCC website or a link on the NERC website. NPCC shall have an opportunity to resolve any objections identified in the comments and may choose to withdraw the request, revise the NPCC Regional Reliability Standard and request another posting for comment, or submit the NPCC Regional Reliability Standard along with a response to any objections received, for approval by NERC.~~

- ~~**NERC/ERO Approval of NPCC Regional Reliability Standards** – Proposed regional reliability standards shall be subject to approval by the NERC/ERO who shall have a process to evaluate and recommend whether a proposed non-Interconnection-wide NPCC Regional Reliability Standard has been developed in accordance with all applicable procedural requirements and whether NPCC has considered and addressed stakeholder objections. NPCC Board, having been notified of the results of the regional ballot concerning a NPCC Regional Reliability Standard, shall vote to submit the Standard to the NERC/ERO Board for approval as a NERC Reliability Standard. The NERC/ERO Board shall consider NPCC's request, the scope and implications of the Standard, the recommendation for action on the Standard, any unresolved stakeholder comments, and NPCC's consideration of comments and unresolved issues if any, in determining whether to approve the NPCC Regional Reliability Standard as a NERC Reliability Standard.~~

- ~~**Regulatory Authority Approval** – An NPCC Regional Reliability Standard that has been approved by the NERC/ERO board shall be filed with FERC and applicable Canadian Governmental and/or Regulatory Authorities for approval and shall become effective and enforceable within the U.S., per Section 215 of the Federal Power Act, only when adopted by FERC, and within Canada, only when adopted by applicable Canadian Governmental and/or Regulatory Authorities. The regional reliability standard, once adopted will be made part of the body of NERC reliability standards and shall be mandatory and enforceable on all applicable bulk power system owners, operators, and users within the NPCC Region, regardless of membership status.~~

5. Retirement of an Approved NPCC Regional Standard

The term "retirement" refers to the discontinuation of a regional standard, variance, interpretation or definition that: 1) has been approved by Applicable Governmental Authorities and 2) is not being superseded by or merged into a new or revised regional standard, interpretation or definition.

DRAFT

Upon identification of a need to retire a regional standard, variance, interpretation or definition, where the item will not be superseded by a new or revised version, a RSAR containing the proposal to retire a regional standard, variance, interpretation or definition will be posted for a comment period and ballot in the same manner as a Reliability Standard. The proposal shall include the rationale for the retirement and a statement regarding the impact of retirement on the reliability of the Bulk Electric System. Upon approval by the NPCC Members and the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the request for retirement to NERC, as the Electric Reliability Organization, for approval and to subsequently petition the Applicable Governmental Authorities to allow for retirement.

6. Approval of Process Waiver

While it is NPCC's intent to adhere to this manual under normal circumstances, NPCC may need to develop a new or modified regional standard, implementation plan, variance, interpretation or definition under extenuating circumstances. Extenuating circumstances may include, but not be limited to, specific time constraint imposed by a regulatory body and urgent reliability issue that requires expedited handling outside of the normal regional Reliability Standards process.

The RSC, by two-thirds (2/3) majority vote, may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:

- Where necessary to meet regulatory deadlines
- Where necessary to address an urgent reliability issue identified by regulatory and/or governmental authorities, including response to national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber-attack on the Bulk Electric System
- Where necessary to meet deadlines imposed by the NPCC Board of Directors
- Where the RSC determines that a revision to a proposed regional standard, implementation plan, variance, interpretation or definition has already been vetted by the industry through the standards development process or is so insubstantial that developing the revision through the processes contained in this manual will add significant time delay without any corresponding benefit.

In no circumstances shall this provision be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

A waiver request may be submitted to the RSC by any entity or individual, including NPCC committees or subgroups and NPCC Standards Staff. Prior to consideration of any waiver request, the NPCC Manager of Reliability Standards must provide notification to stakeholders at least five (5) business days prior to RSC consideration and action. Posting the waiver request on the NPCC website satisfies the notification provision.

Action on the waiver request will be included in the minutes of the RSC. Following the approval of the RSC to waive any provision of the regional Reliability Standards process, the Assistant Vice President Standards shall report the exercise of this waiver provision to the NPCC Board of Directors prior to adoption of the related Reliability Standard, interpretation, definition or variance. Actions taken pursuant to an approved waiver request will be posted on the NPCC Standards webpage.

DRAFT

In addition,

7. PROCESS FOR CORRECTING ERRATA

From time to time, an error may be discovered in a regional standard after it has received final ballot approval by the NPCC ballot body. Such errors may be corrected by the RSC without re-balloting if the RSC agrees that the correction of the error does not change the scope or intent of the associated regional standard, and agrees that the correction has no material impact on the end users of the regional standard.

If the regional standard containing errata is pending approval by the NPCC Board of Directors, the corrected regional standard shall be presented to the NPCC Board for approval in lieu of the regional standard approved by the NPCC ballot body.

The NPCC Board of Directors has resolved to concurrently approve any errata approved by the RSC associated with a regional standard that has received prior approval by the NPCC Board. If the regional standard containing errata is:

- Pending filing with NERC for approval, the corrected regional standard approved by the RSC shall be filed with NERC for approval in lieu of the regional standard approved by the NPCC Board of Directors
- Filed with NERC for approval, then the correction shall be filed for approval with NERC

~~7.~~8. APPEALS

- Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the ~~development,~~ approval, revision, reaffirmation, or withdrawal of a regional ~~reliability~~ standard (appellant) shall have the right to appeal. This appeals process applies only to the regional standards process as defined in this ~~procedure~~manual.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within thirty (30) calendar days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

- LEVEL 1 APPEAL

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the ~~RSPM~~NPCC Manager of Reliability Standards that describes the substantive or procedural action or inaction associated with a ~~reliability standard~~Reliability Standard or the standards process. The appellant describes in the complaint the actual or potential adverse

impact to the appellant. Assisted by any necessary ~~staff~~NPCC Standards Staff and ~~committee~~Committee resources, the ~~RSPM~~NPCC Manager of Reliability Standards shall prepare a written response addressed to the appellant as soon as practical, but not more than forty-five (45) calendar days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response will be made a part of the public record associated with the standard and posted with the standard.

- LEVEL 2 APPEAL

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the ~~regional standards process manager~~NPCC Manager of Reliability Standards, the ~~RSPM~~NPCC Board of Directors shall ~~convene~~appoint a five member panel to serve as a Level 2 Appeals Panel. ~~This panel shall consist of five members total appointed by the NPCC's board.~~

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The ~~RSPM~~NPCC Manager of Reliability Standards shall post the complaint and other relevant materials and provide at least a thirty (30) calendar ~~days~~day notice of the meeting of the Level 2 Appeals Panel.

In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC with a statement of the issues and facts in regard to which unfair and/or inequitable action was taken, or which fair and/or equitable action was not taken. The panel may find for or against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise, approve, disapprove, or adopt a ~~reliability standard.~~Reliability Standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the NPCC Board of Directors for consideration at the time the ~~board~~Board decides whether to adopt a particular ~~reliability standard~~Reliability Standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than thirty (30) calendar days after the announcement of the vote on the standard in question.

DRAFT

DRAFT

APPENDIX A-: RSAR COMPLETION GUIDELINES

The Requester shall complete a RSAR form in accordance with the guidance provided below.

The RSAR, at a minimum, shall contain information in the required fields in order to be qualified for consideration. The NPCC Manager of Reliability Standards will assist the Requester to ensure all required information is submitted on the RSAR.

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC ~~Regional~~Manager of Reliability Standards ~~Process Manager,~~, at ~~NPCCstandard@npcc.org~~ .npccstandard@npcc.org. The NPCC ~~Regional~~Manager of Reliability Standards ~~Process Manager~~ shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:	***[Required Field]***
Request Date:	***[Required Field]***

RSAR Requester Information

Name:	***[Required Field]***	**RSAR Type -(Check box for one of these selections.)**
Company:	***[Required Field]***	☐ New Standard
Telephone:	***[Required Field]***	☐ Revision to Existing Standard
Fax:		☐ Withdrawal of Existing Standard
Email:	***[Required Field]***	☐ Urgent Action

~~Purpose (**Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.**)~~

~~Industry Need (Provide **a detailed statement justifying the need for the proposed standard, along with any supporting documentation.**)~~

~~Brief Description (**Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.**)~~

Purpose: (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.)

[Required Field]

Industry Need: (Provide a detailed statement justifying the need for the proposed standard, along with a technical justification and any supporting documentation.)

[Required Field -- must include technical justification (relevant studies, documentation, etc.) for a new standard or revision to an existing standard.]

Brief Description: (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.)

[Required Field]

Reliability Functions *[Required Field]*

The Standard will Apply to the Following Functions (Check all applicable boxes.)		
☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.

☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission Operator	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.
☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected ~~bulk power systems~~Bulk Electric System 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 power systems~~Bulk Electric System 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 power systems~~Bulk Electric System 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 power systems~~Bulk Electric System 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 power systems.~~Bulk Electric System.
☐	6. Personnel responsible for planning and operating interconnected ~~bulk power systems~~Bulk Electric System shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected ~~bulk power systems~~Bulk Electric System shall be assessed, monitored, and maintained on a wide-area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
Recognizing that reliability is an Common Attribute of a robust North American economy:	
1. A reliability standard shall not give any market participant an unfair competitive advantage~~. Yes~~. Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. ~~Yes~~ Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. ~~Yes~~ Yes	
4. A reliability 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~~ Yes	

Detailed Description: (Provide enough detail so that an independent entity familiar with the industry could draft a standard based on this description.)

[Required Field – Provide: 1) Necessary information to assist the Drafting Team (which is to include relevant study results and documentation), to the extent feasible,

to allow them to draft the standard, 2) Any existing known cross references to NPCC or NERC documents and 3) Technical background for the RSAR to properly address the need for the standard.]

Related Standards *[Required Field, to extent known]*

Standard No.	Explanation

Related SARs or RSARs *[Required Field, to extent known]*

SAR ID	Explanation

APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS

A regional standard Drafting Team shall be comprised of Subject Matter Experts (SMEs) from NPCC Task Forces and Working Groups as determined by the RCC, and from industry. The guidelines provided herein primarily address overall team requirements and more specifically those of a SME.

Formal membership on a Drafting Team should be reserved only for those individuals who intend to work consistently, diligently, and professionally on what is required to be done for a regional standard. Drafting Team members are expected to contribute meaningfully to the ongoing development of the standard.

Drafting team members must be:

- Committed to participating in scheduled Drafting Team meetings, teleconferences, as well as industry outreach (e.g., workshops and webinars)
- Willing to lead teams / sub-teams, as necessary
- Champions for standard development and promoters of the approval of the standard
- Open to consider the comments of others and provide constructive feedback

Subject Matter Experts should possess the necessary expertise and knowledge regarding the topic of the standard. The SMEs should represent a cross section of the registered entities applicable to the standard under development as well as geographical areas within the NPCC footprint.

Industry stakeholders may nominate themselves for consideration by the NPCC Regional Standards Committee (RSC) for the specific Drafting Team vacancies by completing the following Drafting Team Self Nomination form and submitting it to NPCC Manager of Reliability Standards, at npccstandard@npcc.org.

Nomination Form for NPCC [Name of Drafting Team] Drafting Team

Please return this form as soon as possible. If you have any questions, please contact the NPCC Standards Staff at npccstandard@npcc.org.

By submitting the following information you are indicating your willingness and agreement to actively participate in the Drafting Team meetings if appointed to the Drafting Team by the NPCC Regional Standards Committee (RSC). This means that if you are appointed to the DT you are expected to attend all (or at least the vast majority) of the face-to-face DT meetings as well as participate in all the DT meetings held via conference calls. Failure to do so shall result in your removal from the DT.

Name:	
Organization:	
Address:	
Telephone:	

E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Drafting Team.

If you are currently a member of any NERC or Regional drafting teams, please list each team here.

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

_____

_____

_____

_____

If you previously worked on any drafting team please identify the team(s).

☐ No prior NERC or Regional SAR or standard drafting team experience.

☐ Prior experience on the following team(s):

Select each NERC Region that you represent:	**Select each Industry Segment that you represent:**	
☐ ERCOT	☐	1 — Transmission Owners
☐ FRCC	☐	2 — RTOs, ISOs
☐ MRO	☐	3 — Load-serving Entities
☐ NPCC	☐	4 — Transmission-dependent Utilities
☐ RFC	☐	5 — Electric Generators
☐ SERC	☐	6 — Electricity Brokers, Aggregators, and Marketers
☐ SPP	☐	7 — Large Electricity End Users
☐ WECC	☐	8 — Small Electricity End Users
☐ NA – Not Applicable	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities
	☐	NA – Not Applicable

Select each Function[18] in which you have current or prior expertise:

☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner

[18] These functions are defined in the NERC Functional Model, which is downloadable from the NERC website.

☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group.			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS

NPCC regional standards and the Regional Standards Process Manual are living documents that will be updated periodically to remain current and viable (e.g., respond to changing conditions, as well as to incorporate lessons learned and process improvements).

MAINTENANCE OF REGIONAL STANDARDS

NPCC regional standards will be posted for open process review by the RSC for possible revision at least once every five (5) years after the first regulatory approval and follow the same process as in the case of a new standard. If no changes are warranted, the Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or retire a regional standard, a Regional Standard Authorization Request shall be prepared by the RSC and submitted in accordance with the NPCC regional standards process. The existing, approved standard subject to revision will remain in effect until such time as the revised version has received FERC or applicable Provincial Governmental Authorities approvals, as appropriate, at which time it will be retired in accordance with any applicable implementation plan associated with the newly approved regional standard.

MAINTENANCE OF THE REGIONAL STANDARDS PROCESS

This NPCC Regional Standards Process will be reviewed for possible revision at least once every five (5) years, or more frequently if needed, and subject to the same procedure as applies to the development of a Regional Standard. All such revisions shall be subject to approval by the NPCC Board of Directors, NERC Board of Trustees, FERC, and may be subject to approval, if required, by Applicable Governmental Authorities in Canada.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 28, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

RE: Errata to Petition of the North American Electric Reliability Corporation for Approval of Amendments to Regional Reliability Standards Development Procedure of the Northeast Power Coordinating Council, Inc.
Docket No. RR14-7-000

Dear Ms. Bose:

On September 15, 2014, the North American Electric Reliability Corporation ("NERC") filed a Petition for Approval ("Petition") of Proposed Amendments to Regional Reliability Standards Development Procedure of the Northeast Power Coordinating Council, Inc. ("NPCC") with the Federal Energy Regulatory Commission. It has come to NERC's attention that the Petition included an incorrect "Redline" version of the newly renamed NPCC Regional Standards Process Manual (RSPM) in Attachment 2 of the Petition, thus causing an inconsistency between the "Clean" and "Redline" versions therein. The "Clean" version of the RSPM submitted as Attachment 1 of this Petition is correct.

Accordingly, NERC requests approval of the "Clean" version in the Petition. The attached corrected "Redline" in Attachment 1 of this Petition will assist the Commission and others in evaluating the proposed changes.

Respectfully submitted,

/s/ William H. Edwards

William H. Edwards
Counsel for North American Electric Reliability Corporation

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

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 28th day of October, 2014.

/s/ William H. Edwards

William H. Edwards
Counsel for North American
Electric Reliability Corporation

Attachment 1

Revised Regional Reliability Standards Development Procedure of the Northeast Power Coordinating Council, Inc.

Redline

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

NPCC, Inc.

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

Northeast Power Coordinating Council, Inc.

Regional ~~Reliability Standards~~Standard Processes Manual (RSPM)

~~Development Procedure~~



~~Approved by NPCC Board of Directors~~
~~September 19, 2007~~
~~Approved by NERC BOT October 23, 2007~~
~~Adopted by FERC March 21, 2008~~

~~NPCC~~



Adopted by FERC: XXXX XX, 20XX

Approved by NERC Board of Trustees: August 14, 2014

Approved by NPCC Board of Directors: March 11, 2014

Revision History

Version	NPCC Board of Directors Approval	NERC Board of Trustees Approval	FERC Approval
0	9/19/07	10/23/07	3/21/08
1	3/11/14	8/14/14	xx/xx/xx

NPCC REGIONAL RELIABILITY STANDARDS ~~DEVELOPMENT PROCEDURE~~PROCESS MANUAL

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY~~2~~ 3

II. INTRODUCTION 4

PURPOSE 4

BACKGROUND 4

III. REGIONAL ~~RELIABILITY~~ STANDARD ~~DEVELOPMENT PROCEDURE~~CHARACTERISTICS AND ELEMENTS 5

1. CHARACTERISTIC ATTRIBUTES ~~2~~ 5

2. EL EMENTS OF A REGIONAL ~~-~~STANDARD ~~5~~

~~3. TERMS AND FUNCTIONS 8~~

~~4. PROCEDURE DESCRIPTION 10~~

~~5. FLOWCHART 15~~

..... ~~6. ERO AND REGULATORY APPROVALS 16~~

~~7. APPEALS 16~~

TYPES OF RELIABILITY REQUIREMENTS *6*

ELEMENTS OF A REGIONAL STANDARD *7*

IV. REGIONAL STANDARDS DEVELOPMENT PROCESS 9

1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS 9

NOMINATION, REVISION, CLARIFICATION, OR RETIREMENT OF A STANDARD: *9*

PROCESS ROLES AND RESPONSIBILITIES *9*

2. STANDARD DEVELOPMENT PROCESS STEPS 11

STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE *11*

STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD *12*

STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS

.....13
STEP 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 14
STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS 16
STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL.....17
STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL 18
STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD 18
3. STANDARD CLARIFICATION PROCESS STEPS 19
STEP 3.1: REGIONAL STANDARDS CLARIFICATION REQUEST (CR) 19
STEP 3.2: REVIEW AND VALIDATION OF CLARIFICATION REQUEST (CR) 19
STEP 3.3: NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS 20
STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO CR.....20
STEP 3.5: DEVELOPMENT OF RESPONSE TO CR.....20
STEP 3.6: POSTING CR FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS 21
STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF CR 21
STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF CR 21
4. DISCONTINUANCE OF REGIONAL STANDARD DEVELOPMENT 22
5. WITHDRAWAL OF A REGIONAL STANDARD PENDING APPROVAL 23
6. RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD 23
7. APPROVAL OF PROCESS WAIVER 23
8. PROCESS FOR CORRECTING ERRATA 24
9. APPEALS..... 24
LEVEL 1 APPEAL 25
LEVEL 2 APPEAL 25
~~III.~~ APPENDIX
A~~)~~ ~~:~~ RSAR ~~FORM 19~~COMPLETION GUIDELINES A1

APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS B1
APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS ... C1
MAINTENANCE OF REGIONAL STANDARDS C1
MAINTENANCE OF THE REGIONAL STANDARDS PROCESS C1
APPENDIX D: NPCC CLARIFICATION REQUEST D1

I. EXECUTIVE SUMMARY

~~The purpose of the Northeast Power Coordinating Council, Inc. ("NPCC"), is to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of more stringent and specific regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards pursuant to the execution and implementation of a Regional Delegation Agreement with the Electric Reliability Organization ("ERO") and applicable Canadian Memoranda of Understanding that are backstopped by the Federal Energy Regulatory Commission ("FERC") and Canadian Provincial authorities. In the development and enforcement of Regional Reliability Standards, NPCC, to the extent possible, facilitates attainment of fair, effective, efficient, and competitive electric markets.~~

~~General Membership in NPCC is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the ERO that has an interest in the reliable operation of the Northeastern North American bulk power system.~~

The NPCC Bylaws state "NPCC shall develop a Regional Reliability Standards Development Procedure that provides the design-basis approach to a consensus building process by which NPCC may develop Regional Reliability Standards and Regional Variances to be proposed to the ERO for adoption, under delegated authority by the FERC and the Canadian Provincial regulatory and/or governmental authorities."

The NPCC Regional Reliability Standards Development Procedure was originally adopted by the NPCC Board of Directors on September 19, 2007. The NPCC Reliability Standards Staff in concert with the NPCC Regional Standards Committee (RSC) has completed a revision to the NPCC Regional Reliability Standards Process Manual to incorporate process improvements, provide greater clarity and reflect the new NPCC Cost Effectiveness Analysis Procedure (CEAP).

Key changes addressed in this revision include:

- Replacing interpretation with clarification and expanding the Clarification Section narrative into process steps and including an associated flowchart
- Creating separate sections for: 1) Withdrawal of a Regional Standard Pending Approval; 2) Retirement of an Approved NPCC Regional Standard; and 3) Approval of Process Waiver; 4) Process for Correcting Errata
- Recognizing the new NPCC Cost Effectiveness Analysis Procedure (CEAP)
- Identifying the Reliability Standard Audit Worksheet (RSAW) as a companion document to a regional standard that needs to be collaboratively developed by the drafting team and NPCC Compliance Staff
- Creating three new appendices: 1) Appendix A: Regional Standard Authorization Request (RSAR) Completion Guidelines and Form; 2) Appendix B: Selection of drafting team Members and Nomination Form; and 3) Appendix C: Maintenance of Regional Standards and Process

In addressing areas for improvement in the NPCC Regional Reliability Standards Development Procedure, recent improvements made to the NERC Standards Process Manual (e.g., Standards Process Input Group (SPIG) recommendations) as well as the manuals of other Regional Entities were benchmarked to identify best practices for inclusion in this manual.

The process improvements and clarity captured in this revision to NPCC Regional Reliability Standards Development Procedure, will result in a more timely and efficient manner to address the development of regional standards to ensure the reliability of the Bulk Electric System within the NPCC geographical area.

II. INTRODUCTION

PURPOSE

This manual defines the characteristics of a Northeast Power Coordinating Council, Inc. (NPCC) regional Reliability Standard (hereinafter referred to as "regional standard") and establishes the process by which NPCC regional standards are developed, approved, revised, clarified and retired. The NPCC regional standards process is a stakeholder process that is approved by the NPCC members to ensure a transparent standard development process that is "open, fair, and inclusive."

~~The NPCC Regional Reliability Standards Development Procedure describes the procedures, policies and practices implemented to ensure an "open, fair, and inclusive" process for the transparent initiation, development, implementation and revision of NPCC Regional Reliability Standards necessary for the reliable operation~~NPCC regional standards address the reliability of the international and interconnected ~~bulk power system~~ Bulk Electric System in~~-~~ Northeast ~~-~~North America. ~~These Standards~~NPCC regional standards shall enable or support one or more NERC/ERO reliability principles[1] and will, in all cases, not be inconsistent with or less stringent than any requirements of the North American Electric Reliability Council/Electric Reliability Organization (NERC/ERO) ~~Reliability Standards. The procedure will not unnecessarily delay the development of the proposed reliability standards. Each regional reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of pertinent reliability principles and criteria, thereby ensuring that no standard undermines reliability through an unintended consequence~~continent-wide Reliability Standards.

The development of NPCC regional standards is performed according to the following principles using the process contained in this manual:

- Developed in a fair and open process that provides an opportunity for all interested parties to participate;
- Does not have an adverse impact on commerce that is not necessary for reliability;
- Provides a level of Bulk Electric System reliability that is adequate to protect public health, safety, welfare, and national security and would not have a significant adverse impact on reliability; and
- Based on a justifiable difference between Regions or between sub-Regions within the Regional geographic area.

Following industry approval, NPCC regional standards process and NPCC regional standards require approval by the NPCC Board of Directors, NERC as the Electric Reliability Organization (ERO) and the applicable regulatory authorities in the United States (FERC) and Canada.

BACKGROUND

Northeast Power Coordinating Council, Inc. (NPCC) is responsible for promoting and improving the reliability of the international, interconnected Bulk Electric System in Northeastern North America. NPCC carries out its mission through (i) the development of regional standards and compliance assessment and enforcement of continent-wide and regional standards, coordination of system planning, design and operations, and assessment of reliability, (collectively, "Regional Entity activities"), and (ii) the establishment of regionally-specific criteria, and monitoring and enforcement of compliance with such criteria (collectively, "criteria services activities").

The Energy Policy Act (EPA) of 2005 (Section 1211) amended the Federal Power Act (FPA) by

adding Section 215, Electric Reliability. Specifically regarding standards development and pursuant with Section 215(e)(4) of the FPA, NPCC as a Regional Entity with delegated authority from NERC may propose regional standards to NERC for eventual enforcement within the NPCC region.

[1] Reliability Principles are available on the NERC website as amended from time to time

As a condition of NPCC membership, NPCC General and Full Members[2] agree to adhere to NERC Reliability Standards. NERC Reliability Standards are comprised of both continent-wide and regional standards. The NPCC regional standards apply only to that part of the Eastern Interconnection within the NPCC geographical area.

III. ~~II.~~ REGIONAL ~~RELIABILITY~~ STANDARD ~~DEVELOPMENT PROCEDURE~~CHARACTERISTICS AND ELEMENTS

1. CHARACTERISTIC ATTRIBUTES

~~The NPCC Regional Reliability Standards Development Procedure is:~~

~~• **Open** The NPCC Regional Reliability Standards Development Procedure provides any person the ability to participate in the development of~~ The NPCC regional standards development process has the following key characteristics:

- **Fair due process** — The NPCC regional standards development process provides for reasonable notice and opportunity for public comment. At a minimum, the procedure shall include public notice of the intent to develop a standard~~. Any entity that is~~, a public comment period on the proposed standard, due consideration of those public comments, and a ballot of interested stakeholders. Upon approval by the NPCC Members, the NPCC Board of Directors then votes to approve submittal of the regional standard to NERC for ERO approval, followed by submission to FERC and Canadian Authorities for their approvals.
- **Openness** — Participation in the NPCC regional standards development process is open to all persons and organizations that are directly and materially affected by the reliability of the NPCC's ~~bulk power system has the ability to participate in the development and approval of reliability standards.~~Bulk Electric System. There ~~are~~is no undue financial ~~barriers~~burden to participation. ~~—~~Participation ~~in the open comment process is~~shall not ~~conditional~~be conditioned upon membership in the ERO, NPCC or any organization, and ~~participation is~~shall not be unreasonably restricted on the basis of technical qualifications or other such requirements.~~ NPCC utilizes a website to accomplish this. Online posting and review of standards and the real time sharing of comments uploaded to the website allow complete transparency.~~

- **Inclusive** ~~— The NPCC Regional Reliability Standards Development Procedure provides any~~ — Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the reliability of NPCC's Bulk Electric System has the right to participate by: (a) expressing an opinion and its basis~~, have that~~; (b) having their position considered, and ~~appealed~~(c) having the right to appeal a response through an established ~~appeals~~appeal process ~~if adversely affected~~.

- ~~**Balanced** — The NPCC Regional Reliability Standards Development Procedure has a balance of interests and all those entities that are directly and materially affected by the reliability of the NPCC's bulk power system are welcome to participate~~• **Balanced** — The NPCC regional standards development process strives to have an appropriate balance of interest and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter. ~~This will be accomplished through~~ Pursuant with the NPCC ~~Bylaws defining eight~~By- Laws[3] there are seven (7) stakeholder voting sectors ~~(categories)~~and the votes for ~~voting~~each sector are weighted to achieve an appropriate balance.

  - ~~**Fair Due Process** — The NPCC Regional Reliability Standards Development Procedure provides for reasonable notice and opportunity for public comment. The procedure includes public notice of the intent to develop a standard, a 45 calendar day public comment period on the proposed standard request, or standard with due consideration of those public comments, and responses to those comments will be posted on the NPCC website. A final draft will be posted for a 30 calendar day pre-balloting period, and then a ballot of NPCC Members will be conducted. Upon approval by the NPCC Members, the NPCC Board then votes to approve submittal of the Regional Standard to NERC.~~

- **Transparent** ~~——~~ All ~~–~~actions ~~–~~material ~~–~~to ~~–~~the ~~–~~development ~~of Regional Reliability Standards~~ of NPCC regional standards are transparent and information regarding the progress ~~is posted~~of a standard's development action is made available to the public through postings on the NPCC website as well as through ~~extensive email~~E- mail lists.

- **Without undue delay** — The NPCC regional standards development process shall be performed within a reasonable time.

In as much as NPCC is one of ~~several regional entities~~six Regional Entities within the Eastern Interconnection of North~~-~~
America, there will be no presumption of validity by the ERO ~~–~~for~~–~~ any ~~–~~NPCC ~~Regional Reliability Standard.~~ regional standard.

[2] As defined in the NPCC By-Laws – available on the NPCC website
[3] NPCC By-Laws are available on the NPCC website

In order to receive the approval of the ERO, the NPCC ~~Reliability Standards Development Process~~regional standards development process must also achieve the following objectives:

- **No Adverse Impact on Reliability of the Interconnection** — ~~An NPCC Regional Reliability Standard provides a level of bulk power system reliability that is necessary and adequate to protect public health, safety, welfare, and North American security and will not have an adverse impact on the reliability of the Interconnection or other Regions within the Interconnection~~ A NPCC regional standard provides an Adequate Level of Reliability[4] as defined by NERC.

- **Justifiable Difference** — ~~An NPCC Regional Reliability Standard is based on justifiable differences between Regions, such as different electrical systems or facilities, sensitivity of load to disruptions, sensitivity of generation to disruptions, frequency and voltage sensitivity, system operating limit development and facilities ratings process, electrical system interactions, etc.~~

- ~~**Uniformity** NPCC Regional Reliability Standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk~~

power system of the North American continent. A NPCC Reliability Standard shall be more stringent than a continent-wide reliability standard, may include a regional variation that regional standard addresses matters that the continent-wide reliability standard does not, or shall be a regional a justifiable difference necessitated bywithin the NPCC geographical area that results from a physical difference[5] or operating difference in the northeast's bulk power system, where the interpretation of the phrase "physicalNortheast's Bulk Electric System. Although a justifiable difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

- allows for a unique regional standard, a NPCC regional standard shall be no less stringent than a continent-wide standard.

- **Uniformity** — To the extent possible, the NPCC regional standards provides uniformity with Reliability Standards across the interconnected Bulk Electric System of North America.

- **No Undue Adverse Impact on Commerce** — AnA NPCC Regional Reliability Standardregional standard will not cause any undue adverse impact on business activities that are not necessary for reliability of the Region and its interconnected Regions. All regional reliability standards shall be consistent with NERC's market principlesprinciples[6].

Other Attributes of the NPCC Regional Reliability Standards Development Procedure include;

- **Maintenance of Regional Reliability Standards** NPCC Regional Standards will be reviewed for possible revision at least every three years and follow the same process as a new standard. The old standard will remain in place until such time as the revised version has passed through the entire process, at which point the old standard will be retired in accordance with any applicable new implementation plan associated with the approved revised standard. The review process shall be conducted by soliciting comments from the stakeholders and through open posting on the NPCC website. If no changes are warranted, Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or withdraw a standard, a regional standard authorization request shall be prepared by the RSC and submitted in accordance with the standards development process contained in this procedure.

- **Maintenance of Regional Reliability Standards Development Procedure** This NPCC Regional Reliability Standards Development Procedure will be reviewed for possible revision at least once every five years or more frequently if needed and subject to the same procedure as that of the development of a standard. All such revisions shall be subject to approval by the NPCC Board, NERC, FERC, and could be subject to approval, if required, by applicable authorities in Canada. The NPCC RSC has the authority to make non-substantive changes to this procedure and subsequently notify the NPCC Board for their concurrence at their next scheduled meeting.

- **Interpretation of Standards** All persons who are directly and materially

~~affected by the NPCC's bulk power system reliability shall be permitted to request an interpretation of a standard. The person requesting an interpretation will send an email request to the Regional Standards Process Manager (RSPM), as noted on the NPCC website, explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material~~

impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard. The RSPM along with guidance from the RSC will forward the request to the originating Task Force which acted as the drafting team for that regional reliability standard. The Task Force will address, through a written response, the request for clarification as soon as practical, but not more than 45 business days from its receipt by the Task Force. This written interpretation will be posted along with the final approved and adopted standard and will stand until such time as the standard is revised through the normal RSAR process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.

2. ELEMENTS OF A RELIABILITY REGIONAL STANDARD

- **Elements of a Regional Reliability Standard**

  To ensure uniformity of regional reliability standards and avoid inconsistency with NERC continent-wide standards, a NPCC regional reliability standard shall consist ofbe consistent with the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of regional standards. This The application of a systematic discipline is necessary tofor achieving regional standards that are measurable, enforceable, and consistent.

All mandatory requirements of a regional reliability standard shall be within the standard document. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself .

The most current version of the approved NERC Reliability Standard template and its associated elements as or if applicable, will be used at the time of the development of the NPCC Regional Reliability Standard to ensure all essential elements are contained therein to achieve consistency and uniformity and meet all statutory requirements. A sample of the elements contained in the standard appears in Table 1 below, however the latest ERO Board approved Standard template, that may be found on the NERC website, will supersede the list below at the time the regional standard is developed.

Table 1- Elements of a Regional Reliability Standard

Identification Number	A unique identification number assigned in accordance with an administrative classification system to facilitate tracking and reference. (i.e. "NPCC- BAL-002-0-Date" which refers to NPCC Regional Standard, referencing NERC BAL-002 Version 0, with NPCC Effective Date final adoption by all Regional Authorities)
Title	A brief, descriptive phrase identifying the topic of the standard.
Applicability	Clear identification of the functional classes of entities responsible for complying with the standard, noting any specific additions or exceptions. The standard will be applicable to the Bulk Power System unless otherwise noted.
Effective Date	The effective date of the standard or, prior to approval of the

and Status	standard, the proposed effective date.
Purpose	The purpose of the standard. The purpose shall explicitly state what outcome will be achieved or is expected by this standard.
Requirement(s)	Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Each statement in the requirements section shall be a statement for which compliance is mandatory.
Risk Factor(s)	The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below: A High Risk Factor requirement (a) is one that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, 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, or could hinder restoration to a normal condition. A Medium Risk Factor requirement (a) is a requirement that, if violated, 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; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk power system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. A Lower Risk Factor 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.

Measure(s)	Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.

Table 2 — Compliance Elements of a Regional Reliability Standard

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible for providing the data or information for measuring performance or outcomes. • The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating data or information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Measurement data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Supporting Information Elements

Interpretation	Any interpretation of regional reliability standard that is developed and approved in accordance with the "Interpretation of Standards" section of Appendix A of this procedure, to expound on the application of the standard for unusual or unique situations or to provide clarifications.
Implementation Plan	Each regional reliability standard shall have an associated implementation plan describing the effective date of the standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the standard in the compliance program and other considerations in the initial use of the standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and is approved as part of the ballot of the standard.

Supporting References	This section references related documents that support reasons for, or otherwise provide additional information related to the regional reliability standard. Examples include, but are not limited to: • Glossary of terms • Developmental history of the standard and prior versions • Notes pertaining to implementation or compliance • Standard references • Standard supplements • Procedures • Practices • Training references • Technical references • White papers • Internet links to related information

3. TERMS AND FUNCTIONS

• **Regional Standards Committee (RSC)** – An NPCC committee charged with management of the NPCC Standards Procedure under a sector based voting structure as described in the NPCC Bylaws. The NPCC RSC will consider requests for new or revised standards and be available for advisement to the NPCC Board on the standards.

The RSC may not itself modify the standard without issuing a new notice to stakeholders regarding a vote of the modified standard. Any RSC action will only be activated in the event of a minor correction of a standard such as errata.

The RSC is an open and balanced stakeholder committee inclusive of all stakeholder interests that provide for or are materially impacted by the reliability of the bulk power system.

The RSC disposition regarding the regional standard authorization request, which will in all cases be within 60 calendar days of receipt of a completed standard request, shall include:

- Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The RSC may, at its discretion, expand or narrow the scope of the standard request under consideration. The RSC shall prioritize the development of standards in relation to other proposed standards, as may be required based on the volume of requests and resources.

- ~~Reject the standard request. If the RSC rejects a standard request, a written explanation for rejection will be delivered to the requester within 30 calendar days of the decision.~~

- ~~Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the RSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the RSC.~~

~~The NPCC Standard Process responsibilities of the RSC will include:~~

- ~~Review of NPCC Draft Standards for such factors as completeness, sufficient detail, rational result, and compatibility with existing standards; clarifying standard development issues not specified in this procedure. Under no circumstance will the RSC change the substance of a draft standard.~~

~~• Due consideration to the work of the drafting team~~ as well as ~~the comments of stakeholders and minority objections, in approving a~~results oriented[7], i.e.:

- Performance-based,
- Risk-based, and
- Capability-based.

TYPES OF RELIABILITY REQUIREMENTS

Regional reliability standards should be viewed as a portfolio of requirements designed to achieve an effective defense-in-depth strategy. Each requirement should identify a clear and measurable expected outcome, such as: a) a stated level of reliability performance, b) a reduction in a specified reliability risk, or c) a necessary competency.

a) **Performance-based** - defines a specific reliability objective or outcome that has a direct, observable effect on the reliability of the Bulk Electric System, i.e. an effect that can be measured using power system data or trends.

[4] Adequate Level of Reliability is available on the NERC website as amended from time to time

[5] The meaning of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

~~proposed regional reliability standard to go to ballot.~~

- ~~Approve standards for pre-ballot posting under a sector based voting structure as described later in the NPCC Inc. Bylaws or~~
- ~~Remand the standard back to the Task Force acting as the drafting team for further work or recommend a change in those participating in the drafting team (i.e. a new drafting team).~~

- ~~**Regional Standards Process Manager (RSPM)** - The Regional Reliability Standards Procedure shall be administered by a NPCC staff Regional Standards Process Manager. The RSPM is responsible for ensuring that the development and revision of standards is in accordance with this manual. The RSPM works to ensure the integrity of the process, format, consistency of~~

quality, and completeness of the reliability standards. The RSPM facilitates all steps in the process.

- **Reliability Coordinating Committee (RCC)** – The RCC, will support the standards development process through the assignment of NPCC Task Forces. They will also provide a technical advisory role in the Regional Reliability Standards development procedure through recommendations.

- **Requester** – A Requester is any individual or an entity (organization, company, government authority, etc.) that submits a complete request for development, revision, or withdrawal of a standard. Any person or an entity that is directly and materially affected by an existing standard or the need for a new standard may submit a request for a new standard or revision to a standard. The Requester is assisted by the RSAR drafting team (if one is appointed by the RSC) to respond to comments and to decide if and when the RSAR is forwarded to the RSC with a request to draft a standard. The Requester is responsible for the RSAR, assisted by the RSAR drafting team and Regional Standards Process Manager, until such time the RSC authorizes

development of the standard. The Requester has the option at any time to allow the RSAR drafting team to assume full responsibility for the RSAR. The Requester may chose to participate in subsequent standard drafting efforts related to the RSAR.

- **Task Forces and Working Groups,** The committees, task forces and working groups within NPCC , serve an active role in the standards process:
  - Identify the need for new or modified regional standards.
  - Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs).
  - Develop comments (views and objections) to standards actions.
  - Participate in NPCC Standard drafting.
  - Provide technical oversight in response to changing industry conditions and ERO Requirements.
  - Conduct Field Tests as required

4. PROCEDURE DESCRIPTION

STEPS 1 AND 2: REQUEST TO DEVELOP A NEW [6] Market Principles are available on the NERC website as amended from time to time

[7] Results-based Standards see http://www.nerc.com/pa/Stand/Resources/Documents/ResultsBasedStandardGuidance.pdf

b) **Risk-based** - defines actions of entities that reduce a stated risk to the reliability of the Bulk Electric System and can be measured by evaluating a particular product or outcome resulting from the required actions.

c) **Capability-based** - defines capabilities needed to perform reliability functions and can be measured by demonstrating that the capability exists as required.

Each regional standard shall enable or support one or more of the reliability principles[8] as identified in the most recent set posted on the NERC website. Each regional standard shall also be consistent with all of the reliability principles. The intent of the set of NPCC regional standards is to deliver an Adequate Level of Reliability[9] as defined by NERC.

Recognizing that Bulk Electric System reliability and electricity markets are inseparable and mutually interdependent, all regional standards shall be consistent with the most recent set of Market Principles[10] as posted on the NERC website. Consideration of the Market Principles is intended to ensure that regional standards are written such that they achieve their reliability objective without placing undue restrictions or causing adverse impacts on competitive electricity markets.

ELEMENTS OF A REGIONAL STANDARD

A regional standard includes several components designed to work collectively to identify what entities must do to meet their reliability-related obligations as an owner, operator or user of the Bulk Electric System. The components of a NPCC regional standard identified below are based on the NERC Standard Processes Manual (SPM) that was approved by the NERC Board of Trustees at its February 2013 meeting. Future revisions of the NERC SPM will be used at the time of development of a NPCC regional standard if different from the elements listed below~~Requests to develop a new Regional Reliability Standard shall be submitted to the RSPM by completing a **Regional Standard Authorization Request** (RSAR) ***(see Appendix A)***. The RSAR is a description of the new or revised standard in sufficient detail to clearly define the scope, purpose, and importance of the Regional Standard, impacted parties or other relevant information. A "needs" statement will provide the justification for the development of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard. The RSPM shall maintain the RSAR form and make it available electronically on the NPCC website.~~

~~Any person or entity ("Requester") directly or materially affected by an existing standard or the need for a new or revised standard may initiate a RSAR.~~

~~The Requester will submit the RSAR to the RSPM electronically and the RSPM will acknowledge receipt of the RSAR immediately, through electronic receipt. The RSAR, as a minimum, needs to contain the following information in order to be qualified for consideration. The NPCC RSPM will assist the Requester to ensure all the following information is submitted (on the RSAR) in a form appearing in Appendix A:~~

~~1. Proposed Title and Date of New RSAR~~
~~2. Requester's Name and Contact Information~~
~~3. Purpose of the Regional Standard~~
~~4. Description of Industry Need~~
~~5. Provide a Brief Description of the Standard~~

~~6.~~The only mandatory and enforceable components of a regional standard are the: (1) Applicability,

(2) Requirements, and (3) the Effective Dates. The additional components are included in the regional standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to functional entities concerning how compliance will be assessed by the Compliance Enforcement Authority.

The components of a regional standard may include the following:

Title:	A brief, descriptive phrase identifying the topic of the regional standard.
Number:	A unique identification number assigned in accordance with a published classification system to facilitate tracking and reference to the regional standards.
Purpose:	The reliability outcome achieved through compliance with the requirements of the regional standard.
Applicability:	Identifies which entities are assigned reliability requirements; i.e., the specific functional entities and facilities to which the regional standard applies.
Effective Dates:	Identification of the ~~Entities in the Functional Model as being~~date or pre-conditions determining when each Requirement becomes effective in each jurisdiction.

[8] Reliability Principles are available on the NERC website as amended from time to time
[9] Adequate Level of Reliability is available on the NERC website as amended from time to time
[10] Market Principles are available on the NERC website as amended from time to time

Requirement: An explicit statement that identifies the functional entity responsible ~~to adhere to the standard~~, the action or outcome that must be achieved, any conditions achieving the action or outcome, and the reliability-related benefit of the action or outcome. Each requirement shall be a statement for which compliance is mandatory.

~~7. Necessary information to assist the drafting~~

Compliance Elements: Elements to aid in the administration of compliance monitoring and enforcement responsibilities.

Measure: Provides identification of the ~~team, to~~ evidence or types of evidence that may demonstrate compliance with the ~~extent feasible, to allow them to draft the standard~~associated requirement.

Violation Risk Factors and Violation Severity Levels: Violation risk factors (VRFs) and violation severity levels (VSLs) are used as factors when determining the size of a penalty or sanction associated with the violation of a requirement in an approved Reliability Standard. Each requirement in each Reliability Standard has an associated VRF and a set of VSLs. VRFs and VSLs are developed by the drafting team, working with NPCC Standards Staff and Compliance Staff, at the same time as the associated Reliability Standard, but are not part of the Reliability Standard. The Board of Directors is responsible for approving VRFs and VSLs.

- Violation Risk Factors
  VRFs identify the potential reliability significance of noncompliance with each requirement. Each requirement is assigned a VRF in accordance with the latest approved set of VRF criteria.
- Violation Severity Levels
  VSLs define the degree to which compliance with a requirement was not achieved. Each requirement shall have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs. Each requirement is assigned one or more VSLs in accordance with the latest approved set of VSL criteria.

Version History: The version history is provided for informational purposes and lists information regarding prior versions of the regional standard.

Variance: As applied to a NPCC regional standard is a Requirement (to be applied in the place of the NPCC region-wide Requirement) that is applicable to a specific geographic area or to a specific set of Registered Entities.

Compliance Enforcement Authority (CEA): The entity that is responsible for assessing performance or outcomes to determine if an entity is compliant with the associated regional standard. The Compliance Enforcement Authority will be NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the ERO regional standards.

Reliability Standard Audit Worksheets (RSAWs)[11] Reliability Standard Audit Worksheets (RSAWs) are developed as companion documents to regional and continent-wide Reliability Standards to facilitate the CEA assessment of a registered entity's compliance with a standard.

[11] While RSAWs are not part of the regional standard, they are developed through collaboration of the drafting team and NPCC Compliance Staff.

Informational Elements: Elements to aid in the implementation of the regional standard.

Application Guidelines: Guidelines or reference documents to support the implementation of the associated regional standard.

Procedures: Procedures to support implementation of the associated regional standard.

IV. REGIONAL STANDARDS DEVELOPMENT PROCESS

1. ROLES IN THE NPCC REGIONAL STANDARD PROCESS

NOMINATION, REVISION, CLARIFICATION, OR RETIREMENT OF A STANDARD:

Any member of NPCC or group within the NPCC region shall be allowed to request that a NPCC regional standard be developed, modified, clarified, or retired. Additionally, any person (organization, company, government agency, individual, etc.) who is directly and materially affected by the reliability of the NPCC Bulk Electric System shall be allowed to request that a NPCC regional standard be developed, modified, clarified, or retired. The following section identifies the process roles in the NPCC regional standards process. Refer to Step 2 STANDARD DEVELOPMENT PROCESS STEPS and FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS OVERVIEW for the regional standards development process steps and associated flowchart. Refer to Step 3 STANDARD CLARIFICATION PROCESS STEPS and FIGURE 2: FLOWCHART OF REGIONAL STANDARDS CLARIFICATION PROCESS OVERVIEW for the regional standards clarification process steps and associated flowchart.

PROCESS ROLES AND RESPONSIBILITIES

BOARD OF DIRECTORS

The NPCC Board of Directors (Board) shall consider for adoption regional standards, definitions, variances and clarifications and associated implementation plans that have been processed according to the processes identified in this manual.

DRAFTING TEAM

The drafting team (DT) should strive to achieve a portfolio of performance, risk, and capability-based mandatory reliability requirements that support an effective defense-in-depth strategy. The drafting team develops standards-related regional products as directed by the NPCC RSC and within the scope of an approved Regional Standard Authorization Request (RSAR) or a Clarification Request (CR). The product that is developed is typically a new or revised regional standard, but could also be a definition, a reference document, a set of Violation Risk Factors, a set of Violation Severity levels, or the team could be appointed to assist an author in refining a Regional Standard Authorization Request (RSAR). The drafting team also works collaboratively with NPCC Compliance Staff to develop Reliability Standard Audit Worksheets (RSAWs) at the same time regional standards are developed. The drafting team shall remain in place until such time as the NERC Board of Trustees adopts the regional standard.

MANAGER OF RELIABILITY STANDARDS

The NPCC Manager of Reliability Standards has the overall responsibility for managing the NPCC regional standards processes in accordance with this manual. As used herein, the NPCC Manager of Reliability Standards will be the NPCC Manager of Reliability Standards or his/her designee.

NPCC MEMBERS

NPCC members may participate in the comment and ballot periods associated with the development and industry approval of regional standards. The ballot body is comprised of all

entities or individuals that qualify for one of the stakeholder sectors within NPCC as stated in the most recently approved NPCC Bylaws. All General and Full Members of NPCC can participate in the balloting of regional standards. Any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards.

NON-NPCC MEMBERS

Any entity or person that is neither a General nor Full Member of NPCC is not eligible to participate in the ballot body voting on a regional standard. However, any entity or person, including non-NPCC members, may submit comments during the open process comment periods for standards. Subject Matter Experts (SMEs), regardless of NPCC membership status, are encouraged to participate in comment periods for regional standards.

NPCC STANDARDS STAFF

The Standards Staff is responsible for assisting the NPCC Manager of Reliability Standards and the RSC in administering the NPCC regional standards processes in accordance with this manual.

NPCC COMMITTEES, TASK FORCES AND WORKING GROUPS

The Committees, Task Forces and Working Groups within NPCC serve an active role in the standards process. Activities performed by these groups include, but are not limited to, the following:

- Identify the need for new or modified regional standards
- Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs)
- Develop comments (views and objections) to standards actions
- Participate in NPCC Standard drafting
- Dispensation of Clarification Requests (CRs)
- Provide technical oversight in response to changing industry conditions and ERO Requirements
- Conduct Field Tests, as required

REGIONAL STANDARDS COMMITTEE (RSC)

The NPCC Regional Standards Committee (RSC), a committee of the NPCC Board of Directors, is charged with oversight of all drafting team activities and managing the NPCC regional standards development process in accordance with this manual.

~~8. A cross references to existing NPCC or NERC documents~~

~~The RSPM shall forward all properly completed RSARs to the RSC.~~The RSC is responsible for maintenance of the Regional Standard Processes Manual (RSPM), including the endorsement of RSPM revisions for NPCC Board review and approval.

RELIABILITY COORDINATING COMMITTEE (RCC)

The Reliability Coordinating Committee (RCC) supports the standards development process through the assignment of NPCC Task Forces to serve as technical resources for: (1) staffing drafting teams, and (2) performing a technical advisory role in the regional standards process through comments, recommendations and technical justifications.

REQUESTER

Any individual representing an organization (entity, company, government agency, etc.) that is directly and materially affected by the reliability of the Bulk Electric System within the NPCC

geographical area may request a regional standard be developed or an existing regional standard be modified, clarified, or deleted.

QUALITY REVIEW TEAM

The NPCC Standards Staff shall coordinate a quality review of the "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, whether the regional standard is clear and enforceable as written and the VRFs and VSLs are developed according to NERC and FERC guidelines. The Quality Review Team may be comprised of legal and compliance representatives, a technical writer, and NPCC Standards Staff. It will not involve individuals who participated on the drafting team of the standard undergoing the Quality Review.

2. STANDARD DEVELOPMENT PROCESS STEPS

STEP 2.1: REGIONAL STANDARDS AUTHORIZATION REQUEST TO DEVELOP, MODIFY OR RETIRE

A Regional Standard Authorization Request[12] (RSAR) is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified regional standards or the benefit of retiring one or more approved regional standards.

A RSAR shall be used to seek approval and initiate the development, modification or retirement of a NPCC regional standard. A RSAR is not used to seek a Clarification Request (CR) of a NPCC regional standard. The initiation and handling of a CR is covered in Step 3 STANDARD CLARIFICATION PROCESS STEPS, of this manual.

Any individual representing an organization which is directly or materially impacted by the operation of the Bulk Electric System within the geographical footprint of NPCC may request, via a submittal of a RSAR to the NPCC Manager of Reliability Standards, the development, modification, or deletion of a NPCC regional standard. The individual completing the form is referred to herein as the Requester.

STEP 2.1.A. REQUESTER ACTIONS

> *Note: The NPCC Manager of Reliability Standards will assist the Requester, as necessary, to ensure all required information is submitted on the RSAR.*

The Requester shall complete a RSAR form in accordance with the guidance provided in APPENDIX A: RSAR COMPLETION GUIDELINES.

The Requester shall submit the completed RSAR to the NPCC Manager of Reliability Standards, via npccstandard@npcc.org, for processing.

STEP 2.1.B. NPCC MANAGER OF RELIABILITY STANDARDS ACTIONS

The NPCC Manager of Reliability Standards shall review the submitted RSAR and verify that the submitted form has been adequately completed. Within fifteen (15) calendar days[13] of receipt of the submitted RSAR, the NPCC Manager of Reliability Standards will electronically acknowledge

[12] The RSAR is located on the NPCC website under Standards – Regional Standards General

[13] Time periods specified in this manual may be extended as deemed appropriate by NPCC Staff. When business days are specified, this provision could be used to take into account differing Canadian and US holiday schedules. When calendar days are specified, this provision could be used to take into account due dates that fall on a weekend.

receipt of the RSAR. If, at that time, the NPCC Manager of Reliability Standards finds the RSAR to be deficient, the Requester will be contacted to determine how to proceed.

Within ten (10) calendar days of the receipt of an adequately completed RSAR, the NPCC Manager of Reliability Standards shall forward the properly completed RSAR to the NPCC Regional Standards Committee (RSC) for its review and processing. Included in the transmittal of the RSAR to the RSC, the NPCC Manager of Reliability Standards shall include a statement indicating the applicability of the NPCC Cost Effectiveness Analysis Procedure (CEAP) for the proposed change.

STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS

Note: The RSC shall meet ~~at established intervals~~ to review all pending RSARs. ~~-~~ The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for RSC action more than 60 calendar days from the date of receipt by the RSC.

~~for RSC action more than 60 calendar days from the date of receipt. The RSC may~~

The RSC shall review the RSAR and take one of the following actions:

- ~~•~~ Remand the RSAR back to the ~~RSPM~~NPCC Manager of Reliability Standards for additional work.~~–~~

  In this case, the ~~RSPM may request~~ NPCC Manager of Reliability Standards shall work with the Requester to provide additional information or clarification for the RSAR ~~from~~as specified by the ~~Requester~~RSC.

  ~~• Accept the RSAR as a candidate for a new or revised standard. In this case, the RSC will forward the RSAR to the RCC to assign a NPCC Task Force to provide technical support and analysis of comments for that RSAR, and assist the Requester and the RSPM in the remaining steps of the process. The RSPM shall post notification of intent to develop a standard on both NPCC and ERO websites within 30 calendar days of acceptance.~~

- ~~•~~ Reject the RSAR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the Requester within ~~30~~ten (10) calendar days of the rejection decision.

~~STEPS 3, 4, AND 5: RSC ACCEPTS RSAR AND RCC ASSIGNS TF TO DRAFT NEW OR REVISED STANDARD~~

Note: Before the RSC can accept a RSAR for a new or modified standard the applicable CEAP process steps shall be completed.

- Accept the RSAR.
  - If a new or modified standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to develop or modify a regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR.
  - If the retirement of an existing regional standard has been authorized, within ten (10) calendar days of the authorization the NPCC Manager of Reliability Standards shall: 1) post notification on the NPCC website of the intent to retire an existing regional standard; 2) notify the ERO for processing in accordance with its process, as applicable; and 3) notify the Requester of the acceptance of the RSAR. The process to retire an existing regional standard is included in Step 6 RETIREMENT OF AN APPROVED NPCC REGIONAL STANDARD.

STEP 2.2: FORMATION OF DRAFTING TEAM FOR NEW OR MODIFIED STANDARD

A RSAR that ~~is~~has been accepted by the RSC ~~will~~shall, within ten (10) calendar days of the acceptance of the RSAR, be submitted ~~to the~~ by the NPCC Manager of Reliability Standards to the NPCC Reliability Coordinating Committee (RCC). The RCC~~. Within~~ shall, within sixty (60) calendar days ~~the RCC shall~~, assign the development of the regional standard to a NPCC Task Force ~~Drafting Team. The RSPM~~, and notify the NPCC Manager of Reliability Standards of its decision within ten (10) calendar days.

After receipt of the notification of drafting team assignment, the NPCC Manager of Reliability Standards shall ~~solicit~~ oversee solicitation and ~~recommend~~ recommendation of a list of additional qualified [14] candidates over and above the appropriate NPCC Task Force members, for appointment to the ~~team and~~ drafting team. The Requester and a NPCC Compliance Staff person will be included on the drafting team. Within sixty (60) calendar days of the drafting team assignment notification from the RCC, the NPCC Manager of Reliability Standards shall submit the list ~~to the RSC. This list shall include the Requester. The RSC may select other individuals~~of the entire drafting team membership to ~~serve, with the Task Force to draft the Standard. This team shall consist of a small group of people who collectively have the~~the RSC for acceptance. The RSC may accept the recommendations of the NPCC Manager of Reliability Standards as presented or revise the recommendations as necessary ~~technical expertise and work process skills~~.

Upon acceptance of the drafting team slate, the RSC shall provide a target date on which the drafting team is expected to have ready a completed draft regional standard and associated supporting documentation available for consideration by the NPCC membership. Additionally, the RSC shall provide the drafting team with any preliminary development products including, but not limited to, a draft standard, comments, and related white papers.

The RSC shall designate one of its members to actively monitor and assist NPCC staff in the oversight of drafting team milestones and deadlines, and extend or expedite milestones and deadlines, as appropriate, acting as a liaison between the drafting team and the RSC to help resolving any issues.

STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS

Prior to beginning work on the development of a new or revised regional standard and the associated supporting documentation, the drafting team should develop a work plan for completing the regional standard development work, including the establishment of milestones for completing critical elements of the work in sufficient detail to ensure that the drafting team will meet the target date established by the RSC, or the drafting team shall propose an alternative date. This work plan must be submitted to the RSC for its concurrence. When a drafting team begins its work, it shall regularly (at least quarterly) report progress against that aforementioned work plan to the NPCC Manager of Reliability Standards for presentation to the RSC.

> *Note: During the regional standards development, the drafting team will deliberate on whether the requirements in the regional standard are developed enough to begin the Cost Effectiveness Analysis (CEA) of the NPCC Cost Effectiveness Analysis Procedure (CEAP). When appropriate, the drafting team shall request that the RSC initiate the second phase (CEA) of the CEAP process.*

The drafting team shall create and manage its work structure (e.g., sub-teams) and meeting schedule (face-to-face as well as electronic meetings), as necessary, to meet the milestone dates and project deliverables outlined in the work plan.

The work products of the drafting team should consist of the following

- A draft regional standard consistent with the RSAR on which it was based
- An implementation plan, including the nature, extent and duration of field-testing, if any
- Identification of any existing regional standard and NPCC criteria that will be deleted, in part or whole, or otherwise impacted by the implementation of the draft regional standard

[14] Refer to Appendix B: Selection of Drafting Team Members

- Technical reports, white papers and/or work papers that provide technical justification for the draft regional standard under consideration
- Reliability Standard Audit Worksheet (RSAW) collaboratively developed by the drafting team and NPCC Compliance Staff

Any proposed changes to definitions in existing regional standards should be sent to the appropriate Task Force (TF) for consideration of the impact to the standard. If necessary, the TF can produce a RSAR.

~~The RSPM shall assign NPCC staff personnel to~~NPCC Standards Staff can assist in the drafting of the regional standard including compliance ~~measure~~measures, process and elements. ~~-~~ The drafting of measures and compliance administration aspects of the standard will be coordinated with the NPCC Compliance ~~Program~~Staff.

The drafting team shall submit the initial and subsequent interim drafts of the regional standard and associated documents to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post documents for comment.

STEP ~~6: SOLICIT PUBLIC~~ 2.4: POSTING FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS ~~ON DRAFT STANDARD~~

~~Once a draft standard has been verified by the RSC to be within the scope and purpose of the RSAR, the RSPM will post the draft standard for the purpose of soliciting public comments. The posting of the draft standard will be linked to the RSAR for reference. In addition to the standard, an implementation plan shall be posted to provide additional details to the public and aid in their commenting and decision process. Comments on the draft standard will be accepted for a 45 calendar day period from the public notice of posting. Comments will be accepted on-line using the NPCC Open Process web-based application.~~

~~Final draft standards will be concurrently posted on the ERO website for comments.~~

STEPS 7, 8, AND 9: OPEN PROCESS POSTING AND ANALYSIS OF THE COMMENTS

The RSPM will assemble the comments on the new draft standard and distribute those comments to the Task Force acting as the standard drafting team. The Task Force shall give prompt consideration to the written views and comments of all participants. An effort to address all expressed comments shall be made, and each commenter shall be advised of the disposition of the comment and the reasons therefore, in addition to public posting of the responses.

The Task Force acting as the Standard Drafting Team shall take one of the following actions:

- Submit the draft standard for RCC endorsement as it stands, along with the comments received and responses to the comments. Based on the comments received, the Task Force acting as the standard drafting team may include revisions that are not substantive. A substantive change is one that directly and materially affects the application of the standard, including, for example: changing "shall" to "should," changing "should" to "shall"; adding, deleting, or revising requirements; or adding, deleting, or revising measures for which compliance is mandatory.
- Make substantive revisions to the draft standard and reposts it for further open review and comment.
- Task Force recommends Field Test if necessary to RSC.

Requester also may withdraw the request for a standard.

RCC submits proposed RRS to the RSC along with its recommendation based on comments, Task Force statements and any field test results.

STEPS 10 AND 11: RSC APPROVES OF THE NEW OR REVISED STANDARD FOR POSTING

If the RSC, acting with consideration of any recommendations by the RCC and utilizing the composite sector voting structure, as outlined in the NPCC, votes to post the draft standard for approval, the draft standard, all comments received, and the responses to those comments shall be posted electronically for the NPCC Members, by the RSPM and made public through the NPCC Website (www.npcc.org) for a 30 calendar day "pre-ballot review" and request for balloting. If the RSC decides more work is needed, the draft standard will be remanded back to the drafting Task Force. All actions of the RCC, Task Forces acting as drafting teams and the Regional Standards Committee will be recorded in regular minutes of the group(s) and posted on the NPCC website. Once the notice for a ballot has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued

STEPS 12, 13 AND 14: BALLOT OF STANDARD

Upon notification of a ballot, the Members of NPCC's registered ballot body will cast their vote consistent with the NPCC Bylaws. This ballot shall commence no sooner than 15 calendar days and no later than 30 calendar days following the notification of ballot. All members of the NPCC are eligible to participate in the voting on proposed, standard revisions or deletions of regional standards. The ballot period will typically begin immediately following the 30 calendar day pre-ballot posting and will last at least 10 business days.

The NPCC registered ballot body comprises all entities or individuals that qualify for one of the eight NPCC stakeholder sectors and are registered with NPCC as potential

~~ballot participants in the voting on standards. Each member of the NPCC registered ballot body is eligible to vote on standards.~~

~~In order for a NPCC Regional Standard to be approved;~~

- ~~A quorum must be established by at least 50% of the NPCC Members of at least 60% of the Voting Sectors on the roster of Members maintained by NPCC.~~
- ~~A two-thirds majority of the total weighted sector votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions, and non-responses. Weighted sector vote will be calculated as follows;~~
  - ~~Affirmative votes cast in each sector will be divided by the sum of affirmative and negative votes cast, in that same sector, to determine the fractional affirmative vote for each sector. Abstentions and non-responses will not be counted for the purposes of determining the fractional affirmative vote for a sector.~~
  - ~~The sum of the fractional affirmative votes from all sectors divided by the number of sectors voting will be used to determine if a two-thirds majority has been achieved. (A sector will be considered as "voting" if any member of the sector in the ballot pool casts either an affirmative or a negative vote.)~~
  - ~~A standard will be approved if the sum of fractional affirmative votes from all sectors divided by the number of voting sectors is at least 2/3.~~

~~Ballots will be cast electronically and alternatives are as follows;~~

- ~~Affirmative~~
- ~~Affirmative with Comments~~
- ~~Negative~~
- ~~Negative with Comments~~
- ~~Abstain~~

~~The RSPM shall post the final outcome of the ballot process. If the standard is rejected, it may be withdrawn by either the RCC or the original Requester, or the standard may be remanded by the RSC back to the Task Force acting as the drafting team to address the issues. All comments submitted during the process will be posted and archived for consideration when redrafting the standard upon review.~~

~~The standard, once approved by ballot, and a recommendation will be forwarded to the NPCC Board for final Regional approval. The Board may not make substantive modifications to the standard. If the Board does not approve the standard for transmittal to NERC it will be remanded back to the RSC.~~

~~If the standard is approved, the standard will be submitted to the NERC/ERO Board of Trustees for approval.~~

STEPS 15, 16 AND 17: IMPLEMENTATION OF THE NPCC REGIONAL STANDARD

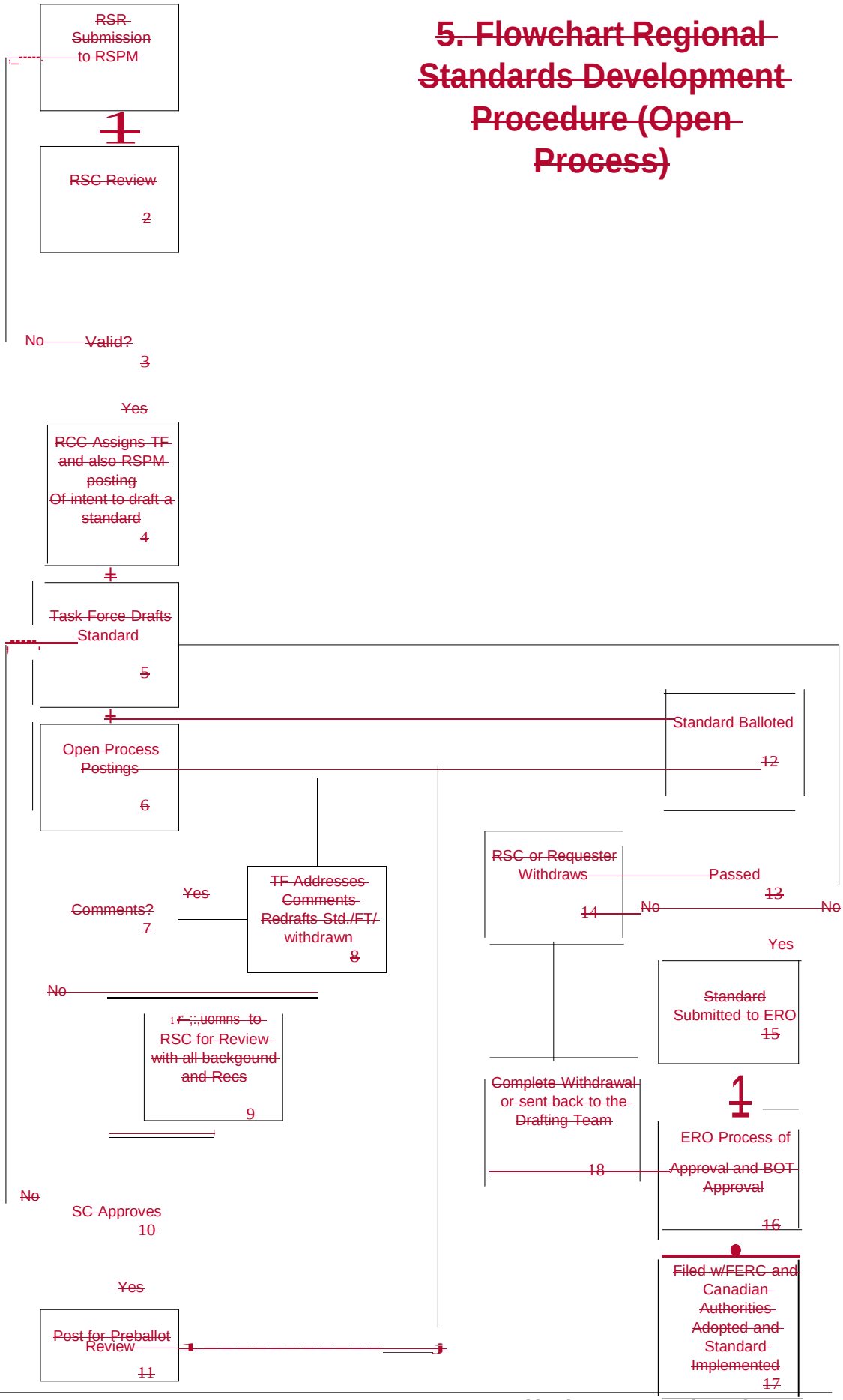
Upon approval within the NPCC , the standard will be submitted to the NERC/ERO for approval(s) and filing with FERC and applicable Canadian Governmental and/or Regulatory Authorities for adoption.

Once a reliability standard is adopted and made effective, all users, owners, planners, and operators of the Bulk Power System in the NPCC geographic area of the Northeast are required to comply with the standard. The NERC/ERO Board of Trustees has established a separate compliance program, also administered in the Northeast by NPCC , to measure compliance with the standards and administer sanctions as appropriate. After adoption of a NPCC Regional Standard, the standard will be forwarded to the compliance program for compliance monitoring and enforcement.

STEP 18: WITHDRAWAL OF STANDARD

Upon rejection of a proposed standard, the RCC or the requester may withdraw the standard completely or remand it back to the Task Force acting as the standard drafting team for further work.

5. Flowchart Regional Standards Development Procedure (Open Process)



6. ERO and Regulatory Process and Approvals

- **NERC/ERO Comment Period** – NERC/ERO shall publicly notice and request comment on the NPCC Regional Reliability Standard, allowing a minimum of 45 calendar days for comment on NERC's website and actively notify all adjoining Regions. Concurrent with this regional posting, final drafts will be forwarded to NERC for posting on the NERC website to ensure full industry awareness of the standard and expedite and coordinate all commenting. All comments will be responded to electronically through a posted response on the NPCC website or a link on the NERC website. NPCC shall have an opportunity to resolve any objections identified in the comments and may choose to withdraw the request, revise the NPCC Regional Reliability Standard and request another posting for comment, or submit the NPCC Regional Reliability Standard along with a response to any objections received, for approval by NERC.

- **NERC/ERO Approval of NPCC Regional Reliability Standards** – Proposed regional reliability standards shall be subject to approval by the NERC/ERO who shall have a process to evaluate and recommend whether a proposed non-Interconnection-wide NPCC Regional Reliability Standard has been developed in accordance with all applicable procedural requirements and whether NPCC has considered and addressed stakeholder objections. NPCC Board, having been notified of the results of the regional ballot concerning a NPCC Regional Reliability Standard, shall vote to submit the Standard to the NERC/ERO Board for approval as a NERC Reliability Standard. The NERC/ERO Board shall consider NPCC's request, the scope and implications of the Standard, the recommendation for action on the Standard, any unresolved stakeholder comments, and NPCC's consideration of comments and unresolved issues if any, in determining whether to approve the NPCC Regional Reliability Standard as a NERC Reliability Standard.

- **Regulatory Authority Approval** – An NPCC Regional Reliability Standard that has been approved by the NERC/ERO board shall be filed with FERC and applicable Canadian Governmental and/or Regulatory Authorities for approval and shall become effective and enforceable within the U.S., per Section 215 of the Federal Power Act, only when adopted by FERC, and within Canada, only when adopted by applicable Canadian Governmental and/or Regulatory Authorities. The regional reliability standard, once adopted will be made part of the body of NERC reliability standards and shall be mandatory and enforceable on all applicable bulk power system owners, operators, and users within the NPCC Region, regardless of membership status.

7. Appeals

-

Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.

STEP 2.4.A. COMMENT PERIOD

Note: For Final Comment Period skip this step and proceed to STEP 2.4.B. FINAL COMMENT PERIOD.

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the draft of the regional standard on the NPCC website, along with a draft implementation plan and available supporting documents, for a forty-five (45) calendar day comment period. The NPCC Manager of Reliability Standards shall also notify NERC to process the draft document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the draft regional standard and associated documents and provide all comments to the drafting team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the drafting team shall convene and consider changes to the draft Standard, the implementation plan and/or supporting technical documents based upon comments received. All submitted comments shall be addressed, and each commenter shall be advised of the disposition, with reasons, of their comments. The NPCC Manager of Reliability Standards shall publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

Based on the comments received, the drafting team may elect to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the draft regional standard, the implementation plan and/or supporting technical documents.
- Recommend that the RSC authorize Field Testing of the draft regional standard. Upon completion of the Field Test, return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD

AND ASSOCIATED DOCUMENTS to revise the draft regional standard based on insights learned during the Field Test.

- Obtain RSC concurrence to post documents for Final Comment Period and request that the RSC initiate the second phase (CEA) of the CEAP process

STEP 2.4.B. FINAL COMMENT PERIOD

The NPCC Standards Staff shall coordinate a Quality Review of "final draft" of the regional standard, implementation plan, VRFs and VSLs to assess whether the documents are within the scope of the associated RSAR, whether the regional standard is clear and enforceable as written and the VRFs and VSLs are developed according to NERC and FERC guidelines. Upon Completion of the Quality Review, including resolution of comments, the drafting team shall submit the regional standard to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post these documents for comment.

As authorized by the RSC, the NPCC Standards Staff shall post the "final draft" of the regional standard on the NPCC website, along with the implementation plan, supporting documents and the Cost Effectiveness Analysis (CEA) survey[15] for a forty-five (45) calendar day comment period. NPCC Standards Staff shall also notify NERC to process the proposed final document in accordance with NERC's regional standards review procedure, as applicable.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard and associated documents and provide all comments to the drafting team for consideration.

In addition, the RSC, pursuant with the requirements of the Cost Effectiveness Analysis Procedure (CEAP), will use the responses to the posted CEA survey to develop a recommendation based on the cost effectiveness of the proposed regional standard.

The NPCC Task Forces (TFs) or Working Groups (WGs) may develop recommendations for submittal to the RSC. Following the RSC deliberations to determine a course of action, the RSC will communicate to the drafting team to:

- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the Standard to address the results of the CEAP
- Accept the Standard "as is" to move forward through the remainder of the process
- Hold the Standard in abeyance until such time as additional guidance can be provided regarding whether or how to continue
- Decide not to pursue the development of certain requirements or the entire Standard due to cost effectiveness considerations

Upon Completion of the final comment period the drafting team shall submit the proposed regional standard, along with any supporting materials, consideration of comments and field test results, to the NPCC Manager of Reliability Standards to obtain RSC concurrence to post the regional standard for ballot and concurrently provide an information copy to the RCC.

[15] In accordance to the Cost Effectiveness Analysis Procedure (CEAP) the Cost Effectiveness Analysis (CEA) survey may be assigned directly to NPCC Task Forces (TFs) or Working Groups (WGs) in addition to the posting process.

The NPCC Manager of Reliability Standards shall also publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS

> *Note: There are no limits to the number of public comment periods and ballots that can be conducted to result in a regional standard that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval.*

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed regional standard on the NPCC website, along with supporting documentation [16] (e.g., implementation plan, consideration of comments, technical reports, white papers and any field test results), for a thirty (30) day pre-ballot review period and a subsequent ten (10) day ballot period. The ten (10) day ballot period will commence immediately following the pre-ballot review period. In the event that a quorum exists for purposes of an electronic vote but the ballot purpose has not been resolved, NPCC may continue to solicit additional responses in order to resolve the matter by electronic voting. In the event that quorum has not been achieved for purposes of an electronic vote, NPCC may continue to solicit electronic ballots, including abstentions, to obtain quorum and resolve the matter.

At the time the regional standard is posted for ballot, the NPCC Manager of Reliability Standards shall also notify NERC to process the proposed regional standard in accordance with NERC's regional standards review procedure, as applicable.

During the ballot period, the NPCC Members of the ballot body can cast their vote as follows:

- Affirmative, with or without comments
- Negative with comments
- Abstain

In accordance with the NPCC Bylaws, a quorum and receipt of a two-thirds (2/3) affirmative majority of the weighted sector votes is required for a ballot to pass.

The NPCC Manager of Reliability Standards shall post the final outcome of the ballot process on the NPCC website.

STEP 2.5.A. BALLOT DOES NOT RECEIVE 2/3 AFFIRMATIVE VOTE

If a ballot fails to achieve the 2/3 majority vote the NPCC Manager of Reliability Standards may:

- Direct the drafting team to respond to ballot comments and return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard. The consideration of comments from prior ballot will be included with the re-posting.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.
- Pursue the discontinuance of the regional standard development by soliciting the Requester to withdraw the RSAR or by soliciting the RSC to reject the RSAR pursuant with STEP 2.1.C. NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS. The NPCC Manager of

[16] The ballot posting is for the regional standard, definition, variance or clarification. Supporting documentation is included for information only and is not balloted.

Reliability Standards, in the event of a discontinuance of the development of a regional standard, shall post a notice of the discontinuance and will post and archive all comments submitted during the process for future consideration, if required. The NPCC Manager of Reliability Standards will also notify NERC to process the proposed regional standard in accordance with NERC's regional standards review procedure, as applicable.

STEP 2.5.B. BALLOT RECEIVES ≥ TWO-THIRDS (2/3) AFFIRMATIVE VOTE

A ballot that achieved two-thirds or greater affirmative vote has successfully passed. However, negative votes with comments should still be reconciled. If there is at least one negative vote with comments proceed to STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT". If there was not any negative vote with comments proceed to STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT".

STEP 2.5.B.1 APPROVED BALLOT WITH "NEGATIVE VOTE WITH COMMENT"

Following the conclusion of the NPCC ballot period, the NPCC Manager of Reliability Standards will assemble the comments on the posted regional standard and provide all comments to the drafting team for consideration. The drafting team shall review all negative votes with comments and elect to:

- Recommend to the RSC to accept the regional standard "as is" and seek RSC endorsement to move forward through the remainder of the process. Upon receiving RSC endorsement to proceed, the regional standard and associated documents, approved by the NPCC ballot body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval. If comments that were received during balloting should be considered in future revisions to the regional standard then the NPCC Manager of Reliability Standards should log comments in an issues database.
- Return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.
- Respond to ballot comments and recommend to the RSC endorse the return to STEP 2.5: POSTING FOR BALLOT PERIOD IN THE OPEN PROCESS to re-ballot the regional standard. The NPCC Manager of Reliability Standards should include the consideration of comments from the prior ballot with the re-posting.

STEP 2.5.B.2 APPROVED BALLOT WITHOUT "NEGATIVE VOTE WITH COMMENT"

Regional standard and associated documents, approved by the NPCC ballot body, shall be forwarded by the Assistant Vice President Standards to the NPCC Board of Directors for final Regional approval.

STEP 2.6: NPCC BOARD OF DIRECTORS APPROVAL

Following approval by the NPCC Members, regional standards require review and approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the regional standard as presented.
- Approve the regional standard with comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive revisions to the standard.]
- Remand the regional standard back to the RSC and the drafting team to address their concerns. The RSC / drafting team can address the BOD comments and re-submit for BOD

approval or return to STEP 2.3: DEVELOPMENT OF A REGIONAL STANDARD AND ASSOCIATED DOCUMENTS to revise the regional standard to address the comments received.

STEP 2.7: NERC BOARD OF TRUSTEES SUBMITTAL

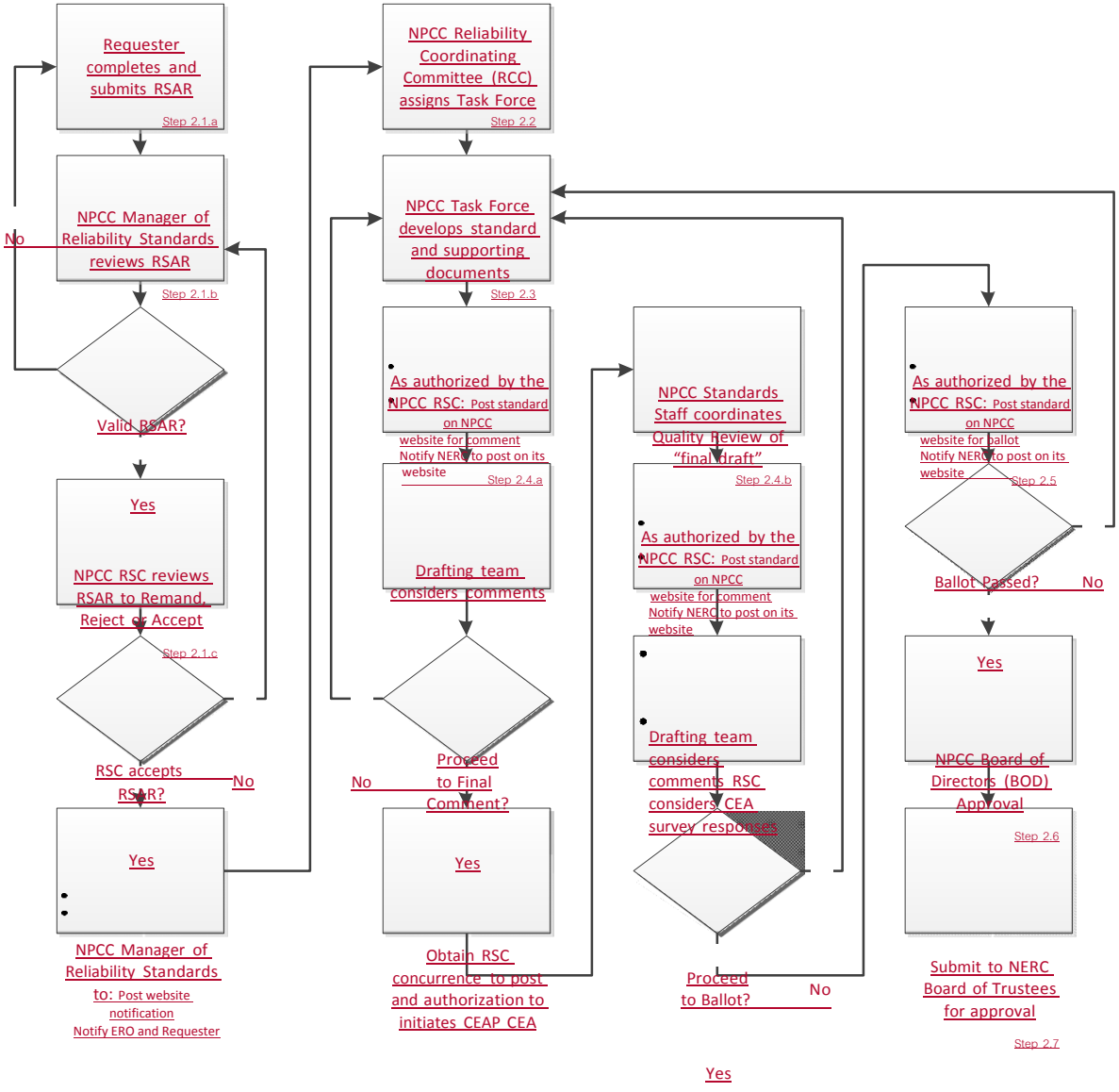
Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the regional standard to NERC, as the Electric Reliability Organization, for approval and subsequent filing with FERC and the applicable Canadian Provincial regulatory and/or governmental authorities for adoption.

STEP 2.8: IMPLEMENTATION OF A NPCC REGIONAL STANDARD

Following the approval of a NPCC regional standard by FERC and the applicable Canadian Provincial regulatory and/or governmental authorities, all users, owners, and operators of the Bulk Electric System in the NPCC geographic area are required to comply with the standard as of its enforcement date.

ERO approved Reliability Standards (both continent-wide and regional) are included in both the NERC and NPCC Compliance Monitoring and Enforcement Programs (CMEPs).

FIGURE 1: FLOWCHART OF REGIONAL STANDARDS DEVELOPMENT PROCESS OVERVIEW



3. STANDARD CLARIFICATION PROCESS STEPS

This section applies to NPCC regional standards that have been approved[17] and are currently enforceable or have a future enforcement date. A clarification request is not permitted for regional standards under development. For regional standards under development, an explanation of a requirement or its meaning can be sought during a comment period. Refer to Step 2, STANDARD DEVELOPMENT PROCESS STEPS of this manual for details on the comment process for a standard under development.

STEP 3.1: REGIONAL STANDARDS CLARIFICATION REQUEST (CR)

Any member of NPCC or group within the NPCC region shall be allowed to submit a Clarification Request (CR) for a NPCC regional standard.

Additionally, any person (organization, company, government agency, individual, etc.) who is directly and materially affected by the reliability of the NPCC Bulk Electric System shall be allowed to submit a Clarification Request (CR) for a NPCC regional standard.

> *Note: A valid Clarification Request is one that seeks additional clarity about one or more requirements in an approved regional standard, but does not request approval as to how to comply with any requirements of the standard.*

The Requester should submit a Clarification Request[18] (CR) for a NPCC regional standard directly to the NPCC Manager of Reliability Standards, via npccstandard@npcc.org, for processing. Alternatively, the Requester can submit a Request for Interpretation (RFI) of a NPCC regional standard under the NERC process for developing an interpretation[19] to the NERC Reliability Standards Staff explaining the clarification required, the specific circumstances surrounding the request, and the impact of not having the clarification provided. A copy of the completed RFI form should also be sent to the NPCC Manager of Reliability Standards.

NERC Reliability Standards Staff will refer the RFI to NPCC and delegate its resolution to NPCC. NPCC will process the NERC delegation pursuant with the NPCC Clarification Request (CR) process described herein.

STEP 3.2: REVIEW AND VALIDATION OF CLARIFICATION REQUEST (CR)

Upon receipt of a Clarification Request (CR) for a NPCC regional standard, the NPCC Manager of Reliability Standards shall review the CR to determine whether:

- It meets the requirements for a valid Clarification Request
- A compliance process or approach could be used in lieu of a clarification

The NPCC Manager of Reliability Standards will utilize, as necessary, the NPCC Standards Staff, NPCC Compliance and Legal Staffs when determining the validity of the CR. Based on this review, the NPCC Manager of Reliability Standards will recommend to the RSC whether to accept or reject the CR. The recommendation to the RSC should be made within thirty (30) calendar days of the receipt of the CR.

[17] Approval is granted by FERC and the Canadian Provincial regulatory and/or governmental authorities, as applicable.
[18] The NPCC Clarification Request form is included as Appendix D
[19] The *Request for Interpretation* form is posted under Resource Documents on the NERC Standards webpage.

The following examples identify situations that may warrant a recommendation from the NPCC Manager of Reliability Standards to reject the CR:

- Requests approval of a particular compliance approach
- Identifies a gap or perceived weakness in the approved regional standard (Requester should be redirected to initiate a RSAR rather than a CR)
- Where an issue can be addressed by an active (regional or continent-wide) standard drafting team
- Where an issue can be better addressed by a compliance process or approach
- Where it requests clarification of any element of a regional standard other than a requirement
- Where a question has already been addressed in the record
- Where the clarification identifies an issue and proposes the development of a new or modified regional or continent-wide standard (such issues should be addressed via submission of a RSAR or SAR)
- Where a clarification seeks to expand the scope of a regional standard
- Where the requirement of the regional standard is clear

STEP 3.3: NPCC REGIONAL STANDARDS COMMITTEE (RSC) ACTIONS

The RSC shall review the CR along with the recommendation from the NPCC Manager of Reliability Standards and take one of the following actions:

- Reject the CR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then provide a written explanation for rejection to the CR to the entity requesting the clarification within ten (10) calendar days of the decision to reject.
- Accept the CR. In this case, the RSC will provide its determination to the NPCC Manager of Reliability Standards, who will then: 1) post notification on the NPCC website of the intent to develop a clarification; 2) notify the NPCC Reliability Coordinating Committee (RCC) of the need to assign the resolution of the CR to one or more Task Forces (if more than one Task Force is assigned, one of them shall be assigned the lead role); and 3) notify the Requester of the acceptance of the CR. The notifications shall be made within ten (10) calendar days of the acceptance of the CR.

STEP 3.4: FORMATION OF DRAFTING TEAM FOR RESPONSE TO CR

A CR that has been accepted by the RSC shall be assigned by the RCC to the responsible NPCC Task Force to make up the clarification drafting team (CDT) and develop the CR response.

STEP 3.5: DEVELOPMENT OF RESPONSE TO CR

> *Note: A valid clarification response provides additional clarity about one or more requirements, but does not expand on any requirement and does not explain how to comply with any requirement.*

Within sixty (60) calendar days from the receipt of being assigned to respond to a CR, the CDT shall submit a proposed clarification response to the NPCC Manager of Reliability Standards. Upon receipt of the proposed clarification response from the CDT, the NPCC Manager of

Reliability Standards shall present the response to the RSC to obtain concurrence to post the proposed response for comment.

Along with the proposed clarification response, the drafting team shall also develop and submit a set of questions to be included in the comment form, for approval by the RSC.

If the RSC concurrence is not received, the drafting team will continue to refine the clarification response.

> *Note: There are no limits to the number of public comment periods that can be conducted to result in a clear and concise clarification of a regional standard requirement.*

STEP 3.6: POSTING CR FOR COMMENT PERIOD AND RESOLUTION OF COMMENTS

As authorized by the RSC, the NPCC Manager of Reliability Standards shall post the proposed clarification response on the NPCC website for a forty-five (45) calendar day comment period.

Following the conclusion of the NPCC comment period, the NPCC Manager of Reliability Standards will assemble the comments on the proposed clarification response and provide all comments to the drafting team for consideration.

Within thirty (30) calendar days of the conclusion of the comment period the drafting team shall convene and consider changes to the proposed clarification response based upon comments received. All submitted comments shall be addressed, which may be in the form of a summary response addressing each of the issues raised in comments received. The NPCC Manager of Reliability Standards shall publicly post all of the drafting team's responses to stakeholder comments on the NPCC website.

Based on the comments received, the drafting team may elect to:

- Return to STEP 3.5: DEVELOPMENT OF RESPONSE TO CR to revise the proposed clarification response.
- Accept the proposed clarification response "as is" to move forward through the remainder of the process.

Upon acceptance of the proposed clarification response "as is," the drafting team shall submit the proposed clarification response to the NPCC Manager of Reliability Standards to obtain RSC endorsement to the submitted CR response.

STEP 3.7: REGIONAL STANDARDS COMMITTEE APPROVAL OF CR

Upon receipt of the CR response from the NPCC Manager of Reliability Standards, the RSC shall elect to:

- Endorse the proposed clarification response and direct the NPCC Assistant Vice President Standards to forward the CR to the NPCC Board of Directors for final Regional approval; or
- Direct the drafting team to return to STEP 3.5: DEVELOPMENT OF RESPONSE TO CR to revise the proposed clarification response

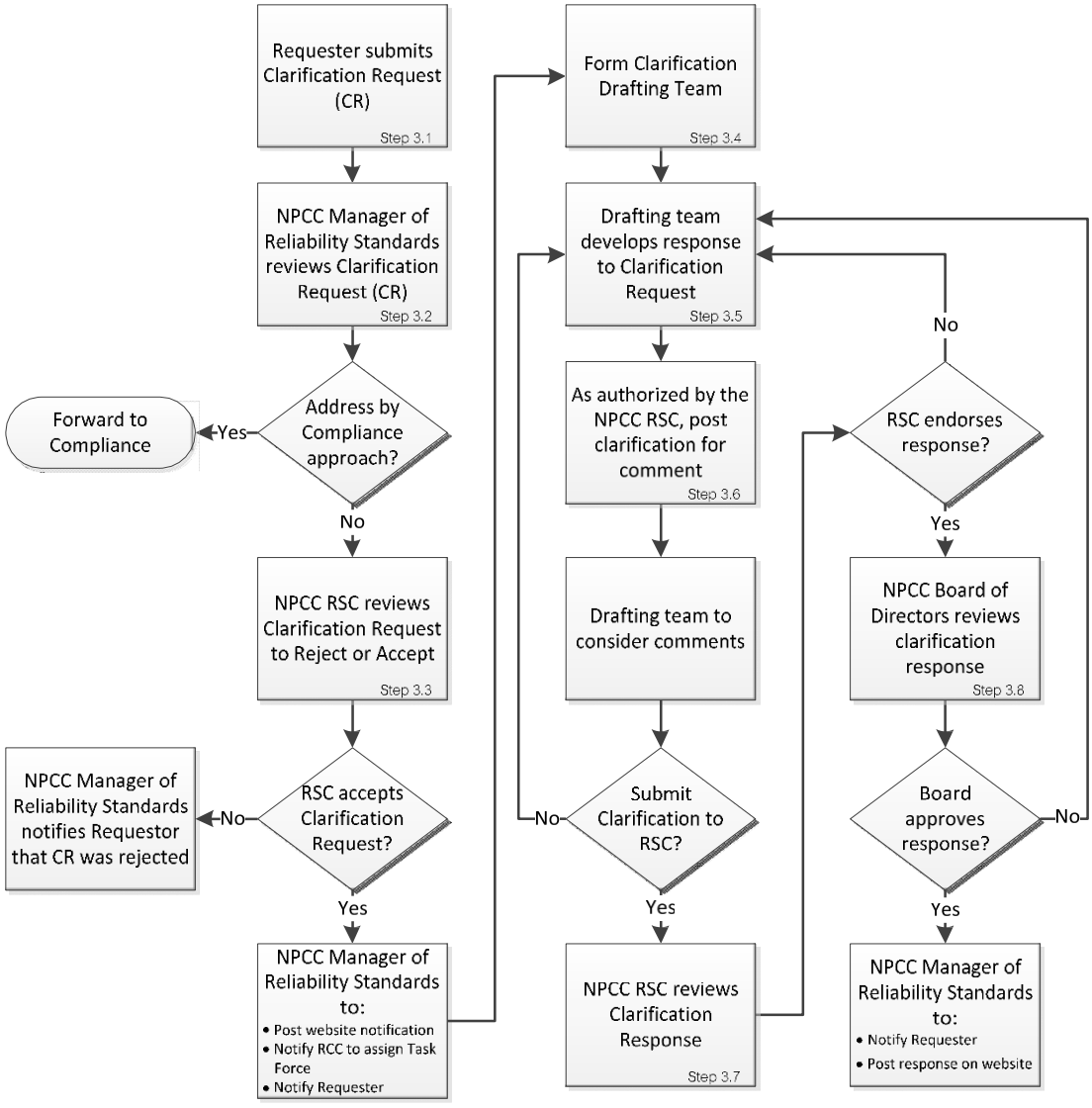
STEP 3.8: NPCC BOARD OF DIRECTORS APPROVAL OF CR

Following endorsement by the RSC, clarification responses require review and approval by the NPCC Board of Directors. The NPCC Board of Directors may take the following actions:

- Approve the clarification response as presented
- Approve the clarification response with comments to incorporate non-substantive revisions. [The NPCC Board of Directors may not make substantive revisions to the clarification response.]
- Remand the clarification response back to the RSC and the drafting team to address their concerns

Upon receipt of Board approval, the NPCC Manager of Reliability Standards shall notify the Requestor and post the approved clarification on the NPCC website.

FIGURE 2: FLOWCHART OF REGIONAL STANDARDS CLARIFICATION PROCESS OVERVIEW



4. DISCONTINUANCE OF REGIONAL STANDARD DEVELOPMENT

The term "discontinuance" as used herein refers to terminating the standard development process after RSAR approval but prior to posting a regional standard for industry ballot. From time to time the need or rationale for a regional standard may change thereby necessitating the curtailment

of the regional standard development. Upon notification or determination that a regional standard under development should be considered for discontinuance due to a perceived change in the need for the standard, the NPCC Manager of Reliability Standards will submit the recommendation for discontinuance to the RSC for approval.

5. Withdrawal of a Regional Standard Pending Approval

The term "withdrawal" as used herein, refers to the revocation of a request for approval of a regional standard, variance, clarification or definition that has been approved by the NPCC Board of Directors and has not been filed with Applicable Governmental Authorities or has been filed but not yet approved by Applicable Governmental Authorities. The RSC may withdraw a regional standard, variance, clarification or definition for good cause subject to approval by the NPCC Board of Directors. Upon approval by the NPCC Board of Directors, the NPCC Manager of Reliability Standards will notify NERC Staff to petition the Applicable Governmental Authorities, as necessary, to allow for withdrawal in the case that the regional standard has been filed.

6. Retirement of an Approved NPCC Regional Standard

The term "retirement" refers to the discontinuation of a regional standard in whole, certain requirements within a regional standard, a variance, clarification or definition that: 1) has been approved by Applicable Governmental Authorities and 2) is not being superseded by or merged into a new or revised regional standard, clarification or definition.

Upon identification of a need for retirement, a RSAR containing the proposal of the retirement will be handled in accordance with the Step 2.1: Regional Standards Authorization Request to Develop, Modify or Retire. The proposal shall include the rationale for the retirement and a statement regarding the impact of retirement on the reliability of the Bulk Electric System. Upon approval by the NPCC Members and the NPCC Board of Directors, the NPCC Manager of Reliability Standards shall submit the request for retirement to NERC, as the Electric Reliability Organization, for approval and to subsequently petition the Applicable Governmental Authorities to allow for retirement.

7. Approval of Process Waiver

While it is NPCC's intent to adhere to this manual under normal circumstances, NPCC may need to develop a new or modified regional standard, implementation plan, variance, clarification or definition under extenuating circumstances. Extenuating circumstances may include, but not be limited to, specific time constraint imposed by a regulatory body and urgent reliability issue that requires expedited handling outside of the normal regional Reliability Standards process.

The RSC, by two-thirds (2/3) majority vote, may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:

- Where necessary to meet regulatory deadlines
- Where necessary to address an urgent reliability issue identified by regulatory and/or governmental authorities, including response to national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber-attack on the Bulk Electric System
- Where necessary to meet deadlines imposed by the NPCC Board of Directors

- Where the RSC determines that a revision to a proposed regional standard, implementation plan, variance, clarification or definition has already been vetted by the industry through the standards development process or is so insubstantial that developing the revision through the processes contained in this manual will add significant time delay without any corresponding benefit.

In no circumstances shall this provision be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

A waiver request may be submitted to the RSC by any entity or individual, including NPCC committees or subgroups and NPCC Standards Staff. Prior to consideration of any waiver request, the NPCC Manager of Reliability Standards must provide notification to stakeholders at least five (5) business days prior to RSC consideration and action. Posting the waiver request on the NPCC website satisfies the notification provision.

Action on the waiver request will be included in the minutes of the RSC. Following the approval of the RSC to waive any provision of the regional Reliability Standards process, the Assistant Vice President Standards shall report the exercise of this waiver provision to the NPCC Board of Directors prior to adoption of the related Reliability Standard, clarification, definition or variance. Actions taken pursuant to an approved waiver request will be posted on the NPCC Standards webpage.

8. PROCESS FOR CORRECTING ERRATA

From time to time, an error may be discovered in a regional standard after it has received final ballot approval by the NPCC ballot body. Such errors may be corrected by the RSC without re-balloting if the RSC agrees that the correction of the error does not change the scope or intent of the associated regional standard, and agrees that the correction has no material impact on the end users of the regional standard.

If the regional standard containing errata is pending approval by the NPCC Board of Directors, the corrected regional standard shall be presented to the NPCC Board for approval in lieu of the regional standard approved by the NPCC ballot body.

If a regional standard containing errata had received prior approval by the NPCC Board of Directors, the corrected regional standard shall be presented to the NPCC Board for approval. Upon approval by the Board, the corrected regional standard will be filed for approval by NERC.

The NPCC Board of Directors has resolved to concurrently approve any errata approved by the RSC associated with a regional standard that has received prior approval by the NPCC Board.

9. APPEALS

Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the approval, revision, reaffirmation, or withdrawal of a regional standard (appellant) shall have the right to appeal. This appeals process applies only to the regional standards process as defined in this manual.

~~inaction related to the development, approval, revision, reaffirmation, or withdrawal of a regional reliability standard shall have the right to appeal.~~

~~This appeals process applies only to the standards process as defined in this procedure.~~

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within thirty (30) calendar days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. ~~-~~In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

- ~~Level~~ LEVEL 1 ~~Appeal~~ APPEAL

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the ~~RSPM~~NPCC Manager of Reliability Standards that describes the substantive or procedural action or inaction associated with a ~~reliability standard~~Reliability Standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary ~~staff~~NPCC Standards Staff and ~~committee~~Committee resources, the ~~RSPM~~NPCC Manager of Reliability Standards shall prepare a written response addressed to the appellant as soon as practical, but not more than forty-five (45) calendar days after receipt of the complaint. ~~-~~ If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response will be made a part of the public record associated with the standard and posted with the standard.

- ~~Level~~ LEVEL 2 ~~Appeal~~ APPEAL

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the ~~regional standards process manager~~NPCC Manager of Reliability Standards, the ~~RSPM~~NPCC Board of Directors shall ~~convene~~appoint a five member panel to serve as a Level 2 Appeals Panel~~. This panel shall consist of five members total appointed by the NPCC's board~~.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The ~~RSPM~~NPCC Manager of Reliability Standards shall post the complaint and other relevant materials and provide at least a thirty (30) calendar ~~days~~day notice of the meeting of the Level 2 Appeals Panel. ~~-~~

In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 ~~Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC~~

Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC with a statement of the issues and facts in regard to which unfair and/or inequitable action was taken, or which fair and/or equitable action was not taken. ~~-~~The panel may find for or against the appellant with a specific

statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise,

approve, disapprove, or adopt a ~~reliability standard.~~ Reliability Standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the NPCC Board of Directors for consideration at the time the ~~board~~Board decides whether to adopt a particular ~~reliability standard~~Reliability Standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than thirty (30) calendar days after the announcement of the vote on the standard in question.

APPENDIX A: RSAR COMPLETION GUIDELINES

The Requester shall complete a RSAR form in accordance with the guidance provided below.

The RSAR, at a minimum, shall contain information in the required fields in order to be qualified for consideration. The NPCC Manager of Reliability Standards will assist the Requester to ensure all required information is submitted on the RSAR.

Information in a Regional Standard Authorization Request ~~(RSAR)~~ (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC ~~Regional Standards Process Manager, NPCCstandard@npcc.org . The NPCC Regional Standards Process Manager shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.~~Manager of Reliability Standards, at npccstandard@npcc.org. The NPCC Manager of Reliability Standards shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard~~:~~: ***[Required Field]***
Request Date: ***[Required Field]***

RSAR Requester Information

Name: ***[Required Field]***	**RSAR Type ~~(~~(Check box for one of these selections.)**
Company: ***[Required Field]***	☐ New Standard
~~Telephone:~~ ***[Required Field]***	☐ Revision to Existing Standard
Fax:	☐ Withdrawal of Existing Standard
~~Email:~~ ***[Required Field]***	☐ Urgent Action
~~**Purpose (**Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.**)**~~	
~~**Industry Need (Provide** a detailed statement justifying the need for the proposed standard, along with any supporting documentation.**)**~~	

Brief Description (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.**)**

Purpose: (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.)

[Required Field]

Industry Need: (Provide a detailed statement justifying the need for the proposed standard, along with a technical justification and any supporting documentation.)

[Required Field -- must include technical justification (relevant studies, documentation, etc.) for a new standard or revision to an existing standard.]

Brief Description: (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.)

[Required Field]

Reliability Functions *[Required Field]*

~~**The Standard will Apply to the Following Functions** (Check all applicable boxes.)~~

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

The Standard will Apply to the Following Functions (Check all applicable boxes.)	
☐ Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐ Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐ Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐ Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐ Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐ Transmission Owner	The entity that owns and maintains transmission facilities.
☐ Transmission Operator	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
☐ Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐ Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐ Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐ Generator Owner	Entity that owns and maintains generating units.

☐

☐

Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*
☐ 1. Interconnected ~~bulk power systems~~Bulk Electric System shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in
☐ 2. The frequency and voltage of interconnected ~~bulk power systems~~Bulk Electric System 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 power systems~~Bulk Electric System 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 power systems~~Bulk
☐ 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected ~~bulk power systems.~~Bulk Electric
☐ 6. Personnel responsible for planning and operating interconnected ~~bulk power systems~~Bulk Electric System shall be trained, qualified, and have the responsibility and authority to implement actions.
☐ 7. The security of the interconnected ~~bulk power systems~~Bulk Electric System shall be assessed, monitored, and maintained on a wide-area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
Recognizing that reliability is an Common Attribute of a robust North American economy:
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes

4. A reliability 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 a standard based on this description.)

[Required Field – Provide: 1) Necessary information to assist the drafting team (which is to include relevant study results and documentation), to the extent feasible, to allow them to draft the standard, 2) Any existing known cross references to NPCC or NERC documents and 3) Technical background for the RSAR to properly address the need for the standard.]

Related Standards *[Required Field, to extent known]*

Standard No.	Explanation

Related SARs or RSARs *[Required Field, to extent known]*

SAR ID	Explanation

APPENDIX B: SELECTION OF DRAFTING TEAM MEMBERS

A regional standard drafting team shall be comprised of Subject Matter Experts (SMEs) from NPCC Task Forces and Working Groups as determined by the RCC, and from industry. The guidelines provided herein primarily address overall team requirements and more specifically those of a SME.

Formal membership on a drafting team should be reserved only for those individuals who intend to work consistently, diligently, and professionally on what is required to be done for a regional standard. Drafting team members are expected to contribute meaningfully to the ongoing development of the standard.

Drafting Team members must be:

- Committed to participating in scheduled drafting team meetings, teleconferences, as well as industry outreach (e.g., workshops and webinars)
- Willing to lead teams / sub-teams, as necessary
- Champions for standard development and promoters of the approval of the standard
- Open to consider the comments of others and provide constructive feedback

Subject Matter Experts should possess the necessary expertise and knowledge regarding the topic of the standard. The SMEs should represent a cross section of the registered entities applicable to the standard under development as well as geographical areas within the NPCC footprint.

Industry stakeholders may nominate themselves for consideration by the NPCC Regional Standards Committee (RSC) for the specific drafting team vacancies by completing the following drafting team Self Nomination form and submitting it to NPCC Manager of Reliability Standards, at npccstandard@npcc.org.

Nomination Form for NPCC [Name of drafting team] Drafting Team

Please return this form as soon as possible. If you have any questions, please contact the NPCC Standards Staff at npccstandard@npcc.org.

By submitting the following information you are indicating your willingness and agreement to actively participate in the drafting team meetings if appointed to the drafting team by the NPCC Regional Standards Committee (RSC). This means that if you are appointed to the DT you are expected to attend all (or at least the vast majority) of the face-to-face DT meetings as well as participate in all the DT meetings held via conference calls. Failure to do so shall result in your removal from the DT.

Name:	
Organization:	
Address:	
Telephone:	

E-mail:	

Please briefly describe your experience and qualifications to serve on the requested drafting team.

If you are currently a member of any NERC or Regional drafting teams, please list each team here.

- ☐ Not currently on any active SAR or standard drafting team.
- ☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any drafting team please identify the team(s).

- ☐ No prior NERC or Regional SAR or standard drafting team experience.
- ☐ Prior experience on the following team(s):

Select each NERC Region that you represent:	Select each Industry Segment that you represent:	
☐ ERCOT	☐	1 — Transmission Owners
☐ FRCC	☐	2 — RTOs, ISOs
☐ MRO	☐	3 — Load-serving Entities
☐ NPCC	☐	4 — Transmission-dependent Utilities
☐ RFC	☐	5 — Electric Generators
☐ SERC	☐	6 — Electricity Brokers, Aggregators, and Marketers
☐ SPP	☐	7 — Large Electricity End Users
☐ WECC	☐	8 — Small Electricity End Users
☐ NA – Not Applicable	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities
	☐	NA – Not Applicable

Select each Function[20] in which you have current or prior expertise:

☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

[20] These functions are defined in the NERC Functional Model, which is downloadable from the NERC website.

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group.			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

APPENDIX C: MAINTENANCE OF REGIONAL STANDARDS AND PROCESS

NPCC regional standards and the Regional Standard Processes Manual are living documents that will be updated periodically to remain current and viable (e.g., respond to changing conditions, as well as to incorporate lessons learned and process improvements).

MAINTENANCE OF REGIONAL STANDARDS

NPCC regional standards will be posted for open process review by the RSC for possible revision at least once every five (5) years[21] after the first regulatory approval and follow the same process as in the case of a new standard. If no changes are warranted, the Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or retire a regional standard, a Regional Standard Authorization Request shall be prepared by the RSC and submitted in accordance with the NPCC regional standards process. The existing, approved standard subject to revision will remain in effect until such time as the revised version has received FERC or applicable Provincial Governmental Authorities approvals, as appropriate, at which time it will be retired in accordance with any applicable implementation plan associated with the newly approved regional standard.

MAINTENANCE OF THE REGIONAL STANDARDS PROCESS

This NPCC Regional Standards Process will be reviewed for possible revision at least once every five (5) years, or more frequently if needed, and subject to the same procedure as applies to the development of a Regional Standard. All such revisions shall be subject to approval by the NPCC Board of Directors, NERC Board of Trustees, FERC, and may be subject to approval, if required, by Applicable Governmental Authorities in Canada.

[21] More frequent reviews of NPCC regional standards may be required to promptly evaluate new or revised NERC reliability standards to ensure NPCC regional standards remain consistent and more stringent than continent-wide reliability standards.

APPENDIX D: NPCC CLARIFICATION REQUEST



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

Note: A valid clarification request is one that requests additional clarity about one or more requirements in approved NPCC regional standards, but does not request approval as to how to comply with one or more requirements.

When completed, email this form to: npccstandard@npcc.org
For questions about this form or for assistance in completing the form, call Lee Pedowicz at 212-840-1070.

Request for an Clarification of a Regional Standard	
Date submitted:	
Contact information for person requesting the clarification:	
Name:	
Organization:	
Telephone:	E-mail:
Identify the standard that needs clarification:	
Standard Number (include version number, e.g. PRC-006-NPCC-1):	
Standard Title:	
Identify specifically what requirement needs clarification:	
Requirement Number and Text of Requirement:	
Identify the nature of clarification that is requested: (Check as many as applicable)	
☐ Clarify the required performance ☐ Clarify the conditions under which the performance is required ☐ Clarify which functional entity is responsible for performing an action in a requirement ☐ Clarify the reliability outcome the requirement is intended to produce Please explain the clarification needed:	
Identify the material impact associated with this clarification:	

Identify the material impact to your organization or others, if known, caused by the lack of clarity or an incorrect clarification of this standard.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Protection System Maintenance Reliability Standard	**)** **)**	**Docket No. RM14-8-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC")[1] hereby provides comments in response to the Notice of Proposed Rulemaking ("NOPR")[2] regarding proposed Reliability Standard PRC-005-3 (Protection System and Automatic Reclosing Maintenance), issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") in this proceeding on July 17, 2014. In the NOPR, the Commission proposes to approve proposed Reliability Standard PRC-005-3 to supersede Reliability Standard PRC-005-2 (Protection System Maintenance). The Commission also proposes to direct NERC to modify the proposed Reliability Standard to add the maintenance and testing of supervisory relays for Automatic Reclosing such as synchronism check and voltage relays. In addition, the Commission proposes to direct NERC to: (1) submit a report that addresses whether the proposed Reliability Standard applies to an appropriate set of autoreclosing relays that can affect Bulk-Power System reliability; and (2) add tracking of automatic reclosing misoperations to NERC's data collection efforts going forward. As discussed more fully below, the Commission seeks comment on

[1] The Federal Energy Regulatory Commission certified NERC as the electric reliability organization in its order issued on July 20, 2006, in Docket No. RR06-1-000. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

[2] *Protection System Maintenance Reliability Standard*, Notice of Proposed Rulemaking, 148 FERC ¶ 61,041 (2014). NERC notes that the title of the modified PRC-005 standard is now "Protection System and Automatic Reclosing Maintenance" and suggests that the Commission modify the title of the proceeding in its final rule to "Protection System and Automatic Reclosing Maintenance Reliability Standard" in order to avoid confusion with its final rule approving PRC-005-2. NERC inadvertently captioned the title of the proposed standard in its petition as "PRC-005-3 (Protection System Maintenance)" instead of "PRC-005-3 (Protection System and Automatic Reclosing Maintenance)."

certain aspects of the proposed Reliability Standard and the proposed actions by the Commission.

As discussed more fully below, NERC supports the Commission's proposal to approve the proposed Reliability Standard. NERC also acknowledges the issues the Commission raises in the NOPR regarding the inclusion of maintenance and testing of certain supervisory devices for autoreclosing. In light of the Commission's concerns and in the interest of improving reliability, NERC would support the addition of voltage supervision and, where used, supervisory inputs associated with selective autoreclosing in the coverage of PRC-005. NERC would also support the addition of synchronism check supervision as it provides a reliability benefit without a significant increase in maintenance burden on industry.

However, NERC does not support the Commission's proposed directives related to further data collection and verification of the applicability thresholds as currently drafted in the NOPR. NERC is generally not opposed to measuring the effectiveness of a proposed Reliability Standard through analysis of data. In this instance, the Commission has not yet justified why further evaluation of the effectiveness of the proposed applicability thresholds is necessary in the short term or why NERC should continue data collection of misoperations information for automatic reclosing on a going forward basis.

Finally, NERC explains how its current project to modify the PRC-005 Reliability Standard addresses the Commission's inquiry on the reasonableness of proposed record retention obligations through a reduction in the required period for document retention.

I. Notices and Communications

Notices and communications with respect to this filing may be addressed to the following:[3]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
William H. Edwards*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

Valerie Agnew*
Director of Standards
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile
valerie.agnew@nerc.net

II. Coverage of Supervisory Devices

A. Supervisory Devices

In the NOPR, the Commission states that the proposed PRC-005-3 Reliability Standard does not include supervisory devices such as synchronism check or voltage relays that may be critical to the operation of an autoreclosing scheme. The Commission continues that the supervisory devices, like synchronism check relays, are "applied to monitor voltages on both sides of a circuit breaker to allow autoreclosing for desirable conditions (e.g., proper phase angle and voltage) or block autoreclosing for undesirable conditions.[4] The Commission explains that "these supervisory devices essentially 'supervise' the actions of an autoreclosing scheme; i.e.,

[3] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2014), to allow the inclusion of more than two persons on the service list in this proceeding.

[4] NOPR at P 28.

allow autoreclosing for desirable conditions or block autoreclosing for undesirable conditions."[5] The Commission asserts that NERC has not explained in its petition how a failure of a synchronism check relay for undesirable conditions would not allow autoreclosing.[6] The Commission proposes to direct that NERC develop modifications to PRC-005-3 that address the appropriateness of including supervisory relays under the mandatory maintenance and testing provisions of the PRC-005 Reliability Standard.

While NERC supports the standard as proposed, NERC acknowledges the issues the Commission raises in the NOPR regarding the inclusion of maintenance and testing of certain supervisory devices for autoreclosing. In light of the Commission's concerns, NERC suggests modifying the proposed Reliability Standard to include maintenance of supervision functions for which a failure can result in autoreclosing into a fault and potentially cause generating unit or plant instability. NERC would support the addition of voltage supervision and, where used, supervisory inputs associated with selective autoreclosing in the coverage of PRC-005.[7] The analysis in the report by the System Analysis and Modeling Subcommittee ("SAMS") and System Protection and Control Subcommittee ("SPCS") ("SAMS/SPCS Report")[8] identified that

---

5 NOPR at P 30.

6 *Id.* (citing *Interpretation of Protection System Reliability Standard*, Order No. 758, 138 FERC ¶ 61,094 at P 24) (2012)). In Order No. 758, the Commission explains that that "a misoperating or miscoordinated reclosing relay may result in the reclosure of a Bulk-Power System element back onto a fault or that a misoperating or miscoordinated reclosing relay may fail to operate after a fault has been cleared, thus failing to restore the element to service." The Commission goes on to explain that misoperated or miscoordinated relays may result in damage to the Bulk-Power System such as excessive shaft torques and winding stresses and exposure of circuit breakers to systems conditions less than optimal for correct operation. Order No. 758 at P 24.

7 In preparing these comments, NERC has reviewed the SAMS/SPCS Report, which provides a thorough analysis of the Commission's concern that autoreclosing failures may impact reliable operation of the Bulk-Power System following reclosure of a Bulk-Power System element back onto a fault, or failure of a reclosing relay to operate after a fault has been cleared, thus failing to restore the element to service. NERC has also consulted with its internal subject matter experts on which supervisory devices should be included within NERC's PRC-005 standard to meet the Commission's concerns raised in the NOPR and ensure entities properly maintain the devices in order to minimize the risk of failure.

8 As noted in the Petition, the SAMS and SPCS jointly performed a technical study to determine which reclosing relays should be addressed within PRC-005 and provide advice to the Standard Drafting Team regarding appropriate maintenance intervals and activities for those relays. *See* NERC Petition at Ex. D.

the failure mode of concern is associated with premature autoreclosing into a fault, which creates the potential for generating unit or plant instability. As noted in the SAMS/SPCS Report, this may occur due to a timing failure in the autoreclosing relay or when a supervision failure results in autoreclosing into a dead-line with a fault when this closing is not intended. Autoreclosing into a fault when dead-line closing is not intended could result from failure of voltage supervision or, when used, failure of a selective autoreclosing input, such as a protective relay output that blocks autoreclosing following a three-phase fault.

NERC would also support the addition of synchronism check supervision. Undesired autoreclosing due to a supervision failure is an infrequent, unplanned disturbance, which falls into the category of unplanned and unavoidable disturbances contemplated in the accepted industry practice for switching near generating stations. For these reasons, NERC asserts that synchronism check failures do not have the potential to affect reliable operation of the Bulk-Power System. However, NERC acknowledges that including synchronism check supervision, as suggested by the Commission, would provide a reliability benefit. Therefore, NERC supports the addition of this device to meet the Commission's concerns. NERC also notes that if the Commission decides to direct inclusion of synchronism check relays in PRC-005-3, the incremental burden on entities to include these within the maintenance and testing program would not be significant.

Inclusion of the maintenance and testing of the above identified devices would: (1) address the Commission's concerns set forth in the NOPR; (2) meet a reliability concern related to "Supervision Function Failures" as identified in the SAMS/SPCS Report[9]; and (3) not be

[9] SAMS/SPCS Report, Ex. D of NERC's Petition at 6.

unduly burdensome to industry to include verification of these permissive inputs in all cases where an autoreclosing relay is subject to PRC-005-3.

If the Commission issues its proposed directive, NERC requests that the Commission direct NERC to develop modifications to PRC-005-3 to include only those supervisory devices related to autoreclosing that are needed to directly address the Commission's concerns raised in the NOPR.[10] A clear and limited directive would provide industry with certainty as to which supervisory devices need to be included in PRC-005-3 in order to address the issues identified by the Commission. In addition, NERC asks the Commission to provide its position on whether the devices identified in NERC's comments would address the Commission's concerns. The Commission's opinion on NERC's suggested additions to the PRC-005 standard would assist NERC during the standard development process to design modifications that would ultimately meet the Commission's concerns related to supervisory devices.

B. Clarification of SAMS/SPCS Report Findings on Synchronism Check Relays

In the NOPR, the Commission states "NERC has not explained in its petition how failure of a synchronism check relay for *undesirable conditions*, such as when static angles are greater than designed, would not allow autoreclosing and, consequently the concern discussed in Order No. 758."[11] The Commission further states that SAMS and SPCS dismissed the need to consider supervision failures because the subcommittees believe supervisory device failures to be a small subset of autoreclosing failures.[12]

---

[10] Some industry participants questioned NERC as to whether the Commission's directive was to include all supervisory devices used in conjunction with an applicable autoreclosing relay.

[11] NOPR at P 30.

[12] The NOPR also states that the Commission rejected almost identical arguments in Order No. 733 regarding inclusion of supervisory relays. NERC asserts that the circumstances related to autoreclosing supervision is substantially different as explained in these comments, because the SAMS/SPCS Report does not use this as a sole basis for excluding supervisory devices; rather, the report only cites the infrequent nature of certain failures in relation to accepted industry practice to conduct planned switching operations, such as simple line restoration, in a

NERC asserts that the Commission has read the SAMS/SPCS Report discussion out of context. The SAMS/SPCS Report does state that premature autoreclosing due to a supervision failure is a small subset of autoreclosing failures (the overwhelming majority of autoreclosing failures are failure to close) and is an infrequent, unplanned disturbance. However, the SAMS/SPCS Report does not use this statement to dismiss concern with all supervisory device failures. Rather, this statement is one part of the rationale regarding why it is not necessary to consider the incremental shaft fatigue that may occur for infrequent events as the basis for whether to include maintenance and testing of autoreclosing relays in PRC-005. The SAMS/SPCS Report explains that autoreclosing when static angles are greater than designed contributes to cumulative shaft fatigue, rather than impacting reliable operation of the Bulk-Power System. The SAMS/SPCS analysis concludes that the incremental shaft fatigue is acceptable because, consistent with accepted industry guidance, planned switching operations (e.g., simple line restoration) are conducted in a way that avoids significant contribution to cumulative shaft fatigue. Entities typically implement this guidance at generating stations by using time-delayed autoreclosing to allow shaft oscillations to dampen, and/or live-line autoreclosing or autoreclosing with synchronism check supervision to minimize shaft torque. By conducting planned switching in this manner, nearly all of the fatigue capability of the shaft is preserved to withstand the impact of unplanned and unavoidable disturbances such as faults, fault clearing, reclosing into system faults, and emergency line switching.

III. Proposed Directives Regarding Applicability Thresholds and Data Collection

In the NOPR, the Commission summarizes that NERC's proposed Reliability Standard would, consistent with Order No. 758, expand the scope of the Protection System maintenance

way that preserves fatigue capability of generating unit shafts to withstand the impact of unplanned and unavoidable disturbances.

Reliability Standard requirements to apply to a limited subset of autoreclosing relays.[13] The Commission states that NERC provided technical support for the applicability thresholds in the proposed Reliability Standard through both the SAMS/SPCS Report and the NERC study of the ten-mile threshold.[14] Despite the support NERC provides for the thresholds, the Commission, without elaboration, finds that it "nonetheless ha[s] concerns whether the thresholds are too narrow and that the standard therefore does not encompass a comprehensive set of autoreclosing relays that could affect the reliable operation of the Bulk-Power System."[15]

The Commission proposes that NERC submit a report, two years after the effective date of the standard, addressing the effectiveness of the autoreclosing provisions based on (1) actual operations data, and (2) simulated system conditions from planning assessments. For actual operations data, the Commission proposes that NERC enhance the granularity of its misoperations database to gather relevant information regarding events that involve autoreclosing relays, such as distance from the fault, whether the relay reclosed into the fault, and whether that reclosure caused or exacerbated an event. The Commission further proposes that NERC continue this enhancement of its data collection on a going forward basis. The Commission also suggests that simulated contingency analyses, generated as part of planning assessments, could serve as an appropriate benchmark or metric to assess whether the right set of autoreclosing relays is included in the proposed Reliability Standard, or whether further enhancements or modifications are appropriate to include those autoreclosing relays that affect reliable operation of the Bulk-Power System. The Commission proposes to require NERC to submit a report two years after the effective date of Reliability Standard PRC-005-3, comparing

---

13 NOPR at P 21.

14 *Id.* (citing NERC Petition at 15-21 and Ex. D at 2-7).

15 *Id.* at P 22.

the set of reclosing relays identified as having an impact on reliability using the contingency analyses generated under TPL-001-4, versus the set of relays covered by PRC-005-3.[16]

While NERC supports the Commission's proposal to approve the proposed Reliability Standard, NERC does not support the Commission's proposed directives related to further data collection and verification of the applicability thresholds as currently drafted in the NOPR. NERC is generally not opposed to measuring the effectiveness of a proposed Reliability Standard through analysis of data. However, in this case, the Commission has not justified why further evaluation of the effectiveness of the proposed applicability thresholds is necessary in the short term or why NERC should continue data collection of misoperations information for automatic reclosing on a going forward basis.[17] Further, NERC contends it has supported its proposed approach in the Reliability Standard and requests that the Commission limit its action regarding the applicability thresholds to approval and allow NERC and industry to focus their time and attention on implementing the proposed Reliability Standard.

A. NERC Support of the Applicability Thresholds

As explained in NERC's petition, the applicability thresholds meet the recommendations of the SAMS and SPCS, which conducted a lengthy review of the use of reclosing within the Bulk-Power System. The applicability section also reflects the agreement, input, and support of NERC's standard drafting team and the industry ballot body that approved the standard. In addition, prior to submitting these comments, NERC reviewed current event analysis data with respect to automatic reclosing failures to determine whether the standard drafting team failed to include applications of automatic reclosing that caused or contributed to an event. NERC

[16] *Id*. at P 26.

[17] NERC also notes that the Commission has not estimated the burden of these collections in the NOPR in its "Information Collection" analysis.

reviewed all 507 qualified events reported since the inception of the NERC Event Analysis Process in October 2010. Of the 507 events, 34 events have relay failures as a part of the event. None of these relay failures included applications of automatic reclosing failures that impact Bulk-Power System reliability.

The Commission also acknowledges in the NOPR that NERC has supported the applicability thresholds in the proposed Reliability Standard through the SAMS/SPCS Report and NERC's petition[18] and that the proposed standard adds automatic reclosing in a manner that is "consistent with the Commission's directive in Order No. 758."[19] In Order No. 758, the Commission agreed with NERC that it is reasonable to require maintenance and testing where reclosing relays are applied to meet performance requirements in approved NERC Reliability Standards, or where automatic restoration of service is fundamental to derivation of an Interconnection Reliability Operating Limit ("IROL").[20] The Commission also noted that a misoperating or miscoordinated reclosing relay may result in the reclosure of a Bulk-Power System Element back onto a fault or that a misoperating or miscoordinated reclosing relay may fail to operate after a fault has been cleared, thus failing to restore the Element to service. As explained in the SAMS/SPCS Report, failure to restore an element to service cannot impact reliable operation of the Bulk-Power System or be fundamental to establishing the transfer limit associated with an IROL because the system must be planned and operated to address the potential that a permanent fault prevents successful autoreclosing. Autoreclosing into a permanent fault results in a more severe system response than a failure to reclose, with the same result that the faulted element is not restored to service. The SAMS/SPCS Report identified that

---

18 NOPR at P 21.

19 *Id*. at P 26.

20 Order No. 758 at P 23.

the only exception is when autoreclosing is an integral part of a Special Protection System, and the proposed Reliability Standard addresses this exception by including autoreclosing applied as an integral part of a Special Protection System.[21]

The Commission further agreed in Order No. 758 with a commenter that states "specific requirements or selection criteria should be used to identify reclosing relays that affect the reliability of the Bulk-Power System."[22] NERC has created, proposed, and supported such criteria in the applicability section. The Commission continues in Order No. 758 by stating that the Reliability Standard should "provide the Transmission Owner, Generator Owner, and Distribution Provider with the discretion to include in a Protection System maintenance and testing program only those reclosing relays that the entity identifies as having an effect on the reliability of the Bulk-Power System."[23] The proposed standard establishes continent-wide criteria for inclusion of autoreclosing relays. The proposed standard also provides entities the ability to exclude autoreclosing relays, based on application of a defined test, in cases where the entity can demonstrate an autoreclosing failure will not impact reliable operation of the Bulk-Power System. This approach results in a robust solution to address the concern by ensuring consistent application on a continent-wide basis.

In addition, NERC staff and standard drafting team members engaged Commission staff throughout the standard development process to ensure that the standard was adequately covering Automatic Reclosing that may have an effect on the reliability of the Bulk-Power System. As a result of that input from Commission staff, NERC developed and provided the

---

[21] NERC notes that inclusion of autoreclosing applied as an integral part of a Special Protection System addresses the Commission concern with an event that ultimately resulted in the loss of over 4,000 MW of generation and multiple 765 kV lines.

[22] Order No. 758 at P 26.

[23] *Id*.

Commission with specific technical analysis of the 10-mile threshold used in the applicability section 4.2.6.2.[24]

Therefore, as discussed above, NERC believes that the coverage of Automatic Reclosing in the applicability section of the Reliability Standard has met all of the Commission's stated concerns in Order No. 758 with respect to setting the applicability of the proposed Reliability Standard and should be approved without additional compliance work necessary. As discussed above and in the SAMS/SPCS Report, the addition of specific supervisory functions to the proposed standard, fully addresses the Commission's concern in Order No. 758 with reclosure of a Bulk-Power System element back onto a fault.

B. Commission Concerns Regarding Applicability Thresholds

As previously noted, the Commission concludes in the NOPR that it "nonetheless ha[s] concerns whether the thresholds are too narrow and that the standard therefore does not encompass a comprehensive set of autoreclosing relays that could affect the reliable operation of the Bulk-Power System."[25] Without a more detailed description of the Commission's concerns regarding the applicability thresholds, NERC and the industry are unable to meaningfully comment on the Commission's proposal. The Commission has not adequately explained the need for further support of the proposed applicability thresholds to justify the additional burden on NERC and industry to collect, analyze, and report back to the Commission on the results, let alone permanently expand data collection indefinitely related to automatic reclosing. NERC asks that the Commission refrain from issuing any directive regarding measuring the effectiveness of the applicability thresholds through data collection and reporting and engage

[24] Section 4.2.6.2 includes Automatic Reclosing applied on the terminals of all Bulk Electric System Elements at substations one bus away from generating plants specified in applicability section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

[25] NOPR at 22.

NERC staff informally to address any concerns that the Commission may have. In the event that the Commission chooses to issue its directive, NERC requests that the Commission identify its specific concerns regarding the applicability thresholds in its final rule so that NERC is able to measure the effectiveness of the standard in a way that will address remaining concerns the Commission may have in the subsequent report. This detail will also allow NERC to limit the data collection scope to just the information necessary to meet the Commission's concerns.

The Commission has not identified a specific reliability concern for NERC to monitor or address through the additional data collection and report other than to verify the effectiveness of the standard. NERC asserts that a follow-up report is not justified since NERC adequately supports the applicability thresholds and the Commission signaled in Order No. 758 that only a subset of autoreclosing relays need to be covered in the PRC-005 standard. NERC does not see a compelling need to expand data collection at this time prior to the proposed standard's implementation. NERC and the Commission staff can revisit this issue at any time on an informal basis. NERC also uses a number of methods to measure the effectiveness of standards, not just data collection, including review by technical committees or subcommittees, periodic reviews through the standard development process, and other technical reviews as deemed necessary. NERC also continuously monitors effective Reliability Standards for issues through its compliance and enforcement program and in response to events analysis findings. NERC would have the option to pursue an expansion of its data collection efforts through Section 1600 of the NERC Rules of Procedure if at any time it determines that the reliability reason for a collection justifies the burden imposed on industry due to reporting.

C. Use of Contingency Analyses in TPL-001-4

As a separate matter, the NOPR asks NERC to address whether the information generated pursuant to the contingency analyses required by Requirement R4 of TPL-001-4 would provide a meaningful metric or benchmark in analyzing the scope of PRC-005-3. Based on NERC's understanding of the NOPR proposal regarding using TPL-001-4 as a source of information, NERC notes that simulations of autoreclosing in planning assessments pursuant to TPL-001-4 only assess the impact of successful autoreclosing (no fault present and the element is restored to service) and unsuccessful autoreclosing into a fault. The former case is the desired outcome and provides no information relative to the Commission's concern. The latter case will assess correct operation of an autoreclosing relay when a fault is still present, but will not provide information regarding the potential impact of an autoreclosing failure that may result in premature reclosing into a fault. Therefore, use of the contingency analyses in the context of measuring the effectiveness of the applicability thresholds in the proposed standard may not return meaningful information.

IV. Record Retention

As noted by the Commission, the proposed standard retains the same evidence retention requirements approved in PRC-005-2, which require entities to maintain documentation of maintenance activities for the longer of: (1) the two most recent performances of each distinct maintenance activity for the component; or (2) all performances of each distinct maintenance activity for the component since the previous scheduled audit date.[26] This could result in entities retaining evidence for up to twenty-four years (two maintenance cycles). The Commission seeks comment regarding the reasonableness of the proposed data retention obligations.

[26] NOPR at 33.

NERC has consulted with its compliance staff and determined that there is not a substantial need to maintain the records for two full cycles. NERC is currently balloting changes to the PRC-005 Reliability Standard in Project 2007-17.3 (PRC-005-X) Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays)[27] and has revised the compliance section. The last ballot of the draft standard in Project 2007-17.3 achieved industry approval and will now transition to a final ballot in preparation for NERC Board of Trustees adoption and submission to the Commission. The compliance section now requires Transmission Owners, Generator Owners, and Distribution Providers to keep documentation of the most recent performance of that maintenance activity for the relevant Component in cases where the interval of the maintenance activity is longer than the audit cycle. In cases where the interval of the maintenance activity is shorter than the audit cycle, documentation of all performances of that maintenance activity for the Component since the previous scheduled audit date must be retained.

V. Conclusion

For the reasons set forth above, NERC respectfully requests that the Commission accept these comments for consideration.

Respectfully submitted,

/s/ William H. Edwards

[27] The standard development page and the draft standard PRC-005-X can be found on NERC's webpage at http://www.nerc.com/pa/Stand/Pages/Project-2007-17_3-Protection-System-Maintenance-and-Testing-Phase-3.aspx.

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
William H. Edwards
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: September 29, 2014

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 29th day of September, 2014.

/s/ William H. Edwards

William H. Edwards
Counsel for the North American Electric Reliability Corporation

SCHIFF HARDIN LLP
A Limited Liability Partnership

Owen E. MacBride
(312) 258-5680
Email: omacbride@schiffhardin.com

233 SOUTH WACKER DRIVE
SUITE 6600
CHICAGO, ILLINOIS 60606

Tel.: 312.258.5500
Fax: 312.258.5700

www.schiffhardin.com

October 14, 2014

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. RR14-6-000
Request to Submit Revisions to the 2015 Budget and Assessments of Peak Reliability, Inc. to Reflect Additional Revenues from British Columbia Hydro and Power Authority

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby submits the "Request of the North American Electric Reliability Corporation to Submit Revisions to the 2015 Budget and Assessments of Peak Reliability, Inc. to Reflect Additional Revenues from British Columbia Hydro and Power Authority" in Docket No. RR14-6.

NERC's filing consists of: (1) this transmittal letter, (2) the narrative text of this filing which follows this transmittal letter, and (3) Attachments 1, 2 and 3, all of which are being transmitted in a single pdf file.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Owen E. MacBride
Owen E. MacBride

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
Before the
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)** **)**	**Docket No. RR14-6-000**

REQUEST OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION TO SUBMIT REVISIONS TO THE 2015 BUDGET AND ASSESSMENTS OF PEAK RELIABILITY, INC. TO REFLECT ADDITIONAL REVENUES FROM BRITISH COLUMBIA HYDRO AND POWER AUTHORITY

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby requests to submit certain revisions to the 2015 Business Plan and Budget of Peak Reliability, Inc. ("Peak"), including a revised schedule of assessments which reduces Peak's 2015 assessments to all load serving entities and designees ("LSEs") in the U.S. and Mexico portions of the Western Electricity Coordinating Council ("WECC") region from the assessment amounts submitted in NERC's original August 22, 2014 filing in this docket. The revised budget and assessment schedules reflect that on October 8, 2014, Peak entered into an agreement with the British Columbia Hydro and Power Authority ("BC Hydro"), pursuant to which BC Hydro's Balancing Authority Area will remain part of the Peak Reliability Coordination Area in the Western Interconnection ("Agreement"). Under the Agreement, BC Hydro will pay its full assessment (determined using the Net Energy for Load ("NEL") method) to Peak for 2015 (and subsequent years during the term of the Agreement) and 50 percent of its assessment for 2014.

On September 30, 2014, in Docket No. RR13-9-003, the Commission approved NERC's petition for a special assessment for Peak. The need for the special assessment was based on the fact that BC Hydro and the Alberta Electricity System Operator ("AESO") had not paid their

2014 assessments to Peak.[1] The original Peak assessment to BC Hydro for 2014 was $2,073,380 (which represents 7.012% of total 2012 NEL in WECC). Pursuant to the Agreement, BC Hydro has now agreed to make a payment to Peak of $1,036,690 (50 percent of the original assessment) for 2014. Invoices have already been issued to the U.S. and Mexico LSEs in the WECC region for the 2014 special assessment approved by the Commission, and it would be confusing and administratively cumbersome to now attempt to issue revised invoices for the special assessment reflecting the payment that Peak will receive from BC Hydro for 2014. Therefore, Peak is proposing to treat the $1,036,690 payment from BC Hydro as other funding (a "Contracted Assessment") for 2014, which will increase Working Capital Reserve at December 31, 2014. The $1,036.690 increase in Working Capital Reserve in turn is being used (as described below) to reduce the 2015 Peak assessments to all U.S. and Mexico LSEs in the WECC region.

Similarly, NERC's original August 22, 2014 filing in this docket included a proposed schedule of 2015 assessments for Peak which did not allocate any portion of Peak's 2015 funding requirement to BC Hydro or the AESO. No assessments were allocated to BC Hydro or AESO because, at that time, these entities had not paid their 2014 assessments to Peak nor entered into any agreements to provide compensation or revenue to Peak for 2015.[2] Based on the Agreement, BC Hydro will now pay an assessment to Peak of $3,063,771 for 2015.[3] The amount of this BC Hydro assessment for 2015 reduces the originally-proposed 2015 Peak assessments to all U.S. and Mexico LSEs in the WECC region on a pro rata basis based on NEL.

The overall impact is that for 2015, the payments from BC Hydro of $1,036,690 for 2014 and the assessment to BC Hydro of $3,063,771 for 2015 is being used by Peak to reduce the

---

[1] *North American Electric Reliability Corporation, Order Approving Special Assessment for Peak Reliability, Inc.*, 148 FERC ¶ 61,252 (2014) ("Peak Special Assessment Order"). NERC's petition in Docket No. RR13-9-003 was filed on July 23, 2014.

[2] *See* NERC's 2015 Business Plan and Budget Filing, August 22, 2014, at 113.

[3] As shown on **Attachment 3**, BC Hydro's NEL for 2013 (the NEL data used to determine 2015 assessments) is 7.303% of the total NEL in the WECC region excluding the NEL of the AESO.

originally-proposed 2015 assessments to all U.S. and Mexico LSEs in the WECC region by $4,100,461, with the reduction allocated among those LSEs on the basis of NEL.

This filing includes the following three attachments:

Attachment 1 to this filing is a revised Total Statutory Statement of Activities, Fixed Assets Expenditures and Changes in Working Capital for Peak for 2015, reflecting the Agreement and in particular the receipt of the 2014 Contracted Assessment from BC Hydro.

Attachment 2 is a revised Table B-1, Working Capital Reserve Analysis for Peak for 2014-2015, reflecting the Agreement and in particular the impact of the Contracted Assessment payment from BC Hydro in reducing Peak's 2015 assessment requirement.

Attachment 3 is a revised 2015 assessment schedule for Peak, showing the calculation of the revised 2015 Peak assessments for all U.S. and Mexico LSEs in the WECC region.

Peak is proposing to replace the assessment schedule submitted in its 2015 Business Plan and Budget included in NERC's original August 22, 2014 filing in this docket with the revised assessment schedule in **Attachment 3**. NERC therefore requests that the Commission issue an order approving the revised 2015 assessment schedule as expeditiously as possible, so that invoices can be issued for Peak's 2015 assessments based on the revised assessment schedule.

II. NOTICES AND COMMUNICATIONS

Notices and communications concerning this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
Michael Walker
Senior Vice President and Chief
Financial and Administrative Officer
North American Electric Reliability
Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-9765 – facsimile

*Persons to be included on the Commission's official service list are identified by an asterisk.

Charles A. Berardesco*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Owen E. MacBride*
Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago, IL 60606
(312) 258-5680
(312) 258-5700 – facsimile
omacbride@schiffhardin.com

III. DISCUSSION

On July 23, 2014, NERC filed a petition in Docket No. RR13-9-003 requesting authority for a supplemental assessment for Peak for 2014, in the total amount of $4,030,696 to U.S. LSEs in the WECC region. The basis for the request was that BC Hydro and AESO had not paid their 2014 assessments to Peak, totaling $ 4,094,340.[4] As stated in that petition, BC Hydro's unpaid assessment for 2014 was $2,073,380. On September 30, 2014, the Commission issued the Peak Special Assessment Order approving the requested special assessment. WECC, as billing agent for Peak, promptly issued invoices to LSEs for the special assessment amounts authorized by the Commission. In the Peak Special Assessment Order, the Commission also directed, as proposed by NERC, that "if Peak Reliability receives any compensation from AESO or BC Hydro for 2014, Peak Reliability use the amount received as a funding source to reduce its requested assessment in the next year for which it submits a budget."[5]

On August 22, 2014, NERC submitted its 2015 Business Plan and Budget filing in this docket, which included Peak's proposed 2015 Business Plan and Budget and proposed assessments.[6] Peak's proposed 2015 assessments as submitted in that filing did not include any assessments to BC Hydro (or the AESO), because at that time, neither entity had paid its 2014 assessment to Peak nor agreed to pay assessments or other compensation to Peak for 2015.

On October 8, 2014, Peak entered into the Agreement with BC Hydro, pursuant to which BC Hydro's Balancing Authority Area will remain part of the Peak Reliability Coordination Area in the Western Interconnection. Under the Agreement, BC Hydro will pay its full assessment to Peak for 2015 (and subsequent years during the term of the Agreement) and 50

[4] The difference between the total unpaid BC Hydro and AESO assessments ($4,094,340) and the requested special assessment amount to U.S. LSEs ($4,030,696), equal to $63,644, was allocated to the LSE in the Mexico portion of the WECC region.

[5] Peak Special Assessment Order at ¶10 and 13.

[6] Peak's schedule of proposed 2015 assessments to LSEs was included with its proposed 2015 Business Plan and Budget, which is Attachment 11 to the August 22, 2014 filing.

percent of its original assessment for 2014. The payment of 50 percent of Peak's original assessment for 2014 is equal to $1,036,690 (*i.e.*, $2,073,380 times 0.50 = $1,036,690).

In accordance with the directive in the Peak Special Assessment Order, Peak is proposing to use the payment of $1,036,690 that BC Hydro will make for 2014 to reduce Peak's requested assessments for 2015, in the manner described below. Similarly, by this filing, Peak is seeking to incorporate BC Hydro's agreement to pay a NEL-based assessment for 2015 into Peak's overall calculation of its 2015 assessments, thereby reducing Peak's 2015 assessments to all U.S. and Mexico LSEs in the WECC region from the amounts requested in the original August 22, 2014 filing in this docket.

Attachment 1 is a revised Total Statutory Statement of Activities, Fixed Assets Expenditures and Changes in Working Capital for Peak for 2015, reflecting the Agreement and in particular the receipt of the Contracted Assessment for BC Hydro.[7] Specifically, BC Hydro's payment of $1,036,690 for 2014 pursuant to the Agreement is now shown in Peak's 2014 Projection as Funding that was not included in Peak's 2014 Budget. As shown on **Attachment 2** (described in the next paragraph below), the $1,036,690 of additional funding for 2014 increases Peak's projected Working Capital Reserve at December 31, 2014, and is therefore used to reduce Peak's required 2015 assessment by that same amount of $1,036,690. In the "2015 Budget" column of **Attachment 1**, the Assessments amount of $40,916,546 is lower by $1,036,690 than the 2015 Assessments amount shown in Peak's original Total Statutory Statement of Activities in Attachment 11 to the August 22, 2014 filing in this docket (which was $41,953,236; *i.e.*, $41,953,236 minus $1,036,690 = $40,916,546).

Attachment 2 is a revised Table B-1, Working Capital Reserve Analysis for Peak for 2014-2015, reflecting the Agreement and in particular the impact of the Contracted Assessment

[7] Peak's original Total Statutory Statement of Activities, Fixed Assets Expenditures and Changes in Working Capital for 2015 appears on page 8 of Attachment 11 to NERC's August 22, 2014 filing in this docket.

payment from BC Hydro for 2014 in reducing the 2015 assessment requirement.[8] BC Hydro's Contracted Assessment payment of $1,036,690 for 2014 is now shown as funding received in 2014, which increases Peak's projected Working Capital Reserve at December 31, 2014 to $1,162,175 from the amount of $125,485 shown on original Table B-1. With the higher Working Capital Reserve at December 31, 2014, the adjustment to Peak's 2015 assessments to achieve its target Working Capital Reserve at December 31, 2015 of $3,230,000 (which is not changed from original Table B-1) is $2,067,825; this number is $1,036,690 lower than the adjustment amount of $3,104,515 shown on original Table B-1. As a result, Peak's required 2015 assessment shown on the revised Table B-1 is $40,916,546, which is $1,036,690 lower than the 2015 assessment amount of $41,953,236 shown on original Table B-1.

Attachment 3 shows the calculation of the revised 2015 assessments to all LSE's (excluding AESO) in the WECC Region. Each LSE's percentage of total NEL is now calculated based on a total 2013 regional NEL amount that includes BC Hydro's NEL of 59,004,439 Mwh (*see* Column 5). BC Hydro's percentage of the total NEL is 7.303% (*see* Column 7); the NEL percentages of all U.S. and Mexico LSEs in the WECC region are corresponding reduced from the percentages shown in Peak's original 2015 assessment schedule. The revised NEL percentages are used to reallocate the original 2015 assessment amount of $41,953,236 among the LSEs, as shown in Column 11. Then, the assessment amount for each LSE except BC Hydro is further reduced by its allocated (based on its NEL percentage) share of BC Hydro's Contracted Assessment payment for 2014 of $1,036,690 (*see* Column 12). BC Hydro is excluded in this step so that its own 2015 assessment amount is not reduced as a result of its 2014 Contracted Assessment payment. Column 13 of **Attachment 3** shows the final, revised 2015 assessment amounts for BC Hydro and for each LSE in the U.S. and Mexico portions of the WECC region, based on the revised total 2015 Peak assessment amount of $40,916,546.

[8] Peak's original Table B-1 for 2015 appears at page 35 of its 2015 Business Plan and Budget, Attachment 11 to the August 22, 2014 filing in this docket.

The end result of the assessment calculation procedure shown on **Attachment 3** and described in the immediately preceding paragraph is that BC Hydro's 2014 Contracted Assessment payment of $1,036,690 and its 2015 assessment of $3,063,771 serve to reduce the 2015 assessments to all LSEs in the U.S. and Mexico portions of the WECC region from the amounts shown in Peak's original 2015 assessment schedule provided in Attachment 11 to NERC's August 22, 2014 filing in this docket.

As noted earlier, promptly after the Commission issued the Peak Special Assessment Order on September 30, 2014, WECC, as billing agent for Peak, issued invoices to LSEs in the U.S. and Mexico portions of the WECC region for the special assessment amounts. For this reason, it would be confusing and administratively cumbersome to now attempt to issue revised invoices for the special assessment reflecting the payment that Peak will receive from BC Hydro for 2014 pursuant to the Agreement. Therefore, Peak is proposing to use the $1,036,690 payment from BC Hydro for 2014 in the manner described above to reduce 2015 assessments to LSEs in the U.S. and Mexico portions of the WECC region. Further, this approach complies with the directive in the Peak Special Assessment Order that "if Peak Reliability receives any compensation from AESO or BC Hydro for 2014, Peak Reliability use the amount received as a funding source to reduce its requested assessment in the next year for which it submits a budget."

As the Commission is aware, pursuant to its regulations at 18 C.F.R. §39.4(c), it issues its order on NERC's annual business plan and budget filings by November 2 of the year preceding the budget year. Invoices are then promptly issued to LSEs by NERC and, for LSE's in the WECC region, by WECC, for the assessment amounts for NERC, the Regional Entities and Peak, in order that revenues for the budget year can begin to be received in December of the preceding year and January of the budget year. Peak is proposing to replace its 2015 assessment schedule submitted in the original August 22, 2014 filing in this docket with the 2015 assessment schedule provided in **Attachment 3** to this filing. Therefore, Peak is requesting that the

Commission issue an order as expeditiously as possible approving the revised 2015 assessments in **Attachment 3**, so that WECC (as billing agent for Peak) can issue invoices for Peak's 2015 assessments during November 2015.

IV. CONCLUSION

For the reasons set forth herein, the Commission is respectfully requested to issue an order, as expeditiously as possible, approving the revisions to Peak's 2015 Business Plan and Budget provided in **Attachments 1** and **2** to this filing and authorizing Peak's revised 2015 assessments to U.S. LSEs in the WECC region shown in **Attachment 3** to this filing.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
Michael Walker
Senior Vice President and Chief
Financial and Administrative Officer
North American Electric Reliability
Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-9765 – facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Owen E. MacBride
Owen E. MacBride
Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago IL 60606
(312) 258-5680
(312) 258-5700 – facsimile
omacbride@schiffhardin.com

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 Chicago, Illinois, this 14th day of October, 2014.

/s/ Owen E. MacBride
Owen E. MacBride

Attorney for North American
Electric Reliability Corporation

ATTACHMENT 1

REVISED 2015 TOTAL STATUTORY STATEMENT OF ACTIVITIES, FIXED ASSETS EXPENDITURES AND CHANGE IN WORKING CAPITAL FOR PEAK RELIABILITY, INC.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget

STATUTORY

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
Funding					
Assessments	$ 29,568,031	$ 29,568,031	$ -	$ 40,916,546	$ 11,348,515
Contracted Assessment		1,036,690	1,036,690	$ -	-
Penalty Sanctions	-	-	-	-	-
Total Funding	**$ 29,568,031**	**$ 30,604,721**	**$ 1,036,690**	**$ 40,916,546**	**$ 11,348,515**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Federal Grants	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	156,000	26,800	(129,200)	78,000	(78,000)
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 29,724,031**	**$ 30,631,521**	**$ 907,490**	**$ 40,994,546**	**$ 11,270,516**
Expenses					
Personnel Expenses					
Salaries	$ 14,959,387	$ 16,965,760	$ 2,006,373	$ 18,424,141	$ 3,464,753
Payroll Taxes	963,710	1,307,150	343,440	1,299,123	335,414
Benefits	2,510,604	2,072,244	(438,360)	2,874,619	364,015
Retirement Costs	963,708	1,219,871	256,162	1,474,873	511,164
Total Personnel Expenses	**$ 19,397,409**	**$ 21,565,024**	**$ 2,167,615**	**$ 24,072,756**	**$ 4,675,347**
Meeting Expenses					
Meetings	$ 306,183	$ 256,605	$ (49,578)	$ 196,445	$ (109,738)
Travel	804,138	714,834	(89,304)	914,035	109,897
Conference Calls	45,084	29,223	(15,861)	29,144	(15,940)
Total Meeting Expenses	**$ 1,155,405**	**$ 1,000,662**	**$ (154,743)**	**$ 1,139,624**	**$ (15,781)**
Operating Expenses					
Consultants & Contracts	$ 1,267,500	$ 1,742,632	$ 475,132	$ 906,600	$ (360,900)
Office Rent	1,276,728	1,519,151	242,423	1,562,120	285,392
Office Costs	6,986,326	6,626,139	(360,187)	7,159,750	173,424
Professional Services	663,280	813,366	150,086	1,310,200	646,920
Miscellaneous	-	-	-	0	0
Depreciation	3,625,000	3,891,221	266,221	4,450,000	825,000
Total Operating Expenses	**$ 13,818,834**	**$ 14,592,510**	**$ 773,676**	**$ 15,388,670**	**$ 1,569,836**
Total Direct Expenses	**$ 34,371,648**	**$ 37,158,196**	**$ 2,786,548**	**$ 40,601,050**	**$ 6,229,402**
Indirect Expenses	**$ -**	**$ (86,122)**	**$ (86,122)**	**$ (110,328)**	**$ (110,328)**
Other Non-Operating Expenses	**$ -**	**$ 56**	**$ 56**	**$ -**	**$ -**
Total Expenses (B)	**$ 34,371,648**	**$ 37,072,131**	**$ 2,700,482**	**$ 40,490,722**	**$ 6,119,073**
Change in Assets	**$ (4,647,618)**	**$ (6,440,610)**	**$ (1,792,992)**	**$ 503,825**	**$ 5,151,442**
Fixed Assets					
Depreciation	$ (3,625,000)	$ (3,891,221)	$ (266,221)	$ (4,450,000)	$ (825,000)
Computer & Software CapEx	1,373,000	1,118,740	(254,260)	2,025,000	652,000
Furniture & Fixtures CapEx	36,000	18,000	(18,000)	11,000	(25,000)
Equipment CapEx	803,000	963,264	160,264	850,000	47,000
Leasehold Improvements	-	-	-	-	-
			-		-
Allocation of Fixed Assets	$ -	$ -	$ -	$ -	$ -
Incr(Dec) in Fixed Assets (C)	**$ (1,413,000)**	**$ (1,791,217)**	**$ (378,217)**	**$ (1,564,000)**	**$ (151,000)**
TOTAL BUDGET (B+C)	**32,958,648**	**35,280,914**	**2,322,265**	**38,926,722**	**5,968,073**
TOTAL CHANGE IN WORKING CAPITAL (A-B-C)	**$ (3,234,618)**	**$ (4,649,393)**	**$ (1,414,775)**	**$ 2,067,825**	**$ 5,302,442**
FTEs	149.1	140.1	(9.0)	162.7	13.6
HC	155.0	151.0	(4.0)	167.0	12.0

ATTACHMENT 2

REVISED TABLE B-1,

WORKING CAPITAL RESERVE ANALYSIS 2014-2015

FOR PEAK RELIABILITY, INC.

Working Capital Reserve Analysis 2014-2015

STATUTORY

Beginning Working Capital Reserve (Deficit), December 31, 2013		0
Plus: Transfer of Reserves from WECC, January 2, 2014		5,811,568
Plus: 2014 Funding (from Load Serving Entities (LSE) or designees)		29,568,031
Plus: 2014 Contracted Assessments		1,036,690
Plus: 2014 Other funding sources		26,800
Less: 2014 Projected expenses & capital expenditures		(35,280,914)
Projected Working Capital Reserve (Deficit), December 31, 2014		**1,162,175**
Desired Working Capital Reserve, December 31, 2015	[1]	3,230,000
Less: Projected Working Capital Reserve, December 31, 2014		(1,162,175)
Increase(decrease) in assessments to achieve desired Working Capital Reserve		2,067,825
2015 Expenses and Capital Expenditures		38,926,722
Less: Other Funding Sources		(78,000)
Adjustment to achieve desired Working Capital Reserve		2,067,825
2015 Peak Assessment		**40,916,546**

ATTACHMENT 3

REVISED 2015 ASSESSMENTS SCHEDULE

FOR PEAK RELIABILITY, INC.

Revised Allocation of 2015 Peak Reliability Assessments
2013 NEL

1	2	3	4	5	6	7	8	9	10	11	12	13
Load Serving Entity	Balancing Authority	NEL w/o AESO	US NEL	Canada NEL	Mexico NEL	Percent Peak Total (w/o AESO)	Percent US Total	Percent Canada Total	Percent Mexico Total	Funding Allocation	Allocation of BCH 2014 Payment	Funding Less BCH Pymt = Assessments
Aguila Irrigation District - APS	Arizona Public Service Company	31,010	31,010			0.004%	0.004%	0.000%	0.000%	1,610	(43)	1,567
Aha Macav Power Service	Western Area Power Administration, Lower Colorado Region	25,289	25,289			0.003%	0.003%	0.000%	0.000%	1,313	(35)	1,278
Ajo Improvement District	Arizona Public Service Company	13,734	13,734			0.002%	0.002%	0.000%	0.000%	713	(19)	694
Ak-Chin	Arizona Public Service Company	38,775	38,775			0.005%	0.005%	0.000%	0.000%	2,013	(54)	1,959
Arizona Public Service Company	Arizona Public Service Company	29,805,265	29,805,265			3.689%	4.042%	0.000%	0.000%	1,547,621	(41,255)	1,506,366
Arkansas River Power Authority (ARPA)	Public Service Company of Colorado	235,150	235,150			0.029%	0.032%	0.000%	0.000%	12,210	(325)	11,885
Avista Corporation	Avista Corporation	9,576,506	9,576,506			1.185%	1.299%	0.000%	0.000%	497,254	(13,255)	483,999
Barrick Goldstrike Mines Inc.	Sierra Pacific Power Company	1,179,964	1,179,964			0.146%	0.160%	0.000%	0.000%	61,269	(1,633)	59,636
Basin Electric Power Cooperative	Western Area Power Administration - Colorado Missouri	3,056,832	3,056,832			0.378%	0.415%	0.000%	0.000%	158,724	(4,231)	154,493
Basin Electric Power Cooperative	Western Area Power Administration - Upper Great Plains West	59,554	59,554			0.007%	0.008%	0.000%	0.000%	3,092	(82)	3,010
Big Bend Electric Cooperative, Inc.	Avista Corporation	139,523	139,523			0.017%	0.019%	0.000%	0.000%	7,245	(193)	7,052
Black Hills Power	Public Service Company of Colorado	1,927,008	1,927,008			0.239%	0.261%	0.000%	0.000%	100,059	(2,667)	97,392
Black Hills Power/Cheyenne Light Fuel & Power	Western Area Power Administration - Colorado Missouri	2,953,785	2,953,785			0.366%	0.401%	0.000%	0.000%	153,374	(4,089)	149,285
Black Hills State University South Dakota	Western Area Power Administration - Colorado Missouri	19,749	19,749			0.002%	0.003%	0.000%	0.000%	1,025	(27)	998
Bonneville Power Administration	Bonneville Power Administration	54,494,712	54,494,712			6.745%	7.391%	0.000%	0.000%	2,829,606	(75,430)	2,754,176
Bonneville Power Administration	Idaho Power Company	1,864,618	1,864,618			0.231%	0.253%	0.000%	0.000%	96,819	(2,581)	94,238
Bonneville Power Administration	NorthWestern Energy	779,199	779,199			0.096%	0.106%	0.000%	0.000%	40,459	(1,079)	39,380
Bonneville Power Administration	Portland General Electric Company	6,817	6,817			0.001%	0.001%	0.000%	0.000%	354	(9)	345
Bonneville Power Administration	Western Area Power Administration - Upper Great Plains West	13,511	13,511			0.002%	0.002%	0.000%	0.000%	702	(19)	683
BPA - Big Bend/Schrag Load	PUD. No. 2 of Grant County	37,344	37,344			0.005%	0.005%	0.000%	0.000%	1,939	(52)	1,887
BPA - Kittitas Load	PUD. No. 2 of Grant County	7,375	7,375			0.001%	0.001%	0.000%	0.000%	383	(10)	373
BPA - USBR Load	PUD. No. 2 of Grant County	131,805	131,805			0.016%	0.018%	0.000%	0.000%	6,844	(182)	6,662
British Columbia Hydro & Power Authority	British Columbia Hydro	59,004,439		59,004,439		7.303%	0.000%	100.000%	0.000%	3,063,771	-	3,063,771
Buckeye Water Conservation and Drainage District - APS	Arizona Public Service Company	19,821	19,821			0.002%	0.003%	0.000%	0.000%	1,029	(27)	1,002
Bureau of Reclamation (Desalter) - c/o DSW EMMO	Western Area Power Administration, Lower Colorado Region	766	766			0.000%	0.000%	0.000%	0.000%	40	(1)	39
Bureau of Reclamation (Wellfield) - c/o DSW EMMO	Western Area Power Administration, Lower Colorado Region	6,499	6,499			0.001%	0.001%	0.000%	0.000%	337	(9)	328
Burlington	Public Service Company of Colorado	36,727	36,727			0.005%	0.005%	0.000%	0.000%	1,907	(51)	1,856
California Independent System Operator	California Independent System Operator	232,339,960	232,339,960			28.756%	31.510%	0.000%	0.000%	12,064,123	(321,599)	11,742,524
Canby Public Utility Board	Portland General Electric Company	181,172	181,172			0.022%	0.025%	0.000%	0.000%	9,407	(251)	9,156
Central Arizona Water Conservation District	Western Area Power Administration, Lower Colorado Region	2,632,527	2,632,527			0.326%	0.357%	0.000%	0.000%	136,692	(3,644)	133,048
Central Montana Electric Power Cooperative	NorthWestern Energy	317,843	317,843			0.039%	0.043%	0.000%	0.000%	16,504	(440)	16,064
Central Montana Electric Power Cooperative	Western Area Power Administration - Upper Great Plains West	63,810	63,810			0.008%	0.009%	0.000%	0.000%	3,313	(88)	3,225
City of Aztec Electric Dept	Public Service Company of New Mexico	39,751	39,751			0.005%	0.005%	0.000%	0.000%	2,064	(55)	2,009
City of Blaine	Puget Sound Energy	78,248	78,248			0.010%	0.011%	0.000%	0.000%	4,063	(108)	3,955
City of Cheney	Avista Corporation	149,356	149,356			0.018%	0.020%	0.000%	0.000%	7,755	(207)	7,548
City of Chewelah	Avista Corporation	23,809	23,809			0.003%	0.003%	0.000%	0.000%	1,236	(33)	1,203
City of Fallon	Sierra Pacific Power Company	37,292	37,292			0.005%	0.005%	0.000%	0.000%	1,936	(52)	1,884
City of Farmington	Western Area Power Administration - Colorado Missouri	1,025,393	1,025,393			0.127%	0.139%	0.000%	0.000%	53,243	(1,419)	51,824
City of Gallup	Public Service Company of New Mexico	189,880	189,880			0.024%	0.026%	0.000%	0.000%	9,859	(263)	9,596
City of Henderson	Nevada Power Company	42,834	42,834			0.005%	0.006%	0.000%	0.000%	2,224	(59)	2,165
City of Las Vegas	Nevada Power Company	41,831	41,831			0.005%	0.006%	0.000%	0.000%	2,172	(58)	2,114
City of Mesa	Western Area Power Administration, Lower Colorado Region	261,581	261,581			0.032%	0.035%	0.000%	0.000%	13,582	(362)	13,220
City of Needles	Western Area Power Administration, Lower Colorado Region	30,990	30,990			0.004%	0.004%	0.000%	0.000%	1,609	(43)	1,566
City of North Las Vegas	Nevada Power Company	4,639	4,639			0.001%	0.001%	0.000%	0.000%	241	(6)	235
City of Page	Western Area Power Administration - Colorado Missouri	92,251	92,251			0.011%	0.013%	0.000%	0.000%	4,790	(128)	4,662
City of Plummer	Avista Corporation	35,994	35,994			0.004%	0.005%	0.000%	0.000%	1,869	(50)	1,819
City of Redding	Balancing Authority of Northern California	799,829	799,829			0.099%	0.108%	0.000%	0.000%	41,531	(1,107)	40,424
City of Roseville	Balancing Authority of Northern California	1,235,079	1,235,079			0.153%	0.168%	0.000%	0.000%	64,131	(1,710)	62,421
City of Shasta Lake	Balancing Authority of Northern California	193,187	193,187			0.024%	0.026%	0.000%	0.000%	10,031	(267)	9,764
City of Sumas	Puget Sound Energy	31,016	31,016			0.004%	0.004%	0.000%	0.000%	1,610	(43)	1,567
City of Tacoma DBA Tacoma Power	Tacoma Power	5,010,435	5,010,435			0.620%	0.680%	0.000%	0.000%	260,164	(6,935)	253,229
City of Williams	Arizona Public Service Company	39,158	39,158			0.005%	0.005%	0.000%	0.000%	2,033	(54)	1,979
Clark County Water Resources	Nevada Power Company	77,436	77,436			0.010%	0.011%	0.000%	0.000%	4,021	(107)	3,914
Clearwater Cooperative, Inc	Avista Corporation	170,714	170,714			0.021%	0.023%	0.000%	0.000%	8,864	(236)	8,628
Colorado River Commission of Nevada	Nevada Power Company	872,387	872,387			0.108%	0.118%	0.000%	0.000%	45,298	(1,208)	44,090
Colorado Springs Utilities	Public Service Company of Colorado	61,174	61,174			0.008%	0.008%	0.000%	0.000%	3,176	(85)	3,091
Colorado Springs Utilities	Western Area Power Administration - Colorado Missouri	4,662,507	4,662,507			0.577%	0.632%	0.000%	0.000%	242,098	(6,454)	235,644
Columbia River PUD	Portland General Electric Company	311,215	311,215			0.039%	0.042%	0.000%	0.000%	16,160	(431)	15,729
Comision Federal de Electricidad	Comision Federal de Electricidad	11,614,895			11,614,895	1.438%	0.000%	0.000%	100.000%	603,097	(16,077)	587,020
Consolidated Irrigation District No. 19	Avista Corporation	6,224	6,224			0.001%	0.001%	0.000%	0.000%	323	(9)	314
Deseret Generation & Transmission Cooperative	Western Area Power Administration - Colorado Missouri	144,583	144,583			0.018%	0.020%	0.000%	0.000%	7,507	(200)	7,307
Douglas Palisades / PUD No. 1 of DC	PUD. No. 2 of Grant County	19,291	19,291			0.002%	0.003%	0.000%	0.000%	1,002	(27)	975
El Paso Electric Company	El Paso Electric Company	8,354,189	8,354,189			1.034%	1.133%	0.000%	0.000%	433,786	(11,564)	422,222
Electrical District #2	Western Area Power Administration, Lower Colorado Region	179,643	179,643			0.022%	0.024%	0.000%	0.000%	9,328	(249)	9,079
Electrical District #2 - Coolidge Generating Station	Western Area Power Administration, Lower Colorado Region	9,195	9,195			0.001%	0.001%	0.000%	0.000%	477	(13)	464
Electrical District No. 6 of Pinal County - APS	Arizona Public Service Company	2,493	2,493			0.000%	0.000%	0.000%	0.000%	129	(3)	126
Electrical District No. 7 of Maricopa County - APS	Arizona Public Service Company	47,058	47,058			0.006%	0.006%	0.000%	0.000%	2,443	(65)	2,378
Electrical District No. 8 of Maricopa County - APS	Arizona Public Service Company	276,912	276,912			0.034%	0.038%	0.000%	0.000%	14,378	(383)	13,995
Electrical Districts 1 & 3	Arizona Public Service Company	578,995	578,995			0.072%	0.079%	0.000%	0.000%	30,064	(801)	29,263
Grand Valley Power	Public Service Company of Colorado	245,738	245,738			0.030%	0.033%	0.000%	0.000%	12,760	(340)	12,420
Harney Electric Cooperative, Inc.	Sierra Pacific Power Company	90,674	90,674			0.011%	0.012%	0.000%	0.000%	4,708	(126)	4,582

Revised Allocation of 2015 Peak Reliability Assessments
2013 NEL

1	2	3	4	5	6	7	8	9	10	11	12	13
Load Serving Entity	Balancing Authority	NEL w/o AESO	US NEL	Canada NEL	Mexico NEL	Percent Peak Total (w/o AESO)	Percent US Total	Percent Canada Total	Percent Mexico Total	Funding Allocation	Allocation of BCH 2014 Payment	Funding Less BCH Pymt = Assessments
Harquahala Valley Power Districts - APS	Arizona Public Service Company	79,282	79,282			0.010%	0.011%	0.000%	0.000%	4,117	(110)	4,007
Holy Cross Energy	Public Service Company of Colorado	1,218,703	1,218,703			0.151%	0.165%	0.000%	0.000%	63,280	(1,687)	61,593
Idaho County Light and Power Cooperative Association, Inc.	Avista Corporation	59,313	59,313			0.007%	0.008%	0.000%	0.000%	3,080	(82)	2,998
Idaho Power Company	Idaho Power Company	16,340,718	16,340,718			2.022%	2.216%	0.000%	0.000%	848,482	(22,618)	825,864
Imperial Irrigation District	Imperial Irrigation District	3,661,545	3,661,545			0.453%	0.497%	0.000%	0.000%	190,124	(5,068)	185,056
Inland Power and Light Company	Avista Corporation	477,845	477,845			0.059%	0.065%	0.000%	0.000%	24,812	(661)	24,151
Intermountain Rural Electric Association	Public Service Company of Colorado	2,153,915	2,153,915			0.267%	0.292%	0.000%	0.000%	111,841	(2,981)	108,860
Kaiser Aluminum Fabricated Products LLC	Avista Corporation	311,536	311,536			0.039%	0.042%	0.000%	0.000%	16,176	(431)	15,745
Kootenai Electric Cooperative, Inc.	Avista Corporation	469,569	469,569			0.058%	0.064%	0.000%	0.000%	24,382	(650)	23,732
Las Vegas Valley Water District	Nevada Power Company	93,430	93,430			0.012%	0.013%	0.000%	0.000%	4,851	(129)	4,722
Los Angeles Department of Water and Power	Los Angeles Department of Water and Power	28,866,202	28,866,202			3.573%	3.915%	0.000%	0.000%	1,498,861	(39,956)	1,458,905
Maricopa County Municipal Water Conservation Dist No. 1 - APS	Arizona Public Service Company	52,365	52,365			0.006%	0.007%	0.000%	0.000%	2,719	(72)	2,647
McMullen Valley Water Conservation & Drainage District - APS	Arizona Public Service Company	69,883	69,883			0.009%	0.009%	0.000%	0.000%	3,629	(97)	3,532
Merced Irrigation District	Turlock Irrigation District	470,352	470,352			0.058%	0.064%	0.000%	0.000%	24,423	(651)	23,772
Modern Electric Water Company	Avista Corporation	234,810	234,810			0.029%	0.032%	0.000%	0.000%	12,192	(325)	11,867
Modesto Irrigation District	Balancing Authority of Northern California	2,577,631	2,577,631			0.319%	0.350%	0.000%	0.000%	133,842	(3,568)	130,274
Montana-Dakota Utilities Co.	Western Area Power Administration - Upper Great Plains West	20,487	20,487			0.003%	0.003%	0.000%	0.000%	1,064	(28)	1,036
Mt. Wheeler Power	Sierra Pacific Power Company	560,779	560,779			0.069%	0.076%	0.000%	0.000%	29,118	(776)	28,342
Municipal Energy Agency of Nebraska	Public Service Company of Colorado	199,657	199,657			0.025%	0.027%	0.000%	0.000%	10,367	(276)	10,091
Municipal Energy Agency of Nebraska	Western Area Power Administration - Colorado Missouri	669,387	669,387			0.083%	0.091%	0.000%	0.000%	34,758	(927)	33,831
Navajo Agricultural Products Industry (NAPI)	Western Area Power Administration - Colorado Missouri	1,093	1,093			0.000%	0.000%	0.000%	0.000%	57	(2)	55
Navajo Tribal Utility Authority	Arizona Public Service Company	54,383	54,383			0.007%	0.007%	0.000%	0.000%	2,824	(75)	2,749
Navajo Tribal Utility Authority	Public Service Company of New Mexico	286,099	286,099			0.035%	0.039%	0.000%	0.000%	14,856	(396)	14,460
Navopache Electric Cooperative, Inc.	Public Service Company of New Mexico	370,656	370,656			0.046%	0.050%	0.000%	0.000%	19,246	(513)	18,733
Nebraska Public Power Marketing	Western Area Power Administration - Colorado Missouri	5,842	5,842			0.001%	0.001%	0.000%	0.000%	303	(8)	295
Nevada Power Company dba NV Energy	Nevada Power Company	26,587,371	26,587,371			3.291%	3.606%	0.000%	0.000%	1,380,534	(36,801)	1,343,733
Noble Americas Energy Solutions, LLC	Portland General Electric Company	1,673,553	1,673,553			0.207%	0.227%	0.000%	0.000%	86,898	(2,316)	84,582
Northern Lights, Inc.	Avista Corporation	36,440	36,440			0.005%	0.005%	0.000%	0.000%	1,892	(50)	1,842
NorthWestern Corp. dba NorthWestern Energy, LLC	NorthWestern Energy	9,167,768	9,167,768			1.135%	1.243%	0.000%	0.000%	476,031	(12,690)	463,341
NorthWestern Corp. dba NorthWestern Energy, LLC	Western Area Power Administration - Upper Great Plains West	241,233	241,233			0.030%	0.033%	0.000%	0.000%	12,526	(334)	12,192
Overton Power District No. 5	Nevada Power Company	381,124	381,124			0.047%	0.052%	0.000%	0.000%	19,790	(528)	19,262
PacifiCorp	Idaho Power Company	2,156	2,156			0.000%	0.000%	0.000%	0.000%	112	(3)	109
PacifiCorp	PacifiCorp Eastern Balancing Area	50,590,830	50,590,830			6.261%	6.861%	0.000%	0.000%	2,626,899	(70,026)	2,556,873
PacifiCorp	Portland General Electric Company	1,876	1,876			0.000%	0.000%	0.000%	0.000%	97	(3)	94
PacifiCorp	Western Area Power Administration - Colorado Missouri	116,284	116,284			0.014%	0.016%	0.000%	0.000%	6,038	(161)	5,877
PacifiCorp West (PACW)	PacifiCorp Western Balancing Authority	21,336,825	21,336,825			2.641%	2.894%	0.000%	0.000%	1,107,902	(29,534)	1,078,368
Pend Oreille County PUD No. 1	Avista Corporation	1,016,523	1,016,523			0.126%	0.138%	0.000%	0.000%	52,782	(1,407)	51,375
Platte River Power Authority	Public Service Company of Colorado	3,244,570	3,244,570			0.402%	0.440%	0.000%	0.000%	168,472	(4,491)	163,981
Port of Seattle - Seattle-Tacoma International Airport	Puget Sound Energy	141,204	141,204			0.017%	0.019%	0.000%	0.000%	7,332	(195)	7,137
Portland General Electric Company	Portland General Electric Company	18,600,632	18,600,632			2.302%	2.523%	0.000%	0.000%	965,827	(25,746)	940,081
Public Service Company of Colorado (Xcel)	Public Service Company of Colorado	26,537,376	26,537,376			3.284%	3.599%	0.000%	0.000%	1,377,938	(36,732)	1,341,206
Public Service Company of Colorado (Xcel)	Western Area Power Administration - Colorado Missouri	35,594	35,594			0.004%	0.005%	0.000%	0.000%	1,848	(49)	1,799
Public Service Company of New Mexico	Public Service Company of New Mexico	10,787,283	10,787,283			1.335%	1.463%	0.000%	0.000%	560,123	(14,931)	545,192
Public Utility District No. 1 of Chelan County	PUD No. 1 of Chelan County	4,025,516	4,025,516			0.498%	0.546%	0.000%	0.000%	209,023	(5,572)	203,451
PUD No. 1 of Asotin County	Avista Corporation	4,975	4,975			0.001%	0.001%	0.000%	0.000%	258	(7)	251
PUD No. 1 of Douglas County	PUD No. 1 of Douglas County	1,486,659	1,486,659			0.184%	0.202%	0.000%	0.000%	77,194	(2,058)	75,136
PUD No. 1 of Kittitas County	Puget Sound Energy	16,412	16,412			0.002%	0.002%	0.000%	0.000%	852	(23)	829
PUD No. 1 of Whatcom County	Puget Sound Energy	4,995	4,995			0.001%	0.001%	0.000%	0.000%	259	(7)	252
PUD No. 2 of Grant County	Avista Corporation	93,675	93,675			0.012%	0.013%	0.000%	0.000%	4,864	(130)	4,734
PUD No. 2 of Grant County	PUD. No. 2 of Grant County	3,839,087	3,839,087			0.475%	0.521%	0.000%	0.000%	199,342	(5,314)	194,028
Puget Sound Energy, Inc.	Puget Sound Energy	24,437,530	24,437,530			3.025%	3.314%	0.000%	0.000%	1,268,904	(33,826)	1,235,078
Raton Public Service	Public Service Company of Colorado	51,732	51,732			0.006%	0.007%	0.000%	0.000%	2,686	(72)	2,614
Roosevelt Irrigation District - APS	Arizona Public Service Company	37,851	37,851			0.005%	0.005%	0.000%	0.000%	1,965	(52)	1,913
Sacramento Municipal Utility District	Balancing Authority of Northern California	11,226,639	11,226,639			1.389%	1.523%	0.000%	0.000%	582,937	(15,540)	567,397
Salt River Project	Salt River Project	28,911,429	28,911,429			3.578%	3.921%	0.000%	0.000%	1,501,209	(40,018)	1,461,191
San Carlos Indian Irrigation Project	Arizona Public Service Company	7	7			0.000%	0.000%	0.000%	0.000%	-	-	-
Seattle City Light	Seattle Department of Lighting	10,035,929	10,035,929			1.242%	1.361%	0.000%	0.000%	521,110	(13,891)	507,219
Sierra Pacific Power Company dba NV Energy	Sierra Pacific Power Company	11,116,111	11,116,111			1.376%	1.508%	0.000%	0.000%	577,198	(15,387)	561,811
Silver State Energy - c/o Colorado River Commission of Nevada	Western Area Power Administration, Lower Colorado Region	515,076	515,076			0.064%	0.070%	0.000%	0.000%	26,745	(713)	26,032
Southern Montana Electric Generation & Transmission	NorthWestern Energy	522,515	522,515			0.065%	0.071%	0.000%	0.000%	27,131	(723)	26,408
Southern Nevada Water Authority	Nevada Power Company	118,357	118,357			0.015%	0.016%	0.000%	0.000%	6,146	(164)	5,982
Southwest Transmission Cooperative, Inc.	Western Area Power Administration, Lower Colorado Region	2,012,236	2,012,236			0.249%	0.273%	0.000%	0.000%	104,484	(2,785)	101,699
Tanner Electric Cooperative	Puget Sound Energy	99,115	99,115			0.012%	0.013%	0.000%	0.000%	5,146	(137)	5,009
The Incorporated County of Los Alamos	Public Service Company of New Mexico	364,095	364,095			0.045%	0.049%	0.000%	0.000%	18,905	(504)	18,401
Tohono O'Odham Utility Authority	Arizona Public Service Company	67,110	67,110			0.008%	0.009%	0.000%	0.000%	3,485	(93)	3,392
Tonopah Irrigation District - APS	Arizona Public Service Company	22,698	22,698			0.003%	0.003%	0.000%	0.000%	1,179	(31)	1,148
Town of Center	Public Service Company of Colorado	20,928	20,928			0.003%	0.003%	0.000%	0.000%	1,087	(29)	1,058
Town of Fredonia	Western Area Power Administration - Colorado Missouri	10,953	10,953			0.001%	0.001%	0.000%	0.000%	569	(15)	554
Town of Wickenburg	Arizona Public Service Company	26,570	26,570			0.003%	0.004%	0.000%	0.000%	1,380	(37)	1,343
Tri-State Generation & Transmission Assoc. Inc - Reliability	Public Service Company of Colorado	2,062,440	2,062,440			0.255%	0.280%	0.000%	0.000%	107,091	(2,855)	104,236
Tri-State Generation & Transmission Assoc. Inc - Reliability	Western Area Power Administration - Colorado Missouri	7,419,925	7,419,925			0.918%	1.006%	0.000%	0.000%	385,275	(10,270)	375,005

Revised Allocation of 2015 Peak Reliability Assessments
2013 NEL

1	2	3	4	5	6	7	8	9	10	11	12	13
Load Serving Entity	**Balancing Authority**	**NEL w/o AESO**	**US NEL**	**Canada NEL**	**Mexico NEL**	**Percent Peak Total (w/o AESO)**	**Percent US Total**	**Percent Canada Total**	**Percent Mexico Total**	**Funding Allocation**	**Allocation of BCH 2014 Payment**	**Funding Less BCH Pymt = Assessments**
Tri-State Generation & Transmission Association, Inc.	Public Service Company of New Mexico	2,642,944	2,642,944			0.327%	0.358%	0.000%	0.000%	137,233	(3,658)	133,575
Truckee Donner Public Utility District	Sierra Pacific Power Company	154,280	154,280			0.019%	0.021%	0.000%	0.000%	8,011	(214)	7,797
Tucson Electric Power Company	Tucson Electric Power Company	15,085,818	15,085,818			1.867%	2.046%	0.000%	0.000%	783,322	(20,881)	762,441
Turlock Irrigation District	Turlock Irrigation District	2,135,260	2,135,260			0.264%	0.290%	0.000%	0.000%	110,872	(2,956)	107,916
U.S. Army Yuma Proving Ground	Western Area Power Administration, Lower Colorado Region	16,326	16,326			0.002%	0.002%	0.000%	0.000%	848	(23)	825
U.S. BOR East Greenacres (Rathdrum)	Avista Corporation	4,176	4,176			0.001%	0.001%	0.000%	0.000%	217	(6)	211
U.S. Bor Spokane Indian Development`	Avista Corporation	3,136	3,136			0.000%	0.000%	0.000%	0.000%	163	(4)	159
Unit B Irrigation District	Arizona Public Service Company	24	24			0.000%	0.000%	0.000%	0.000%	1	-	1
US Air Force Base, Fairchild	Avista Corporation	49,053	49,053			0.006%	0.007%	0.000%	0.000%	2,547	(68)	2,479
US Dept of Energy - Kirtland AFB	Public Service Company of New Mexico	410,793	410,793			0.051%	0.056%	0.000%	0.000%	21,330	(569)	20,761
Wells Rural Electric Cooperative	Sierra Pacific Power Company	672,455	672,455			0.083%	0.091%	0.000%	0.000%	34,917	(931)	33,986
Wellton-Mohawk Irrigation & Drainage District	Western Area Power Administration, Lower Colorado Region	401	401			0.000%	0.000%	0.000%	0.000%	21	(1)	20
West Oregon Electric Cooperative, Inc.	Portland General Electric Company	12,860	12,860			0.002%	0.002%	0.000%	0.000%	668	(18)	650
Western Area Power - Loveland, CO	Public Service Company of Colorado	364,173	364,173			0.045%	0.049%	0.000%	0.000%	18,909	(504)	18,405
Western Area Power - Loveland, CO	Western Area Power Administration - Colorado Missouri	2,054,674	2,054,674			0.254%	0.279%	0.000%	0.000%	106,688	(2,844)	103,844
Western Area Power Administration - CRSP	Western Area Power Administration - Colorado Missouri	2,053,652	2,053,652			0.254%	0.279%	0.000%	0.000%	106,635	(2,843)	103,792
Western Area Power Administration - Sierra Nevada Region	Balancing Authority of Northern California	1,324,532	1,324,532			0.164%	0.180%	0.000%	0.000%	68,776	(1,833)	66,943
Western Area Power Administration-Desert Southwest Region	Western Area Power Administration, Lower Colorado Region	3,225,943	3,225,943			0.399%	0.438%	0.000%	0.000%	167,505	(4,465)	163,040
Western Area Power Administration-Upper Great Plains Region	NorthWestern Energy	7,688	7,688			0.001%	0.001%	0.000%	0.000%	399	(11)	388
Western Area Power Administration-Upper Great Plains Region	Western Area Power Administration - Upper Great Plains West	391,282	391,282			0.048%	0.053%	0.000%	0.000%	20,317	(542)	19,775
Wyoming Municipal Power Agency	Western Area Power Administration - Colorado Missouri	280,327	280,327			0.035%	0.038%	0.000%	0.000%	14,556	(388)	14,168
Yampa Valley Electric Association	Public Service Company of Colorado	630,694	630,694			0.078%	0.086%	0.000%	0.000%	32,748	(873)	31,875
Yuma Irrigation District	Arizona Public Service Company	3,112	3,112			0.000%	0.000%	0.000%	0.000%	162	(4)	158
Yuma-Mesa Irrigation District	Arizona Public Service Company	175	175			0.000%	0.000%	0.000%	0.000%	9	-	9
		807,967,432	**737,348,098**	**59,004,439**	**11,614,895**	**100.000%**	**100.000%**	**100.000%**	**100.000%**	**41,953,236**	**(1,036,690)**	**40,916,546**
		-	**91.3%**	**7.3%**	**1.4%**	-	-	-	-	-	-	-
			-	-	-							

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC	**)**	**Docket No. RR10-1-___**
RELIABILITY CORPORATION	**)**	**Docket No. RR13-3-___**

ANNUAL REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON WIDE-AREA ANALYSIS OF TECHNICAL FEASIBILITY EXCEPTIONS

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

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

September 30, 2014

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby provides the 2014 Annual Report on Wide-Area Analysis of Technical Feasibility Exceptions (the "2014 Annual Report") in compliance with Paragraphs 220 and 221 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Order No. 706[1] and Appendix 4D of the NERC Rules of Procedure ("ROP").

In Order No. 706, FERC approved eight Critical Infrastructure Protection ("CIP") Reliability Standards and, among other things, directed NERC to develop a set of conditions or criteria that a Responsible Entity must follow to obtain a Technical Feasibility Exception ("TFE") from specific requirements in the CIP Reliability Standards.[2] The Commission stated that the TFE process must include: mitigation steps, a remediation plan, a timeline for eliminating the use of the TFE unless appropriate justification otherwise is provided, regular review of the continued need for the TFE, internal approval by senior managers, and regional approval through the Electric Reliability Organization ("ERO").[3]

Order No. 706 also required that NERC submit an annual report to the Commission that provides a wide-area analysis of the use of TFEs and their effect on Bulk-Power System reliability. The Commission stated:

> The annual report must address, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address vulnerabilities, and efforts to eliminate future reliance on the exception. . . [T]he report should contain aggregated data with sufficient detail for the Commission to understand the frequency with which

---

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (January 18, 2008) ("Order No. 706").

[2] *Id.* at P 178.

[3] *Id.* at P 222.

> specific provisions are being invoked as well as high level data regarding mitigation and remediation plans over time and by region . . . .[4]

In October 2009, NERC filed amendments to its ROP to implement the Commission's directive in Order No. 706, proposing Section 412 (Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards) and Appendix 4D (Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards). In a January 21, 2010 order, the Commission approved NERC's amended ROP.[5]

On April 8, 2013, NERC filed revisions to Appendix 4D of the ROP to streamline the TFE approval process reflecting NERC, Regional Entity and industry experience processing TFE requests since the inception of the program. On September 3, 2013, FERC approved the proposed revisions and directed limited revisions to Appendix 4D, including modifications to: (1) specify a time frame for reporting Material Changes to TFEs upon identification and discovery; and (2) require the annual TFE report to include information on Material Change Reports and TFE expiration dates.[6] NERC submitted a compliance filing consistent with the directives from the September 2013 Order, which the Commission approved on January 30, 2014.[7] Sections 11.2.4 and 13 of Appendix 4D set forth the requirements for the annual TFE report, as modified in

---

4 *Id*. at P 220.

5 *North American Electric Reliability Corp.*, 130 FERC ¶ 61,050 (2010), *order on compliance*, 133 FERC ¶ 61,008 (2010) (October 1 Order), *order on reh'g*, 133 FERC ¶ 61,209 (2010), *order on compliance*, 135 FERC ¶ 61,026 (2011) (April 12 Order). The Commission requested further information and clarification regarding certain aspects of the TFE process. On April 21, 2010, NERC submitted its compliance filing in response to the January 21 Order. On October 1, 2010, the Commission issued an order accepting NERC's April 2010 filing as partially compliant and directing further changes to the TFE Procedure. October 1 Order, 133 FERC ¶ 61,008. On December 23, 2010, NERC submitted a compliance filing in response to the Commission's October 1 Order, which the Commission subsequently accepted. April 12 Order, 135 FERC ¶ 61,026.

6 *North American Electric Reliability Corporation*, 144 FERC ¶ 61,180 (2013) ("September 2013 Order").

7 Letter Order, Docket No. RR13-3-001 (Jan. 30, 2014).

accordance with the September 2013 Order. The 2014 Annual Report includes the information required by the September 2013 Order.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G St., N.W., Suite 600
Washington, DC 20005
202-400-3000
holly.hawkins@nerc.net
shamai.elstein@nerc.net

III. 2014 ANNUAL REPORT

In accordance with Appendix 4D of the ROP, NERC prepared the 2014 Annual Report in consultation with the Regional Entities. The Regional Entities provided regular reports to NERC regarding the types of Covered Assets for which the Regional Entities have approved TFEs.[8] In addition, each Regional Entity provided information on the 10 elements identified in Section 13 of Appendix 4D to be included in the 2014 Annual Report. NERC compiled and analyzed the TFE data provided by the Regional Entities in preparation for the 2014 Annual Report.

In addition to the new information required by the September 2013 Order regarding Material Change Reports and TFE expiration dates, there are two other differences between the 2014 Annual Report and prior annual reports. First, as a result of the new streamlined TFE process approved in the September 2013 Order, there is no longer a two-step process for evaluating TFE requests. Prior to the revisions, the Regional Entities would conduct an initial review to determine

[8] As defined in Appendix 4D, a Covered Asset is a Cyber Asset or Critical Cyber Asset that is subject to a TFE.

whether the request was complete and could move to a formal ERO review (i.e., initial acceptance or rejection). Data regarding this initial step was included in prior annual reports.[9] As that initial step is no longer part of the TFE approval process and a request for a TFE proceeds directly to formal review, the 2014 Annual Report does not include any data on initial acceptances or rejections, only the number of TFE requests that were submitted and approved/disapproved.

Second, during the course of the reporting period for the 2014 Annual Report, Requirement R2.6 of Reliability Standard CIP-005-3a was retired.[10] Because TFEs for CIP-005-3a, Requirement R2.6 were only applicable for a portion of the reporting period and are not relevant going forward, the 2014 Annual Report does not include data on TFEs for CIP-005-3a, Requirement R2.6.

a. Elements Required by Appendix 4D, Section 13.1

The following is a summary of the TFE data reported by each Regional Entity for the 10 elements identified in Section 13.1 of Appendix 4D:[11]

1. *The frequency of use of the TFE Request process, disaggregated by Regional Entity and in the aggregate for the United States and for the jurisdictions of other Applicable Governmental Authorities, including (A) the numbers of TFE Requests that have been submitted, accepted/rejected, and approved/disapproved during the preceding year and cumulatively since the effective date of this Appendix, (B) the numbers of unique Covered Assets for which TFEs have been approved, (C) the numbers of approved TFEs that are still in effect as of on or about the date of the Annual Report; (D) the numbers of approved TFEs that reached their Expiration Dates or were terminated during the preceding year;*

[9] Tables 2 and 3 of the 2013 Annual Report included information on the initial acceptances and rejections, respectively.

[10] *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, 145 FERC ¶ 61,147 (2013).

[11] Unless stated otherwise, a table or reference to "2014" refers to the reporting period for this report: July 1, 2013 – June 30, 2014.

and (E) the numbers of approved TFEs that are scheduled to reach their Expiration Dates during the ensuing year.

a. TFE Requests that have been Submitted and Approved/Disapproved

During the 2014 reporting period (July 1, 2013 through June 30, 2014) there were 692 new TFE requests submitted, of which 611 were approved. For purposes of this report, "submitted" indicates a new request (as opposed to an amendment or change to a previously received request).[12] Table 1, below, provides the number of new TFE requests submitted to the ERO during the 2014 reporting period per CIP requirement and Region.

U.S. Entities only	Table 1: Requests for New TFEs Submitted during Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	1	0	2	2	0	0	5
005 R3.1	0	0	0	3	1	0	0	2	6
005 R3.2	0	0	1	4	13	1	0	3	22
006 R1.1	0	0	0	7	6	0	0	0	13
007 R2.3	0	0	3	9	8	2	3	25	50
007 R3	14	4	0	10	3	9	7	9	56
007 R4	13	3	31	35	45	13	13	65	218
007 R5.3	4	2	11	10	22	13	6	21	89
007 R5.3.1	0	0	0	5	5	2	0	9	21
007 R5.3.2	3	0	6	17	15	2	7	11	61
007 R5.3.3	2	0	6	11	15	2	2	9	47
007 R6	2	3	6	13	22	7	4	30	87
007 R6.3	0	0	5	1	4	2	1	4	17
Totals	38	12	70	125	161	55	43	188	692

Table 2 shows the number of those new TFE requests that were approved and Table 3 shows the number of those new TFE requests that were disapproved during the 2014 report period.

[12] Information regarding amendment to active TFEs approved during the 2014 reporting period is provided below in Table 13.

U.S. Entities only	Table 2: TFE Requests Submitted & Approved during Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	1	0	1	1	0	0	3
005 R3.1	0	0	0	2	1	0	0	2	5
005 R3.2	0	0	1	4	13	1	0	3	22
006 R1.1	0	0	0	6	5	0	0	0	11
007 R2.3	0	0	3	8	7	2	2	25	47
007 R3	6	4	0	10	2	7	1	9	39
007 R4	12	3	31	31	34	13	12	60	196
007 R5.3	3	3	11	9	22	12	6	21	87
007 R5.3.1	0	0	0	4	2	2	0	8	16
007 R5.3.2	3	0	6	11	8	2	6	10	46
007 R5.3.3	2	0	6	9	11	2	2	7	39
007 R6	1	3	6	13	21	7	4	29	84
007 R6.3	0	0	5	1	4	2	0	4	16
Totals	27	13	70	108	131	51	33	178	611

U.S. Entities only	Table 3: TFE Requests Submitted & Disapproved during Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	0	0	1	1	0	0	2
005 R3.1	0	0	0	1	0	0	0	0	1
005 R3.2	0	0	0	0	0	0	0	0	0
006 R1.1	0	0	0	1	1	0	0	0	2
007 R2.3	0	0	0	1	1	0	1	0	3
007 R3	8	0	0	0	1	2	6	0	17
007 R4	0	0	0	4	11	0	1	5	21
007 R5.3	0	-1	0	1	0	1	0	0	1
007 R5.3.1	0	0	0	1	3	0	0	1	5
007 R5.3.2	0	0	0	6	7	0	1	1	15
007 R5.3.3	0	0	0	2	4	0	0	2	8
007 R6	0	0	0	0	1	0	0	1	2
007 R6.3	0	0	0	0	0	0	1	0	1
Totals	8	-1	0	17	30	4	10	10	78

Table 4 provides the cumulative total of TFE requests submitted since the program's inception, including the 2014 reporting period.

U.S. Entities only	Table 4: TFE Requests Submitted - Cumulative (new submissions and amendments)								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	2	12	2	10	6	3	16	42	93
005 R3.1	1	0	0	17	2	2	0	32	54
005 R3.2	5	12	4	13	35	17	106	84	276
006 R1.1	12	14	0	74	29	2	13	15	159
007 R2.3	57	31	7	117	84	12	84	237	629
007 R3	23	25	5	101	25	20	13	51	263
007 R4	138	168	66	856	391	165	378	1087	3249
007 R5.3	83	46	45	465	223	50	96	217	1225
007 R5.3.1	22	14	6	76	99	18	107	154	496
007 R5.3.2	71	49	35	337	205	45	151	245	1138
007 R5.3.3	45	55	18	169	87	28	105	201	708
007 R6	53	44	13	235	174	30	141	391	1081
007 R6.3	47	24	11	89	82	15	96	180	544
Totals	559	494	212	2559	1442	407	1306	2936	9915

Tables 5 and 6 show the cumulative number of TFEs that the ERO has approved and disapproved, respectively, since the inception of the program. As noted above, because the TFE program prior to the revisions to Appendix 4D approved in the September 2013 Order included an initial "Accepted/Rejected" phase, the totals in Tables 5 and 6 do not match the totals from Table 4. Numerous submissions included in Table 4 were initially rejected and sometimes more than once. Tables 5 and 6 only reflect those TFE requests that were accepted in the initial stage and ultimately approved or disapproved. Additionally, the automated tracking of amendments early in the TFE program resulted in amendments to existing requests or active TFE to be counted in the same way as the submission of an a new TFE request. As such, the aggregated "submissions" total in Table 4 is significantly includes both new requests and amendments and is different from the "Approved" and "Disapproved" total of new TFE requests.

U.S. Entities only	Table 5: New TFE Requests Submitted and Approved - Cumulative								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	1	9	3	4	2	1	10	6	36
005 R3.1	1	0	0	13	1	0	0	7	22
005 R3.2	3	9	10	12	24	7	54	25	144
006 R1.1	7	11	3	40	11	1	12	4	89
007 R2.3	26	25	24	69	30	10	44	97	325
007 R3	8	20	14	67	13	10	6	28	166
007 R4	95	130	316	522	229	71	228	390	1981
007 R5.3	43	35	89	278	106	30	50	89	720
007 R5.3.1	13	12	18	51	38	10	62	41	245
007 R5.3.2	44	36	71	193	104	37	95	76	656
007 R5.3.3	20	42	35	101	26	17	66	61	368
007 R6	29	39	57	139	116	27	86	135	628
007 R6.3	27	18	42	53	69	12	58	75	354
Totals	317	386	682	1542	769	233	771	1034	5734

U.S. Entities only	Table 6: New TFE Requests Submitted and Disapproved - Cumulative								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	0	0	1	1	2	3	7
005 R3.1	0	0	0	1	0	2	0	2	5
005 R3.2	0	0	0	0	3	4	9	18	34
006 R1.1	2	0	0	1	9	0	0	5	17
007 R2.3	8	1	0	2	34	0	7	30	82
007 R3	12	1	0	0	4	6	6	3	32
007 R4	7	0	0	21	63	36	16	98	241
007 R5.3	6	-1	0	6	58	7	2	32	110
007 R5.3.1	3	0	0	4	16	4	5	40	72
007 R5.3.2	3	3	0	9	37	0	6	42	100
007 R5.3.3	3	3	0	5	10	2	5	42	70
007 R6	5	0	0	9	22	4	9	48	97
007 R6.3	2	0	0	7	8	1	10	40	68
Totals	51	7	0	65	265	67	77	403	935

b. Number of Unique Covered Assets for which TFEs have been Approved

Tables 7a and 7b provide the number of unique Covered Assets for which the ERO has approved TFEs. Specifically, Table 7a details the numbers of assets, by Regional Entity, covered by TFEs for the respective requirements. Table 7b takes the total number of assets and groups them by category. Table 8 provides several examples of devices that are not clearly assigned to the more common categories and listed as "Other" in Table 7b.

U.S. Entities only	Table 7a: Assets for which TFEs were Approved								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	2	534	43	12	0	8	599
005 R3.1	0	0	0	47	5	0	0	1	53
005 R3.2	0	0	0	63	154	16	0	22	255
006 R1.1	1	0	0	8	219	0	0	0	228
007 R2.3	118	0	24	1,047	506	296	4	149	2,144
007 R3	14	13	0	953	373	81	0	17	1,451
007 R4	194	8	356	3,457	3,382	703	186	840	9,126
007 R5.3	85	41	237	2,278	2,383	379	61	411	5,875
007 R5.3.1	0	0	0	60	592	12	0	66	730
007 R5.3.2	109	0	238	1,706	1,716	245	89	134	4,237
007 R5.3.3	7	0	24	1,974	600	41	64	95	2,805
007 R6	80	7	73	1,657	2,365	377	34	583	5,176
007 R6.3	109	0	18	52	653	9	0	19	860
Totals	717	69	972	13,836	12,991	2,171	438	2,345	33,539

U.S. Entities only	Table 7b: Assets for which TFEs were Approved (includes new and amended TFEs)			
	Network Data Communications Device	Relay	Workstation/Server	Other*
FRCC	76	87	15	539
MRO	6	0	18	45
NPCC	218	2	35	717
RF	1,713	5,384	2,890	3,849
SERC	2,757	1,218	2,244	6,772
SPP	374	724	240	833
TRE	229	0	44	165
WECC	297	880	47	1,121
Totals	5,670	8,295	5,533	14,041

*see Table 8 for a list of assets considered within the category of "Other"

Table 8: Examples of Asset Types Considered as "Other"		
Adapter (to convert serial data streams to/from attached devices into TCP/IP traffic)	Industrial Process Control System	Physical security measures
Badge reader controllers	Infrastructure for managing real-time data and events	Remote access applications for keyboard, mouse, video
Communications media	Intrusion Detection and Protection System (IDP)	Remote power controller for server rack
Data Communications Device	Intrusion Detection System (IDS)	Remote Terminal Unit (RTU)
Data mover for storage network	Intrusion Prevention System (IPS)	Scanner (for assessing security of internal networks, devices, & applications)
Database application	Legacy EMS application	Storage Area Network (SAN) switch
Default and shared accounts	Management interface for blade unit	TrueTime clock
Electronic Access Control System	Management interface for Enterprise Service Bus	Uninterruptible Power Supply (UPS)
Environmental monitoring systems and devices	Network appliance to improve traffic performance and extend appliance utilization	Video streaming devices
Ethernet switches	Network attached storage appliance	Video Wall Controller
Firewalls in high availability (HA) configuration acting as virtual firewall	Network copper and fiber optic cables between PSPs.	Virtual network appliance
Hardware administrative interface for blade chassis	Phasor Data Concentrator (PDC)	

c. Numbers of Approved TFEs still in effect as of the 2014 Annual Report

As of the date of the 2014 Annual Report, there are 959 TFEs that remain in effect.

Table 9 provides a breakdown of these TFEs by requirement and Region.

U.S. Entities only	Table 9: TFEs - Active								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	2	0	8	0	2	0	3	15
005 R3.1	0	0	0	3	0	0	0	2	5
005 R3.2	0	1	0	0	1	3	1	2	8
006 R1.1	1	1	0	0	1	0	0	1	4
007 R2.3	5	9	1	25	4	11	12	9	76
007 R3	2	10	1	14	3	4	1	4	39
007 R4	9	36	25	71	46	38	33	97	355
007 R5.3	4	18	0	47	13	19	15	12	128
007 R5.3.1	0	1	0	2	12	1	1	7	24
007 R5.3.2	4	8	7	30	26	22	13	9	119
007 R5.3.3	3	4	1	17	7	11	4	11	58
007 R6	3	7	4	26	12	14	9	24	99
007 R6.3	4	2	2	3	5	1	1	11	29
Totals	35	99	41	246	130	126	90	192	959

d. Number of TFEs that Expired or Terminated During the Reporting Period

Table 10 provides the numbers of TFEs that expired or terminated during the 2014 reporting period. During the 2014 reporting period, no TFEs were terminated due to a material misrepresentation by the Responsible Entity as to the facts relied upon by the Regional Entity in approving the TFE.

U.S. Entities only	Table 10: TFEs that Expired or Terminated during Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	0	0	0	0	0	0	0
005 R3.1	0	0	0	0	0	0	0	0	0
005 R3.2	0	0	2	0	1	0	0	0	3
006 R1.1	0	0	0	2	0	0	0	0	2
007 R2.3	0	0	0	0	3	0	0	0	3
007 R3	0	0	3	1	0	0	1	0	5
007 R4	0	0	16	1	17	1	1	0	36
007 R5.3	0	0	8	1	9	0	0	0	18
007 R5.3.1	0	0	0	0	2	0	0	0	2
007 R5.3.2	0	0	3	0	14	1	0	0	18
007 R5.3.3	0	0	1	0	6	0	0	0	7
007 R6	0	0	5	0	10	0	0	0	15
007 R6.3	0	0	1	0	6	0	0	0	7
Totals	0	0	39	5	68	2	2	0	116
005 R2.6	2	2	22	10	24	3	5	4	72
Overall	2	2	61	15	92	5	7	4	188

e. Number of Approved TFEs Scheduled to Reach their Expiration Dates during the Ensuing Year

Table 11 provides the numbers of approved TFEs scheduled to reach their Expiration Dates during the ensuing year.

U.S. Entities only	Table 11: TFEs Scheduled to Expire or Terminate in the next Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	0	0	0	0	0	0	0
005 R3.1	0	0	0	0	0	0	0	0	0
005 R3.2	0	0	2	0	1	0	0	0	3
006 R1.1	0	0	0	2	0	0	0	0	2
007 R2.3	0	0	0	0	3	0	0	0	3
007 R3	0	0	3	1	0	0	1	0	5
007 R4	0	0	16	1	17	1	1	0	36
007 R5.3	0	0	8	1	9	0	0	0	18
007 R5.3.1	0	0	0	0	2	0	0	0	2
007 R5.3.2	0	0	3	0	14	1	0	0	18
007 R5.3.3	0	0	1	0	6	0	0	0	7
007 R6	0	0	5	0	10	0	0	0	15
007 R6.3	0	0	1	0	6	0	0	0	7
Totals	0	0	39	5	68	2	2	0	116

2. *Categorization of the submitted and approved TFE Requests to date by broad categories such as the general nature of the TFE Request, the Applicable Requirements covered by submitted and approved TFE Requests, and the types of Covered Assets that are the subject of submitted and approved TFE Requests.*

NERC and the Regional Entities categorize submitted and approved TFEs by Applicable Requirement and type of Covered Asset. The types of Covered Assets for which the ERO has approved TFEs has remained generally consistent since the program's inception. Tables 7a, 7b, and 8, above, provide details about the types of Covered Assets that are the subject of submitted and approved TFE requests. Further, Tables 1-4 identify the Applicable Requirements for which the ERO has approved or disapproved TFEs.

3. *Categorization of the circumstances or justifications on which the approved TFEs to date were submitted and approved, by broad categories such as the need to avoid replacing existing equipment with significant remaining useful lives, unavailability of suitable equipment to achieve Strict Compliance in a timely manner, or conflicts with other statutes and regulations applicable to the Responsible Entity.*

The categories of circumstances or justifications on which TFEs to date were submitted and approved have not changed since the inception of the TFE program. They include:

- Not technically possible
- Operationally infeasible

- Precluded by technical limitations
- Adverse effect on bulk electric system reliability
- Cannot achieve by compliance date
- Excessive cost that exceeds reliability benefit
- Conflicts with other statutory or regulatory requirement
- Unacceptable safety risks

4. *Categorization of the compensating measures and mitigating measures implemented and maintained by Responsible Entities pursuant to approved TFEs, by broad categories of compensating measures and mitigating measures and by types of Covered Assets.*

As described in previous annual reports, Regional Entities find that Responsible Entities are employing multiple strategies to protect Covered Assets that are unable to meet applicable Reliability Standards. Typically, Responsible Entities apply more than one strategy to mitigate the risk posed by a TFE. The principal strategies employed include protecting devices with physical and logical security controls. A significant portion of compensating and mitigating measures involve firewalls, the use of Intrusion Detection and Intrusion Prevention systems, and strong access policies.

The compensating and mitigating measures used most often is an Electronic Security Perimeter ("ESP"). Other significant compensating and mitigating measures deployed include Physical Security Perimeter ("PSP"), Authentication, Intrusion Detection and Prevention ("IDS/IPS"), and System Status Monitoring. Table 13 provides information on the common compensating and mitigating measures reported by the Regional Entities. As described below, the use of these compensating and mitigating measures has resulted in adequate protection for the bulk electric system.

Table 12: Compensating & Mitigating Measures	
Electronic Security Perimeter (ESP)	Covered Assets asserted in the TFE are protected as they reside within a defined ESP and access to/from these assets is controlled via defined access points.
Physical Security Perimeter (PSP)	Covered Assets asserted in the TFE are protected as they reside within a defined PSP and access to these assets is controlled via defined access points.
Status Monitoring	Covered Assets are protected by implementation of System Status Monitoring of all cyber assets residing within a defined ESP. Detection and alerting of system state and condition provides early warning and proactive troubleshooting and corrective action.
Enhanced Authentication	Access to Covered Assets asserted in the TFE and all cyber assets that reside within a defined ESP are protected by multi-factor authentication services (*e.g.* , SecurID, Biometrics).
Intrusion Detection and/Prevention Systems	Covered Assets asserted in the TFE are protected by network or host based IDS/IPS services. Anomalous data traffic is detected and alerted on and/or prevented from affected Covered Assets.
Training	Covered Assets are protected by general cyber security training and awareness related to CIP-004 or augmented training is provided due to the lack of strict compliance.
Host-Based Malware Prevention	When Covered Assets asserted in a TFE cannot implement anti-virus or anti-malware tools, they are protected by all other cyber assets within a defined ESP having these security controls installed and managed. Propagation of viruses (*e.g.* , Trojans) to Critical Cyber Assets (CCAs) is a low risk.
Physical Monitoring	When other mandatory controls cannot be implemented, Covered Assets and/or access to them are physically monitored by Responsible Entity staff.
Data Encryption	When other mandatory controls cannot be implemented, data is encrypted between cyber assets to protect data confidentiality.

5. *For each TFE Request that was rejected or disapproved, and for each TFE that was terminated, but for which, due to exceptional circumstances as determined by the Regional Entity, the Effective Date was later than the latest date specified in Section 5.1.5, 5.2.6, or 9.3, as applicable, a statement of the number of days the Responsible Entity was not subject to imposition of findings of violations of the Applicable Requirement or imposition of penalties or sanctions pursuant to Section 5.3.*

All eight Regional Entities reported that during the 2014 reporting period there were no instances of rejection, disapproval, or termination of TFE requests where the effective date was extended past the latest date specified in Section 5.1.5, 5.2.6, or 9.3, as applicable.

6. *A discussion, on an aggregated basis, of Compliance Audit results and findings concerning the implementation and maintenance of compensating measures and mitigating measures, and the implementation of steps and the conduct of research and analyses to achieve Strict*

Compliance with the Applicable Requirements, by Responsible Entities in accordance with approved TFEs.

The TFE Procedure, in conjunction with the Compliance Monitoring and Enforcement Program ("CMEP"), is the framework that Regional Entities use to review and audit TFE requests. During a compliance audit, a Responsible Entity that has a TFE for a particular requirement is *not* evaluated against the applicable Reliability Standard for which a TFE was accepted and approved. Instead, the Responsible Entity is evaluated against the alternative compliance obligations assumed by the Responsible Entity (*i.e.*, compensating and mitigating measures).

All eight Regional Entities have conducted Compliance Audits where approved or terminated TFEs were in scope. Typically, an audit of a Registered Entity with TFEs will be managed according to the TFEs that need to be reviewed; i.e., based on factors such as quantity, locations, etc. Reviews include interviewing subject matter experts specifically about TFEs, sampling evidence pertaining to a TFE's mitigating and compensating measures, etc. As was indicated in previous annual reports, Regional Entities continue to report that Responsible Entities are managing and maintaining their TFEs within the procedural requirements of Appendix 4D. Regional Entities have also issued audit findings that identify TFEs to be processed consistent with the CMEP.

7. *Assessments, by Regional Entity (and for more discrete areas within a Regional Entity, if appropriate) and in the aggregate for the United States and for the jurisdictions of other Applicable Governmental Authorities, of the wide-area impacts on the reliability of the Bulk Electric System of approved TFEs in the aggregate, including the compensating measures and mitigating measures that have been implemented.*

The Regional Entity representatives who are designated "TFE Managers" continue to hold regular meetings to discuss various topics, including those pertaining to issues related to the impact of TFEs. The consensus from those discussions is that there have been no negative wide-area

impacts on the reliability of the bulk electric system as a result of any TFEs. Any wide-area impact of approved TFEs on the reliability of the bulk electric system, in the aggregate, remains negligible.

The Regional Entities have reported similar experiences with the execution and management of the TFE process and the manner in which it impacted the reliability of the bulk electric system. Regional Entities reported that a large majority of Responsible Entities have implemented multiple compensating and mitigating measures for Covered Assets, and, in general, the mitigating and compensating measures of approved TFEs that were implemented in lieu of strict compliance with applicable CIP Reliability Standards accomplished the stated alternate compliance objective. As a result, the level of security for the bulk electric system achieved through the TFE process is comparable to strict compliance with the applicable Reliability Standards.

8. *Discussion of efforts to eliminate future reliance on TFEs.*

Regional Entities reported that they are undertaking a number of efforts to eliminate future reliance on TFEs, including:

- Upgrading or replacing Covered Assets that will enable implementation of security controls defined in CIP Standards and Requirements.
- Removing Critical Cyber Assets that are covered by approved TFEs that reside within defined ESPs.
- Retiring legacy systems that are now subject to coverage by an approved TFE.
- Implementing previously unused or unidentified functionality on Covered Assets that will achieve Strict Compliance with the Applicable Requirement

Where applicable, upgrades of Covered Assets will result in strict compliance without having to rely on TFEs.

In addition, efforts to better train personnel on the requirements of applicable Reliability Standards and coordination with Regional Entity compliance monitoring and enforcement staff

regarding the need for TFEs have led to the continuing decline of devices that rely on a TFE for compliance. Moreover, non-essential devices are also being evaluated for continued inclusion within a defined ESP. Where a device does not need to reside within the ESP for operational necessity, Covered Assets have been relocated outside of the ESP, eliminating the need for a TFE and reducing residual risk to devices remaining within the ESP.

The Regional Entities have observed that the primary barrier to the elimination of TFEs continues to be the inherent design of much BES equipment, particularly legacy equipment that is unable to satisfy various requirements of the CIP Standards. The anticipated implementation of the Version 5 CIP Reliability Standards will provide additional compliance options, but the need for TFEs will remain. Regional Entities have noted the difficulty in providing flexibility for future technology and security changes when developing a standard, thereby making it difficult to eliminate the TFE.

Additionally, the Regional Entities support requirements in the standards to use products that have been independently certified as offering adequate and appropriate security measures. Applying enhanced security features often requires that properly operating equipment be replaced with a more modern, secure models. Therefore, in order to eliminate the need for a TFE, replacement costs may become a barrier to implementing enhanced security features. Without a concerted and coordinated effort from industry, manufacturers will continue with the status quo.

9. *Data and information regarding Material Change Reports, including the number of Material Change Reports filed annually and information regarding the types of circumstances or events that led to Material Changes, as well as any additional information NERC believes would be useful.*

As Responsible Entities update their systems, replace equipment, and add assets to inventory, requests to modify existing TFEs have become more common. The update to the TFE procedure in Appendix 4D streamlined that process, moving from a formal approval process to the

submission of a "Material Change Report" ("MCR"). An MCR does not require approval by the respective Regional Entity, but information from an MCR is available to the Regional Entity and is helpful for subsequent compliance activities (e.g., audits, spot checks, self-certifications, etc.).

The revision to Appendix 4D was approved during the period covered by this report and Regional Entities are in the process of implementing the MCR process, which requires updating the compliance portals. Regional Entities and Responsible Entities use the portals to submit TFE data, and are being modified to support the submission of MCRs. From a reporting perspective, the ERO views TFEs that have were amended prior to the Appendix 4D revisions or changed via an MCR as the same, and for the purposes of the data in the 2014 Annual Report, the terms are synonymous. Table 13 provides the number of active TFE that were amended/changed during the 2014 reporting period.[13]

U.S. Entities only	Table 13: TFE Amendments & Changes during the Report Period								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	2	0	3	0	2	0	1	8
005 R3.1	0	0	0	4	0	0	0	0	4
005 R3.2	0	1	0	1	1	2	0	1	6
006 R1.1	1	1	0	0	1	0	0	0	3
007 R2.3	5	5	1	10	4	3	10	3	41
007 R3	2	4	0	12	3	0	0	2	23
007 R4	13	23	24	58	56	11	20	24	229
007 R5.3	5	11	0	30	19	5	8	6	84
007 R5.3.1	0	1	0	5	14	1	0	5	26
007 R5.3.2	5	7	7	46	30	6	8	3	112
007 R5.3.3	4	4	1	19	8	5	2	7	50
007 R6	4	4	3	14	15	5	6	5	56
007 R6.3	4	2	2	4	5	1	0	3	21
Totals	43	65	38	206	156	41	54	60	663

Table 14 provides additional data about active TFEs that were amended or changed during the reporting period. As indicated by that data, over two-thirds of the changes and amendments pertain to asset count changes and administrative updates.

[13] Approximately 1/3 of amendments/changes reported during the 2014 reporting period were submitted via MCRs.

Table 14: Request Categories – Amendments & Changes	
Category of Request	**Percentage**
Updates to asset data (added quantities, modify types, manufacturer, etc.)	**59%**
Updated security measures (procedural changes, implement new equipment, response to audit findings, etc.)	**22%**
Administrative (update point of contact information, correct typographical errors, termination date change, etc.)	**12%**
Other	**6%**

10. *Additional information about TFEs and their expiration dates, including the number of TFEs by expiration year and CIP Standard requirement, the percentage of currently approved TFEs without expiration dates, and the number of new TFEs approved without expiration dates annually.*

In the September 2013 Order, the Commission directed NERC to provide additional information in the annual reports related to TFEs with and without expiration dates. As has been the case in previous annual reports, the majority of TFEs (approximately 82%) do not have expiration dates. As shown in Table 15, below, of the 959 active TFEs, 787 TFEs do not have an expiration dates. TFEs are approved without expiration dates where the system, device, or technology in question is fundamentally unable to satisfy the corresponding CIP requirement, and there is no indication that such a capability is likely in the foreseeable future. In most cases, these open ended TFEs are considered to be the best approach for managing the applicable devices because of uncertainty about if or when compliant equipment will become available. Of the 172 TFEs with expiration dates, 116 are scheduled to expire in the ensuing year (see Table 11).

U.S. Entities only	Table 15: Active TFEs, Amended & Approved, with no Expiration Date (2014)								
	FRCC	MRO	NPCC	RF	SERC	SPP	TRE	WECC	Total
005 R2.4	0	0	0	3	0	2	0	3	8
005 R3.1	0	0	0	4	0	0	0	2	6
005 R3.2	0	0	0	1	1	3	1	2	8
006 R1.1	1	0	0	0	1	0	0	1	3
007 R2.3	5	0	1	10	4	11	12	9	52
007 R3	0	1	1	11	3	0	1	1	18
007 R4	8	1	25	57	46	39	33	97	306
007 R5.3	4	0	0	30	13	18	15	12	92
007 R5.3.1	0	0	0	4	12	1	1	6	24
007 R5.3.2	5	0	7	45	26	15	13	8	119
007 R5.3.3	3	0	1	16	7	7	4	10	48
007 R6	2	0	4	13	12	14	8	23	76
007 R6.3	3	0	2	4	5	1	1	11	27
Totals	31	2	41	198	130	111	89	185	787

b. Consistency in Review, Approval and Disapproval of TFE Requests

Appendix 4D requires that NERC and the Regional Entities collaborate to assure "consistency in the review, approval and disapproval of TFE Requests…."[14] Also, as noted above, Section 11.2.4 of the NERC Rules of Procedure requires that NERC submit with each Annual Report certain information concerning the manner in which Regional Entities have made determinations to approve or disapprove TFE requests.

NERC has received no reports of inconsistency either in assessing the accuracy or validity of TFEs submitted by Responsible Entities, or in the decisions approving or rejecting TFEs. NERC and the Regional Entities review TFE requests for consistency. Primary and alternate representatives from each Regional Entity, facilitated by NERC staff, meet regularly to discuss common issues. Those representatives also led the efforts at their respective Regional Entities for receiving, reviewing, and reporting TFE-related data.

[14] Section 11 of Appendix 4D of the NERC Rules of Procedure.

In addition to regularly scheduled conference calls and face-to-face meetings, the TFE Managers communicate regularly by email and in person at workshops and regular meetings with the goal of reaching consistency among the Regional Entities on the pertinent issues.

IV. CONCLUSION

For the foregoing reasons, NERC respectfully requests that the Commission accept the 2014 Annual Report as compliant with the directives contained in Order No. 706, the September 2013 Order, and Appendix 4D of NERC's Rules of Procedure.

Respectfully submitted,

/s/ Shamai Elstein

Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G St., N.W., Suite 600
Washington, DC 20005
202-400-3000
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Attorney for North American Electric Reliability Corporation

September 30, 2014

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 30th day of September, 2014.

/s/ Shamai Elstein
Shamai Elstein

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Monitoring System Conditions - Transmission Operations Reliability Standard	**Docket No. RM13-12-000**
Transmission Operations Reliability Standards	**Docket No. RM13-14-000**
Interconnection Reliability Operations and Coordination Reliability Standards	**Docket No. RM13-15-000**

QUARTERLY STATUS REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, THIRD QUARTER 2014

On December 20, 2013, the North American Electric Reliability Corporation ("NERC") filed a motion requesting that the Commission defer action, until January 31, 2015, to allow NERC time to consider the reliability concerns raised by the Commission in the November 21, 2013, Notice of Proposed Rulemaking ("NOPR") in connection with the revisions to the Transmission Operations ("TOP") and Interconnection Reliability Operations and Coordination ("IRO") Reliability Standards in the above-referenced dockets.[1] NERC committed to providing the Commission with quarterly reports regarding the status of revisions, and the instant filing is submitted consistent with that commitment. On January 14, 2014, the Commission granted NERC's motion to defer action until January 31, 2015.[2] On April 1, 2014, NERC filed a quarterly status report regarding standard development activities in the first quarter of 2014 and on July 1, 2014 NERC filed a quarterly status report for the second quarter of 2014. The following quarterly report addresses standard development activities in the third quarter of 2014, (*i.e.*, July 1, 2014 – September 30, 2014).

---

[1] *Monitoring System Conditions - Transmission Operations Reliability Standard, Transmission Operations Reliability Standards, Interconnection Reliability Operations and Coordination Reliability Standards*, Notice of Proposed Rulemaking, 145 FERC ¶ 61,158 (2013).

[2] *Monitoring System Conditions - Transmission Operations Reliability Standard, Transmission Operations Reliability Standards, Interconnection Reliability Operations and Coordination Reliability Standards*, Order on Motion to Defer Action on Notice of Proposed Rulemaking, 146 FERC ¶ 61,023 (2014).

I. Notices and Communication

Notices and communications with respect to this filing may be addressed to the following:[3]

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
(404) 446-2560
(404) 446-2595– facsimile

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

II. Status of Revisions – Project 2014-03

A. First Quarter 2014, January 1 – March 31, 2014

A Standards Authorization Request ("SAR") was submitted on February 12, 2014 to address the concerns identified by the Commission in the NOPR. A standard drafting team was appointed by the NERC Standards Committee on February 12, 2014. This project has been designated as 2014-03.[4]

Two technical conferences were held by NERC in March to facilitate discussion of the issues identified by the Commission in the NOPR.[5] An informal comment period was held from March 11, 2014 through March 24, 2014 to allow for industry comments on the topics discussed during the conferences, or suggestions for further consideration of issues identified in the NOPR.

---

[3] Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[4] The project page is *available here*: http://www.nerc.com/pa/Stand/Pages/Project-2014-03-Revisions-to-TOP-and-IRO-Standards.aspx.

[5] The slides from the conferences are *available here*: http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/top_iro_technical_conference_presentation_20140306.pdf.

These comments are posted on the project webpage as part of the development record and have been considered by the standard drafting team for Project 2014-03.[6]

B. Second Quarter 2014, April 1, 2014 – June 30, 2014

A standard drafting team meeting was held from April 8-10, 2014,[7] followed by a meeting from April 22-24, 2014.[8] Revisions to the IRO and TOP Reliability Standards were posted for a 45-day formal comment period from June 23, 2014 through July 2, 2014. Revisions to the defined terms "Operational Planning Analysis" and "Real-time Assessment" were also proposed and posted for comment. Initial ballots of the standards, definitions, and proposed implementation plan were conducted during the last ten days of the comment period, with the following results:

Reliability Standard	Approval
TOP-001-3 – Transmission Operations	30.99%
TOP-002-4 - Operations Planning	62.18%
TOP-003-3 – Operational Reliability Data	63.07%
IRO-001-4 – Reliability Coordination – Responsibilities	68.57%
IRO-002-4 – Reliability Coordination	36.94%
IRO-008-2—Reliability Coordinator Operational Analyses and Real-time Assessments	47.87%
IRO-010-2—Reliability Coordinator Data Specification and Collection	60.26%
IRO-014-3—Coordination Among Reliability Coordinators	61.67%
IRO-017-1 – Outage Coordination	57.94%

The definitions received an approval of 62.64% and the implementation plan received an approval of 64.70%.

---

[6] *Available here*: http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/Comments%20Received%20-%20Tech%20Conferences%20TOP_IRO%20Mar%202014.pdf.

[7] This information is publicly posted on the NERC calendar, *available here*: http://www.nerc.net/meetings/details.asp?id=3979.

[8] This information is publicly posted on the NERC calendar, *available here*: http://www.nerc.net/meetings/details.asp?id=3992.

The Project 2014-03 standard drafting team has written a whitepaper on System Operating Limits ("SOLs") in order to clarify how to establish SOLs and mitigate an exceedance of an SOL.[9] In addition, consistent with the NOPR, the team has reviewed the recommendations of the 2011 Southwest Outage Blackout Report[10] and has addressed how the proposed Reliability Standards fulfill many of these recommendations.[11]

C. Third Quarter 2014, July 1, 2014 – September 30, 2014

A drafting team meeting was held on July 22, 2014 – July 24, 2014. A technical conference was held on August 12, 2014 in order to discuss proposed revisions to the standards. Revisions to the TOP and IRO Reliability Standards were posted for a 45-day formal comment period from August 6, 2014 – September 19, 2014. Revisions to the defined terms "Operational Planning Analysis" and "Real-time Assessment," as well as the implementation plan for these new and revised standards and definitions, were also proposed and posted for comment. Additional ballots of the standards, definitions, and proposed implementation plan were conducted during the last ten days of the comment period, with the following results:

---

9 *Available here*: http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/2014_03_first_posting_white_paper_sol_exceedance_20140509.pdf.

10 *Available here*: https://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

11 *Available here*: http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/2014_03_first_posting_sw_outage_recommendations_201405012.pdf. In addition, the standard drafting team has also considered issues raised in the NOPR, in the following document, *available here*: http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/2014_03_first_posting_nopr_issues_20140509.pdf.

Reliability Standard	Approval
TOP-001-3 – Transmission Operations	48.73%
TOP-002-4 - Operations Planning	78.87%
TOP-003-3 – Operational Reliability Data	87.03%
IRO-001-4 – Reliability Coordination – Responsibilities	76.12%
IRO-002-4 – Reliability Coordination	74.23%
IRO-008-2—Reliability Coordinator Operational Analyses and Real-time Assessments	75.67%
IRO-010-2—Reliability Coordinator Data Specification and Collection	85.49%
IRO-014-3—Coordination Among Reliability Coordinators	75.96%
IRO-017-1 – Outage Coordination	78.67%

The definitions received an approval of 93.34% and the implementation plan received an approval of 90.13%. A drafting team meeting is scheduled for September 30 – October 2, 2014. The Project 2014-03 standard drafting team and NERC Staff are diligently working to revise the IRO and TOP Reliability Standards.

III. Conclusion

The North American Electric Reliability Corporation respectfully requests that the Commission accept this quarterly report for informational purposes.

Respectfully submitted,

/s/ Stacey Tyrewala

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

Counsel for the North American Electric Reliability Corporation

Dated: October 1, 2014

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF THE BYLAWS AND RELIABILITY STANDARDS DEVELOPMENT PROCEDURES OF THE WESTERN ELECTRICITY COORDINATING COUNCIL

Pursuant to §215(e)(4) of the Federal Power Act[1] ("FPA") and 18 C.F.R. §§39.8, 39.10, the North American Electric Reliability Corporation ("NERC") requests the Commission's approval of amendments to the Delegation Agreement of the Western Electricity Coordinating Council ("WECC Delegation Agreement") consisting of amendments to the WECC Bylaws in Exhibit B and the WECC Reliability Standards Development Procedures ("WECC RSDP") in Exhibit C.[2] By approving the proposed amendments to the WECC RSDP included in this filing, the Commission will also be approving the amendments for purposes of the WECC Delegation Agreement. The Bylaws and RSDP are "Regional Entity Rules" as defined in 18 C.F.R. §39.1; thus, in accordance with 18 C.F.R. §39.10, amendments to the Bylaws and the WECC RSDP require Commission approval.

As described in greater detail in Section II of this Petition, the principal purpose of the amendments to the WECC RSDP is to revise the process to gain efficiencies based on WECC's

---

1 16 U.S.C. §824o (2012).

2 The complete currently effective WECC Delegation Agreement is available at: http://www.nerc.com/FilingsOrders/us/Regional%20Delegation%20Agreements%20DL/WECC_RDA_Effective_20140212_executed.pdf.

experience to date. The changes include: (1) revising and expand existing definitions; (2) separating the RSDP into separate sections for the "Normal Process" for development and an "Expedited Action"; (3) updating the timeline in Exhibit C: Common Attributes; and (4) adjusting the table of contents to correlate with the other changes. The proposed revisions also implement various updates, corrections, and typographical and format changes. The revisions to the WECC Bylaws, found in Section III, were made in order to align the WECC Bylaws with the NERC Rules of Procedure ("NERC ROP") with respect to the definition of the term "Regional Criteria," and to set forth a process for the WECC Board of Directors to schedule and conduct reviews of the structure and governance of WECC after the first full year of operation following internal bifurcation. The changes to the Bylaws also remove from the Bylaws provisions related to standard development that are contained in the WECC RSDP and consolidate the remaining provisions related to standard development into one Section 8.7 in the Bylaws.

NERC has included a clean and redline version of the WECC RSDP as Attachments 1 and 2, respectively. A clean and redline version of the WECC Bylaws are found in Attachments 3 and 4, respectively. Finally, a clean and redline version of the WECC Common Attributes in Exhibit C of the WECC Delegation Agreement are found in Attachments 5 and 6, respectively. There are no proposed changes to the WECC Delegation Agreement other than the proposed changes to the WECC Bylaws, Exhibit C, and the WECC RSDP.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following[3]:

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
William H. Edwards*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation 3353 Peachtree Road
Suite 600, North
Tower Atlanta,
GA 30326
(404) 446-2560
(404) 467-0474 – facsimile

Steve Rueckert*
Director of Standards
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, Utah 84103-1114
(801) 883-6878
steve@wecc.biz

[3] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2014), to allow the inclusion of more than two persons on the service list in this proceeding.

II. PROPOSED WECC RSDP

The currently effective version of the WECC Delegation Agreement was approved by FERC and became effective on December 6, 2013. The proposed amendments revise the WECC RSDP and Exhibit C of the WECC Delegation Agreement to revise the process to gain efficiencies based on WECC's experience to date, including: (1) to revise and expand existing definitions; (2) to separate the WECC RSDP into separate sections for the "Normal Process" for development and an "Expedited Action"; (3) to update the timeline in Exhibit C: Common Attributes; and, (4) to adjust the table of contents to correlate with the other changes. The proposed revisions also implement various updates, corrections, and typographical and format changes. The discussion in the following subsections describes the proposed amendments to the WECC RSDP.

A. Introduction

The introductory paragraph with itemized steps for the process of introducing and solemnizing new Reliability Standards is removed and replaced with a description of WECC and an explanation of the RSDP. The definition of "WECC Standards Committee" is removed and relocated in the "Definitions" section. Other changes are made to improve the text or correct grammatical inconsistencies.

B. Definitions

A new term, "Ballot Pool," is added and defined as "[t]hat pool of Ballot Body entities that have registered to vote on a specific document."

A new term, "Day," is added and defined as:

> All references to days are calendar days. When counting the number

> of days, the count shall exclude the first day of the time window to be measured. If a terminus date falls on a weekend or a day that WECC is scheduled to be closed, the new terminus date shall be the day following the weekend or WECC closure day. For example, if a 15-day period ends on a holiday the terminus date is on the following WECC business day.

A new term, "Drafting Team (DT)," is added and defined as:

> A team of pertinent subject matter experts (SME) that was appointed by the WECC Standards Committee (WSC) to develop the document(s) that were called for in a Standard Authorization Request (SAR) consider and respond to industry comments, participate in forums to help build consensus on draft documents, and perform other tasks as assigned by the WSC.

A new term, "Electric Line of Business," is added and defined as "[t]he generation, transmission, distribution, or trading of electricity or the provision of related energy services in the Western Interconnection."

A new term, "NERC Compliance Registry," is added and defined as "[r]egistry of the Bulk Electric System owners, operators, and users that are subject to approved reliability standards."

A new term, "Non-Substantive Changes," is added and defined as:

> A Non-Substantive Change is one that does not change the scope, applicability, intent of the document, or the actions required by affected entities. For example, Non-Substantive Changes include, but are not limited to: correcting grammar or sentence structure, typographical or spelling errors, font and formatting, numbering, references, adding an obviously missing word, or rephrasing a statement to improve its clarity. Non-Substantive Changes do not require, but may receive posting for comments and/or revision of the document under these Procedures.

A new term, "Other Projects (OP)," is added and defined as "[a]ny document type other than an RRS developed under these Procedures. These include, but are not limited to, WECC Criteria."

A new term, "Participating Stakeholder," is added and defined as "[a]ny person or entity that is not a WECC Member, but who has applied for and been granted participating stakeholder rights as defined and currently set forth in the WECC Bylaws."

A new term, "Regional Reliability Standard (RRS)," is added and defined as:

> A requirement approved by FERC under Section 215 of the Federal Power Act, to provide for reliable operation of the Bulk Electric System in the United States. Regional Reliability Standards are specific to the Western Interconnection and shall be established using these Procedures. When approved by FERC and applicable authorities in Canada and Mexico, Regional Reliability Standards shall be made part of the body of NERC Reliability Standards and shall be enforced upon all applicable Bulk-Electric System owners, operators, and users within the WECC area, regardless of membership in the region.

A new term, "Standard Authorization Request (SAR)," is added and defined as "[t]he WECC Standard Authorization Request ("SAR") administered by the WECC Standards Department for the purpose of requesting development, revision, retirement, or interpretation of an RRS or OP."

A new term, "Standards Briefing," is added and defined as "[a]ny meeting initiated by WECC for the purpose of creating an open forum for discussion and explanation of an RRS or OP, generally but not exclusively held during the development process of those documents in advance of a ballot window."

A new term, "Standards Email List (SEL)," is added and defined as "[e]mail list(s) established and maintained by WECC for the purpose of communicating due process activity; generally, but not exclusively, for standards-related activities."

A new term, "Substantive Changes," is added and defined as "[a] Substantive Change is one that changes the scope, applicability, intent of the document, or the actions required by

affected entities. For example, Substantive Changes include but are not limited to: changes to the functional entities listed in the applicability section of the RRS or OP, changes to the effective date, adding, deleting or revising requirements, measures or explanatory narrative. Substantive Changes to an RRS or an OP require at least one posting/comment/response cycle."

A new term, "WECC Member," is added and defined as "[a]ny entity that has applied and been accepted for membership in WECC and is current in the payment of dues."

A new term, "WECC Standards Committee (WSC)," is added and defined as "Committee established by the WECC Board of Directors (Board) for the purpose of overseeing the implementation of these Procedures pursuant to its Board-approved charter."

C. Overview

The "Overview" divides the document into two sections for the development steps: one section details the "Normal Process" for Regional Reliability Standards, and the other, titled "Supporting Processes," addresses exceptions to the normal process such as an "Expedited Process for Urgent Action" and "Regulatory Directives" as well as "Maintenance of the Procedures" and "Maintenance of RRS and OPs Documents." A table of contents for Steps 1 through 14 is added to provide reference to each development step of the normal Reliability Standards development process.

A new subsection, "Notices," is added to describe the type of notice required to be provided by WECC to both the public and to NERC related to Reliability Standards activities. A subsection titled "WECC Standards Committee (WSC)" is added to define the WSC role in the management of development procedures, and another subsection titled "WECC Standards Voting Sectors" is created to revise definitions for the eight Standards Voting Sectors (SVS) in which an entity may vote and to describe the process for registration and voting on Regional Reliability

Standards.

D. Normal Process for Regional Reliability Standards and Other Projects

Step 1 is renamed from "Request to Revise or Develop a Standard" to "Submit and Validate a Standard Authorization Request," and the substance of the step is revised to reflect the new process.

Step 2 is renamed from "Standard Authorization Request Validation and Submission to the WSC" to "Step 2—Complete SAR and Present to the WSC," and the substance of the step is revised with procedures for receipt of the SAR by WECC, for the WSC to accept or remand the SAR, and for the SAR author to remedy deficiencies found by the WSC.

Step 3 is renamed from "Drafting Team Begins" to "Step 3—Convene the Drafting Team," and the substance of the step is revised to explain the prioritization of the development of the SAR and the procedure for convening a drafting team to develop the RRS or OP required by the SAR.

"Step 4—Begin Drafting Phase and Submit Draft to WSC" is added to provide the process for beginning drafts of the new standard proposed in the SAR and what should be required in the RRS. The existing requirements for the Drafting Team are removed and replaced with a more robust description of the Drafting Team, its roles, its involvement with the new or revised standard, and requirements for the final submission of the RRS.

"Step 5—Post for Comment," is added to explain the procedure for posting the draft of the RRS or OP for comment for a period of no less than 45 days for the first iteration and no less than 30 days for each subsequent iteration. A requirement to create an implementation plan and to provide notice that the comment period has been opened is added to this section, and directions for opening a web portal to serve as the means of receiving comments included. The WSC is directed to monitor the posting and review the posted documents to ensure the development process

remains within the scope of the SAR.

"Step 6—Respond to Comments" is added to explain the process for the DT to consider and organize comments related to the proposed RRS or OP and the resulting changes to them. A requirement is added to ensure the comment posting is done within 30 days after the comment window has closed. Separate requirements are articulated for changes in the RRS or OP that are substantive and for changes that are non-substantive.

"Step 7—Submit Proposed Draft to the WSC with a Request for Ballot" is added to require the DT to present the proposed RRS or OP to the WSC with a request for ballot and to require the WSC to respond no later than its next regularly scheduled meeting. Language is also added to require the WSC to ensure the RRS or OP complies with the SAR and with FERC orders, board directives, or other regulatory directives. Several lines are added to describe the required actions of the WSC if the RRS or OP is ready for ballot or is not ready for ballot, as well as the process for a remanded RRS or OP.

"Step 8—Convene a Standards Briefing" is added to require WECC to conduct a briefing after the RRS or OP is approved by the WSC and to provide notice of that briefing 15 days or more before it occurs.

"Step 9—Form the Ballot Pool and Ballot the Standard," is added to require an individual or entity desiring to participate in the ballot of an RRS or OP to apply to WECC for Ballot Body membership if eligible. Further guidance is added to instruct the formation of the ballot pool from the ballot body and the required notices upon the forming of the pool. A limitation on subsequent additions or withdrawals from the Ballot Pool is added, as well as the ability of the WECC Director of Standards to authorize deviations for the rule under extraordinary circumstances. The specific procedures for voting on an RRS or OP is outlined, including the following: (i) the ability

of Participating Stakeholders to vote on an RRS or OP, (ii) the requirements for casting a "Negative Vote" on an RRS or OP, (iii) the necessary quorum of two-thirds of the Ballot Pool for each vote, (iv) the requirement of a weighted majority of the Ballot Pool to approve the RRS or OP based on a clearly articulated weighting schedule, and (v) the actions available to the WSC after a vote by the Ballot Pool.

"Step 10—Initiate the Appeals Process-If Needed" is added to inform the required processes of bringing an appeal related to either a technical reliability concern or a due process concern. A line is added to ensure that the appeal does not halt development of the standard but that the appeal is settled by the Board before the Board votes for final approval of the RRS or OP.

"Step 11—Obtain Board Approval" is added to require the Board to consider the RRS or OP for approval, taking into account enumerated considerations, no later than the next regularly scheduled meeting after the close of the Ballot Pool window and recommendation for approval by the WSC. Further, lines are added describing actions of the WECC upon approval or rejection and subsequent remediation of the RRS or OP.

"Step 12—Submit RRSs for ERO Review, FERC Approval & Implementation of WECC Regional Reliability Standards" is added to describe the process for submitting a new, revised, or retired RRS to NERC for NERC and FERC approval. A line is added to clarify that the step only applies to RRSs.

"Step 13—Retire an OP" is added to provide the WSC with authority to retire a WECC OP on its own initiative if the subject matter of a NERC Reliability Standard is duplicated and retirement will not cause a reliability gap.

"Step 14—Submit a Request for Interpretation" is added to describe a "Request for Interpretation (RI)" and the process for submitting the RI on the WECC online SAR form. Certain

exceptions to the Procedures are made for processing of the RIs, including the creation of an Interpretation Drafting Team (IDT) to respond to RIs.[4]

E. Supporting Processes

Supporting Processes is added with four subsections as described below.

The first subsection, "Expedited Process for Urgent Action," allows any person or entity to propose an interim RRS or OP for approval in cases requiring urgent action and allows the Board to approve the interim document with an initial effective date. A line is added that requires that the Board take action within 90 days after the initial effective date of the document.

The second subsection, "Regulatory Directives," replaces the existing "Special Procedures for Addressing Regulatory Directives" section. In this subsection, a process is articulated for the Board to determine whether a Directive Regional Reliability Standard (DRRS) meets a federal regulatory directive, and if not, to take action to ensure that the DRRS is responsive to the regulatory directive. Requirements are added to "Regulatory Directives" requiring the Board to take certain steps to meet the regulatory obligations.

The third subsection, "Maintenance of the Procedures," is added to describe the responsibilities of the WSC with regard to maintenance of the procedures in the RSDP, including changes to the procedures and response to comments on any redraft.

The fourth subsection, "Maintenance of RRS and OPs Documents," is added to ensure that each RRS is reviewed periodically for the identification of needed changes if necessary and subsequent communication of the decision regarding changes.

---

[4] In addition to the revisions that are mentioned in this section, Step 14 of the Normal Process for Regional Reliability Standards also includes instruction for the Drafting Team to make a recommendation to the Standing Committee for retirement of certain documents if that document is to be subsumed into the new PSS RRS. WECC has recognized and notified NERC that inclusion of this line is a clerical error. NERC requests that FERC act on the WECC RSDP as filed. NERC will submit WECC's at a later date if the errata is adopted.

The Standards Drafting Procedures Flowchart at the end of the WECC RSDP was removed, as it is inapplicable to the revised Bylaws due to the changes in procedure.

F. Exhibit C—Regional Standard Development Procedure

In Common Attribute 5 of Exhibit C, the WECC Standing Committees are removed from involvement in the Reliability Standards development process. The WECC Standards Committee (WSC) will no longer be assisted by the standing committees regarding the requests for new or revised Reliability Standards.

In Common Attribute 6 of Exhibit C, an exception for Participating Stakeholders who vote for Regional Reliability Standards and Regional Criteria is added by noting that these entities may only vote on Regional Criteria that would result in a sanction to a non-WECC member. Other non-substantive revisions are made to improve the text.

In Common Attribute 7 of Exhibit C, outdated references to standard development steps in the WECC RSDP are updated to reflect changes made to that document.

In Common Attribute 9 of Exhibit C, the amount of time given to the WSC to determine the disposition of a standard request is increased from fourteen days to sixty days.

In Common Attribute 10 of Exhibit C, the amount of time given to the WSC to deliver an explanation for rejection to a requester of a standard is increased from fourteen days to thirty days.

In Common Attribute 14 of Exhibit C, the WSC is removed from the process of preparing a summary of comments received and changes made so that the drafting team has sole responsibility for this job. With regard to the time of posting of the summary, the attribute is edited to require the summary to be posed no later than the next posting of the proposed standard.

In Common Attribute 16, the process for voting on a standard is revised to allow for

voting by the Ballot Pool instead of the WECC lead standing committee and to change the time period for dating from thirty days to fifteen days after the issuance of the notice for vote. The last sentence is removed, thereby deleting the requirement that voting not begin sooner than seven days after the Joint Session of the Standing Committee where the draft was considered.

In Common Attribute 17, the word "business" is deleted so that only 15 days total are required for a vote of the Ballot Pool on a proposed standard.

In Common Attribute 18, the first sentence allowing all Ballot Body members to vote on proposed new Reliability Standards is deleted and a sentence requiring that each standard be considered by a newly formed Ballot Pool of interested members of the registered Ballot Body is added.

In Common Attribute 19, the word "non responses" is deleted and changed to "negative votes cast without explanation" to include votes that are made but that do not offer an explanation for purposes of determining whether a quorum of the Ballot Pool is achieved.

In Common Attribute 34, a bullet point is added for "Violation Severity Levels," to require that this term be defined in the Compliance Monitoring Process.

III. PROPOSED WECC BYLAWS

The proposed WECC Bylaws include a variety of amendments to the currently effective WECC Bylaws, a document found in Exhibit B of the WECC Delegation Agreement. Substantive changes to the Bylaws along with an explanation of the change are enumerated below, according to its section therein. The proposed Bylaws also implement various non-substantive, inconsequential updates, corrections, and typographical and format changes.

A. Definitions

The definition for the term "Ballot Body" is edited to remove reference to the "voting

sectors" described in section 8.6.5.2 and replaced with a reference to the "voting sectors" found in the RSDP. The definition for the term "Ballot Pool" is deleted from the definition section entirely, and the definition for "Regional Criteria" is removed and replaced with a reference to the definition of "Regional Criteria" as set forth in the NERC Rules of Procedure.

B. Members and Membership

Section 4.5 (Affiliates and Distinct Business Entities) provides an alternative route to membership for Affiliates of a Member, given compliance with four subsections. Section 4.5.2, one of those subsections which evinces the requirement for affiliates who are members of the same class, is edited to add a limitation on the ability of a group of affiliates to split their single vote amongst all affiliates or designate a single Affiliate as the group's voting Member. This limitation excludes situations as set forth in Section 8.7.6 of the Bylaws (Procedures for Developing and Voting on Reliability Standards)(described below), including when Affiliates are within a single Standards Voting Sector that may only have one vote and must designate a single Affiliate as the group's Ballot Pool member to vote in that Standards Voting Sector. Because WECC added this explicit exception in section 4.5.2, the requirement that non-WECC members identify their affiliations with other Ballot Body members and that WECC staff limit the voting of these members is removed and placed in Section 8.7.6. .. These changes allow WECC to consolidate the provisions related to Standards development in Section 8.7, including affiliate voting on Reliability Standards.

Under Section 4.9 (WECC Structure and Governance Review), a line is added to provide guidance on the commencement of the initial review of WECC performance required by Section 4.9. Under the new provision, the review will occur after the first year of operation under the July 2013 Bylaws and will be done collaboratively with the Member Advisory Committee (MAC).

C. Member Committees

In the description of the WECC Standards Committee, a reference to "WECC Standards Voting Sectors" as it was described Section 8.6.5.2 is replaced with a reference to the term "WECC Standards Voting Sectors" found in the RSDP.

The subsection titled "Assessment of Standing Committee Activities" is wholly repealed. The assessment envisioned by this section has been replaced by the review of WECC's structure and governance set forth in section 4.9, as mentioned above.

Section 8.5 (formerly titled "Procedures for Committee Decision-Making") is revised and renamed "Procedures for Member Advisory Committee Decision-Making" to avoid confusion and to provide clarity on the type of committee for which the subsection is providing guidance.

Under Section 8.6 (Procedures for Committees other than the Member Advisory Committee), the description of "Committee Membership" in Section 8.6.4 is revised to remove the exception for interested stakeholders to vote on proposed Reliability Standards or revisions to Reliability Standards due to the fact that voting by participating stakeholders is addressed in the WECC RSDP and Section 8.7 of the Bylaws. The description of "WECC Standards Voting Sectors" in Section 8.6.5.2, including all subsections therein, is wholly removed from the WECC Bylaws. WECC also removes a lengthy, unnumbered provision in Section 8.6 called "Voting on Regional Reliability Standards and Regional Criteria." This provision used to provide the procedure for a Ballot Body to cast a vote on a WECC Standards Committee-approved draft of a Regional Reliability Standard or Regional Criteria is removed in its entirety. These provisions were removed from Section 8.6 of the Bylaws because they are addressed in the WECC RSDP.

Under Section 8.7 (Procedures for Developing and Voting on Reliability Standards), the reference to Sections 8.6.5.2 and 8.6.5.4 for procedures and conditions of voting in Section 8.7.2 is deleted because the language in these sections was deleted as explained above. Further, the

explanation of the ability of Participating Stakeholders to vote on a proposed Reliability Standard or revision is deleted because this explanation is contained in the WECC RSDP. The complete process associated with the Board Authority to Address Regulatory Directives is deleted because this process is contained in the WECC RSDP and only a reference to the Board's authority in this regard is retained. Finally, two new sections, 8.7.5 and 8.7.6 are added to define entry into the WECC Standards Voting Sectors and to require WECC Ballot Body members to identify affiliations with other Ballot Body members, respectively. These sections were added to Section 8.7 because they were removed from Sections 8.6.5.2 and 4.5.5, respectively, as part of WECC's effort to consolidate all Reliability Standards related provisions into Section 8.7.

IV. CONCLUSION

The North American Electric Reliability Corporation respectfully requests that the Commission approve the proposed amendments to its Delegation Agreement with Western Electricity Coordinating Council, Inc., shown in Attachment 1, Attachment 3, and Attachment 5 to this Petition, including approving the amendments to the WECC RSDP and Exhibit C as amendments to Regional Entity Rules.

Respectfully submitted,

/s/ William H. Edwards

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
William H. Edwards
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

Counsel for the North American Electric Reliability Corporation

September 15, 2014

Attachment 1

Reliability Standards Development Procedures

Amended Exhibit of the Delegation Agreement Between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council

Clean Version

RELIABILITY STANDARDS DEVELOPMENT PROCEDURES

Introduction

The Western Electricity Coordinating Council (WECC) is a Regional Entity[1] authorized through a delegation agreement between the North American Electricity Reliability Corporation (NERC) and WECC pursuant to Section 215 of the Federal Power Act. NERC delegates designated powers, rights, and responsibilities to WECC regarding the administration within the Western Interconnection of electric Reliability Standards adopted or approved by NERC and the Federal Energy Regulatory Commission (FERC).

These Reliability Standards Development Procedures (Procedures) define the process to be used by WECC for the development, revision, and retirement of Regional Reliability Standards (RRS) and various Other Projects (OP) created under these Procedures.

These Procedures were established to create the structure for open and transparent due process in the development of WECC RRSs and OPs. These Procedures include, but are not limited to, public notice of intent to develop RRSs and OPs, a public comment period on the proposed documents, due consideration of comments provided, and a balanced ballot of interested stakeholders.

The Procedures shall be interpreted and applied in a manner that is consistent with the WECC Bylaws. Should any conflict arise between the Procedures and the WECC Bylaws, the WECC Bylaws will prevail.

Definitions

Ballot Body

That body of qualified WECC Members and non-members that register with WECC for participation in Ballot Pools.

Ballot Pool

That pool of Ballot Body entities that have registered to vote on a specific document.

Day

All references to days are calendar days. When counting the number of days, the count shall exclude the first day of the time window to be measured. If a terminus date falls on a weekend or a day that WECC is scheduled to be closed, the new terminus date shall be the day following the weekend or WECC closure day.

[1] Unless otherwise specified, capitalized terms are defined in the NERC Glossary of Terms Used in Reliability Standards.

For example, if a 15-day period ends on a holiday the terminus date is on the following WECC business day.

Drafting Team (DT)

A team of pertinent subject matter experts (SME) that was appointed by the WECC Standards Committee (WSC) to develop the document(s) that were called for in a Standard Authorization Request (SAR) consider and respond to industry comments, participate in forums to help build consensus on draft documents, and perform other tasks as assigned by the WSC.

Electric Line of Business

The generation, transmission, distribution, or trading of electricity or the provision of related energy services in the Western Interconnection.

NERC Compliance Registry

Registry of the Bulk Electric System owners, operators, and users that are subject to approved reliability standards.

Non-Substantive Changes

A Non-Substantive Change is one that does not change the scope, applicability, intent of the document, or the actions required by affected entities.

For example, Non-Substantive Changes include, but are not limited to; correcting grammar or sentence structure, typographical or spelling errors, font and formatting, numbering, references, adding an obviously missing word, or rephrasing a statement to improve its clarity. Non-Substantive Changes do not require, but may receive posting for comments and/or revision of the document under these Procedures.

Other Projects (OP)

Any document type other than an RRS developed under these Procedures. These include, but are not limited to, WECC Criteria.

Participating Stakeholder

Any person or entity that is not a WECC Member, but who has applied for and been granted participating stakeholder rights as defined and currently set forth in the WECC Bylaws.

Regional Reliability Standard (RRS)

A requirement approved by FERC under Section 215 of the Federal Power Act, to provide for reliable operation of the Bulk Electric System in the United States. Regional Reliability Standards are specific to the Western Interconnection and shall be established using these

Procedures. When approved by FERC and applicable authorities in Canada and Mexico, Regional Reliability Standards shall be made part of the body of NERC Reliability Standards and shall be enforced upon all applicable Bulk-Electric System owners, operators, and users within the WECC area, regardless of membership in the region.

Standard Authorization Request (SAR)

The WECC form titled *Standard Authorization Request (SAR)* administrated by the WECC Standards Department for the purpose of requesting development, revision, retirement, or interpretation of an RRS or OP.

Standards Briefing

Any meeting initiated by WECC for the purpose of creating an open forum for discussion and explanation of an RRS or OP, generally but not exclusively held during the development process of those documents in advance of a ballot window.

Standards Email List (SEL)

Email list(s) established and maintained by WECC for the purpose of communicating due process activity; generally, but not exclusively, for standards-related activities.

Substantive Changes

A Substantive Change is one that changes the scope, applicability, intent of the document, or the actions required by affected entities.

For example, Substantive Changes include but are not limited to:

- changes to the functional entities listed in the applicability section of the RRS or OP;
- changes to the effective date;
- adding, deleting or revising requirements, measures or explanatory narrative.

Substantive Changes to an RRS or an OP require at least one posting / comment / response cycle.

WECC Member

Any entity that has applied and been accepted for membership in WECC and is current in the payment of dues.

WECC Standards Committee (WSC)

Committee established by the WECC Board of Directors (Board) for the purpose of overseeing the implementation of these Procedures pursuant to its Board-approved charter.

Overview

This document has two dominate sections. The first section describes the development steps for the Normal Process for Regional Reliability Standards and Other Projects. The second section augments the first with Supporting Processes to address exceptions such as an expedited process for urgent actions, addressing regulatory directives, and maintenance of certain documents.

Development Steps/Table of Contents

The following development steps are included in the normal process for Regional Reliability Standards and Other Projects section:[2]

Step 1 – Submit and Validate a Standard Authorization Request 7

Step 2 – Complete SAR and Present to the WSC 7

Step 3 – Convene the Drafting Team 8

Step 4 –Begin Drafting Phase and Submit Draft to WSC 9

Step 5 – Post for Comment 10

Step 6 – Respond to Comments 11

Step 7 – Submit Proposed Draft to the WSC with a Request for Ballot 12

Step 8 – Convene a Standards Briefing 12

Step 9 – Form the Ballot Pool and Ballot the Standard 13

Step 10 – Initiate the Appeals process – If Needed 15

Step 11 – Obtain Board Approval 15

Step 12 – Submit RRSs for ERO Review, FERC Approval & Implementation of WECC Regional Reliability Standards

Step 13 – Retire an OP 16

Step 14 – Submit a Request for Interpretation 16

The following related processes are included in the Supporting Processes section:

- Expedited Process for Urgent Action
- Regulatory Directives

[2] This Table of Contents will reflect the final actual pagination after final formatting. This footnote will be deleted from the final document.

- Maintenance of Procedures
- Maintenance of RRSs and OPs Documents

Notices

Notices required under these Procedures shall be distributed electronically via WECC's SEL(s) and deemed delivered when posted on the WECC website, except as noted in the following paragraph. Concurrent running of notice and posting periods is explicitly allowed.

WECC shall provide notice to NERC of all standards-related activities by including NERC on WECC's SEL. Inclusion of a NERC-provided email address on the related SEL shall constitute coordination of notice to NERC of standards-related activities and shall be deemed delivered upon dispatch via the SEL(s).

All WECC Members and Participating Stakeholders will be given an opportunity to receive notices provided via the SEL.

WECC Standards Committee (WSC)

The WSC manages these Procedures. The WSC protects the integrity, credibility and implementation of the Procedures while acting in accordance with the WSC Charter. Delineation of specific WSC duties, WSC composition and governance, WSC voting privileges, and other related practices, shall be in accordance with the WSC charter as approved by the Board.

WECC Standards Voting Sectors

There are eight (8) Standards Voting Sectors (SVS) in which an entity may register to vote. The SVSs are divided into two separate categories: Registered and Non-Registered.

The Registered category is for those entities *registered* on the NERC Compliance Registry and to those Canadian and Mexican entities that perform functions that, if performed in the United States, would allow those entities to be registered for compliance in the NERC Compliance Registry. The Non-Registered category is for all others meeting the qualifications of those defined SVSs. A single entity cannot be in the Registered category and the Non-Registered category at the same time.

SVSs 1 through 5 are "Registered" SVSs.

1) Transmission Sector. This sector consists of Western Interconnection entities registered in the NERC Compliance Registry as Transmission Owners, Transmission Operators, Transmission Service Providers, or Transmission Planners;

2) Generation Sector. This sector consists of Western Interconnection entities registered in the NERC Compliance Registry as Generation Owners or Generation Operators;

3) Marketers and Brokers Sector. This sector consists of Western Interconnection entities registered in the NERC Compliance Registry as Purchasing-Selling Entities.

4) Distribution Sector. This sector consists of Western Interconnection entities registered in the NERC Compliance Registry as Distribution Providers or Load-Serving Entities;

5) System Coordination Sector. This sector consists of Western Interconnection entities registered in the NERC Compliance Registry as Balancing Authorities, Reserve Sharing Groups, Planning Authorities/Coordinators, Resource Planners, Interchange Authorities/Coordinators, or Reliability Coordinators.

SVS 6 through 8 are “Non-Registered” SVSs.

6) End-Use Representative Sector. This sector consists of entities not on the NERC Compliance Registry, but that are WECC Members and are end users of significant amounts of electricity in the Western Interconnection, including; industrial, agricultural, commercial and retail entities as well as organizations in the Western Interconnection that represent the interests of a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public or the environment.

7) State and Provincial Representatives Sector. This sector consists of entities not on the NERC Compliance Registry, but that are WECC Members that are representatives of states and provinces in the Western Interconnection provided that such representatives will have policy or regulatory roles and do not represent state or provincial agencies and departments whose function involves significant direct participation in the market as end users or in Electric Line of Business activities.

8) Other Non-Registered WECC Members and Participating Stakeholders Sector. This sector consists of (1) Participating Stakeholders as defined in the WECC Bylaws, (2) WECC Members not on the NERC Compliance Registry that are Electric Line of Business entities doing business in the Western Interconnection that do not own, control or operate transmission or distribution lines in the Western Interconnection, including power markets, independent power producers, any other entities whose primary business is the provision of energy services, and (3) those entities that are not eligible for membership in any other Standards Voting Sector and who have a substantial interest in the purposes of WECC.

If a single entity qualifies for more than one Registered SVS, that entity may register and vote in each Registered SVS for which it qualifies. For example, if a single entity was registered in the NERC Compliance Registry as a transmission owner and also a generator owner; that single entity could register and vote once in SVS 1 and once in SVS 2.

Non-Registered SVSs 6 through 8 represent those entities that are *not registered* in the NERC Compliance Registry. Unlike Registered SVSs 1 through 5, entities in Non-Registered SVSs 6 through 8 are only eligible to register and vote in a single SVS.

Normal Process for Regional Reliability Standards and Other Projects

Step 1 – Submit and Validate a Standard Authorization Request

Development, revision or retirement of a Regional Reliability Standard (RRS) or Other Project (OP) shall be initiated by the filing of a Standard Authorization Request (SAR) by any person or entity. A SAR is filed by completing the electronic fields of the online WECC SAR form. WECC staff shall review the incoming SAR to ensure it is valid. Once deemed valid, the SAR shall be immediately posted on the WECC website and notification shall be sent to the SEL.[3]

Step 2 – Complete SAR and Present to the WSC

WECC staff shall assign a unique tracking number to each SAR. The unique tracking number shall be used to identify the SAR throughout the development and archival processes. The SAR and those documents developed in response to the SAR shall be publicly accessible on the WECC website.

WECC staff shall determine within 30 days of receipt whether a SAR is complete. WECC staff may assist with completing the SAR, or report to the WSC that the SAR is incomplete and request guidance.

To be deemed complete, each SAR shall contain a description of the proposed RRS or OP subject matter sufficiently detailed to clearly define the purpose, scope, impacted parties, requirements and any other information relevant to the proposed RRS or OP.

Once deemed complete by WECC staff, WECC staff shall notify the WSC that the SAR has been received and is complete, and shall place the SAR on the agenda for the next scheduled WSC meeting for disposition, subject to required notice. Notice of WSC meetings and posting of WSC agendas will be provided in accordance with the WSC Charter.

The WSC shall determine whether the SAR is within the scope of WECC's authority and activities, and is appropriate for development. The WSC shall make that determination within 60 days of the date that the SAR is received by WECC, except where the SAR has been remanded, in which case the WSC shall make that determination within 30 days of receiving the curative SAR. Public comment on the SAR will be reviewed and considered by the WSC during a duly noticed WSC meeting prior to the WSC approving the SAR.

[3] A "valid" SAR is different than a "complete" SAR. A SAR is deemed valid by staff as a threshold review that filters out spam and unwanted nuisance documents that may be received via an open website portal. Whether a SAR is "complete" is addressed in Step 2.

The WSC shall ensure that the SAR provides enough information that a Drafting Team (DT) will have a clear understanding of the reasons for, and nature of, the RRS or OP to be developed. The SAR author may be asked to further assist in the development or clarification of the SAR.

The WSC may accept the SAR, in which case development proceeds to Step 3.

The WSC may remand a SAR if it determines the content of the SAR is deficient. If the SAR is deemed deficient, the WSC shall specify the deficiency identified in the SAR and suggest potential remedies as part of its remand. WECC staff will make reasonable efforts to assist the SAR author in addressing the deficiencies identified by the WSC.

The SAR author shall have 30 days from the date of remand or until the 60th day following submittal of the SAR, whichever is longer, to remedy each deficiency identified in the remand, or withdraw the SAR.

If the deficiencies are remedied, WECC staff will resubmit the SAR to the WSC for disposition. If the deficiencies are not remedied within the allotted period: 1) the SAR will be deemed incomplete, 2) no further developmental action will be taken on the SAR, and 3) the SAR will be archived. The SAR author may submit a new SAR without prejudice based on the same or similar fact pattern.

The WSC may reject a SAR if it determines the SAR is outside the scope of WECC's authority or is not appropriate to be undertaken by WECC. If a SAR is rejected, the WSC shall post its explanation for rejection on the WECC website. Notification of the WSC's decision shall: 1) be communicated to the SAR author, the Board, and the Standards Email List (SEL), 2) reference the unique SAR tracking number and direct the recipient to supporting information as appropriate, and 3) be made no more than 30 days from the date of the WSC's determination. The WSC's decision to reject a SAR may be appealed to the Board.

Step 3 – Convene the Drafting Team

If it accepts a SAR, the WSC may, at its discretion, expand or narrow the scope of the SAR. The WSC shall prioritize the development of the SAR in relation to other RRSs or OPs proposed for development under the Procedures, as may be required based on the volume of requests and resources. If prioritization dictates a postponed starting date, the WSC shall either set a postponed starting date or set a review date upon which the WSC shall re-evaluate the SAR for purposes of its progress through these Procedures. In no case shall the review date be more than 180 days after the date the SAR was received.

Upon establishing a start date for the development of an RRS or OP, the WSC shall convene a DT to develop the RRS or OP required by the SAR. The WSC may either directly assign a DT or solicit team member nominations from the industry. The WSC shall approve the DT membership within 60 days of establishing a start date. The WSC may augment or modify DT membership at any time as needed.

Because the DT chair's primary responsibility is leadership and coordination, the DT chair need not be a SME in the field associated with the SAR.

Names of DT members will be posted on the associated project development website.

The WSC should provide to the DT a proposed starting date and an expected completion date.

Step 4 –Begin Drafting Phase and Submit Draft to WSC

All DT meetings shall be open and publicly noticed on the WECC website.

The DT will begin working on the documents required by the SAR following assignment by the WSC. Notice of each DT meeting shall be posted on the WECC website for a minimum of 15 days prior to the meeting.

The author of the SAR may participate in the drafting process. The author of the SAR may be asked to provide additional information, supporting studies, and other information to support the requirements of the proposed RRS or OP.

An RRS shall include those sections mandated by NERC, such as an applicability section, effective date, mandatory requirements, affected time horizons, measures, compliance, violation risk factors (VRF), and violation severity levels (VSL).

Each RRS shall promote at least one reliability principle and be consistent with all reliability principles and NERC market interface principles. Each RRS shall provide for as much uniformity as possible with reliability standards across the interconnected Bulk-Power System of the North American continent. An RRS shall be more stringent than a continent-wide reliability standard, include a regional difference that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the Bulk-Power System.

An RRS or OP may include a guidance section, background section or other narrative sections; however, these sections are not required. Incorporation of extrinsic documents into an RRS or OP should be avoided.

An RRS or OP may include new definitions of terms that need to be added to the WECC or NERC glossaries. Wherever possible, DTs are encouraged to use existing defined terms rather than create new defined terms.

In drafting the applicability section of an RRS, only those functional entities listed in the currently approved NERC Functional Model shall be used. When drafting the applicability section of an OP, use of the NERC Functional Model is not required. Development of an OP should conform to WECC internal policies and practices, unless otherwise specified herein.

In the course of its assignment, the DT shall, at a minimum:

- Review any preliminary technical assessment provided with the SAR;
- Perform or request additional technical studies as needed;
- Prepare supporting documents to support the RRS or OP as needed; and
- Request from the WSC additional time to develop the RRS or OP, if necessary.

Step 5 – Post for Comment

Upon completion of each iterative draft of the RRS or OP, WECC staff shall facilitate the posting of the draft RRS or OP on the WECC website, along with supporting documents, if any, for a comment period of no less than 45 days for the first iteration and no less than 30 days for each iteration thereafter, except as allowed in the Expedited Process for Urgent Action section of these Procedures.

An implementation plan shall be included in at least one iterative posting during the development of the RRS or OP and shall be a part of the final record for consideration prior to ballot.

A notice that the comment period has been opened shall be distributed via the SEL. The notice shall include, at a minimum, the following information:

- Identification of the RRS or OP;
- What action is being taken (e.g., request for 30- or 45-day comment);
- The location of the document for review;
- How to submit comments or perform the requested action; and
- The opening and closing dates during which the solicited action shall take place. Unless otherwise posted, all posting periods close at 5:00 p.m. (Mountain).

WECC shall open a Web portal to serve as the sole means of receiving comments on the RRS or OP. Comments received via other media or received outside of the posted comment period will be accepted at the discretion of the DT. Comments may be submitted by any individual or entity, or a group of parties with a common comment. To streamline the process, if a group of parties elects to submit a common comment, those parties are encouraged to submit that common comment only once and append to the comment the names of all those individuals, entities or groups that are in support of the common position. DTs are charged to give due weight to such a joint comment and not to view the comment as having been received by a single individual or entity.

The WSC shall monitor each posting and review the posted documents to determine whether the DT remains within the scope of the SAR. At any time prior to opening a Ballot Pool, if the WSC concludes that the proposed RRS or OP is not within the scope of the SAR or does not meet other regulatory requirements or directives, the WSC shall either remand the RRS or OP to the DT with a specific explanation identifying the deficiencies that must be remedied, adjust the scope of the SAR, or retain the SAR as drafted and replace the DT.

Upon receiving the remanded RRS or OP and explanation of deficiencies, the DT shall

initiate a redraft following the steps contained in these Procedures. If a new DT is assigned, the new DT shall start the development efforts at Step 4 of these Procedures.

Step 6 – Respond to Comments

The DT shall consider all comments submitted in accordance with these Procedures. If the same comment is provided more than once, the DT may provide a single response to all comments that raise the same or a similar concern.

The DT shall prepare a summary of the comments received and the changes made to the proposed RRS or OP as a result of comments received. The DT shall summarize comments that were rejected by the DT, in whole or in part, and the reason(s) that these comments were rejected. The summary, along with a response to each comment received, will be posted on the WECC website no later than the next posting of the proposed RRS or OP.

All parties submitting comments are encouraged to participate in the DT meetings during which responses to their comments are considered and drafted.

The DT should target posting its responses to the WECC website no later than 30 days after the comment window has closed. If more than 30 days are required, the DT chair shall advise the WSC chair of the DT's progress and request additional assistance as needed.

Substantive Changes

If the DT determines that comments received during any posting warrant a Substantive Change to the language of an RRS or OP, the DT shall consider each comment and redraft the RRS or OP accordingly, repeating the posting / comment / response cycle as many times as needed to address the Substantive Changes while staying within the scope of the SAR.

If at any time during the development process the DT determines that the scope of the SAR should be adjusted, the DT shall present that request to the WSC for disposition.

If at any time during the development process the DT determines that it has reached a developmental impasse, the DT shall present the issue to the WSC for disposition.

If comments received during any posting do not warrant a Substantive Change to the language of an RRS or OP, the DT shall be polled at a regularly scheduled and announced DT meeting and asked whether the RRS or OP should be forwarded to the WSC with a recommendation to ballot the document. If the DT concludes by an affirmative majority vote that the RRS or OP should be forwarded to the WSC with a recommendation for ballot, the document will be forwarded accordingly.

Non-Substantive Changes

These Procedures acknowledge that a Non-Substantive change may be discovered at any point during or after the final development of the RRS or OP.

Non-Substantive Changes to an RRS shall be handled in accordance with the NERC Standards Development Manual or its successor.

Non-Substantive Changes to an OP shall be addressed using WECC's internal policies and practices. Non-Substantive changes for OPs do not require a comment / response cycle.

Step 7 – Submit Proposed Draft to the WSC with a Request for Ballot

Upon completion of the proposed RRS or OPs, the DT shall present the proposed RRS or OPs to the WSC with a request for ballot. The WSC shall address that request no later than its next regularly scheduled meeting.

After receiving a request for ballot, the WSC shall review the RRS or OP as presented and determine whether it fulfills the requirements stated in the SAR. The WSC shall also consider whether extrinsic requirements, such as FERC orders, Board directives, or other regulatory directives are met by the content of the document.

If the WSC concludes that the proposed RRS or OP is ready for ballot, the WSC shall forward the RRS or OP to WECC staff with a request that a Ballot Pool be formed from the Ballot Body, for the specific intent of seeking approval of the proposed RRS or OP. The results of the WSC's vote to forward the RRS or OP to the Ballot Pool shall be documented. Any WSC member that opposes submittal of the RRS or OP will be encouraged to provide dissenting comments, and if possible, specific language that would make the draft document acceptable to the dissenting member. If the WSC cannot reach agreement to submit the RRS or OP to the Ballot Pool, the WSC will report to and seek guidance from the Board.

If the WSC concludes that the proposed RRS or OP is not ready for ballot because it does not fulfill the requirements of the SAR or because it fails to meet other regulatory requirements or directives, the WSC shall remand the RRS or OP to the DT with a specific explanation identifying the deficiencies that must be remedied.

Upon receiving the remanded RRS or OP and explanation of deficiencies, the DT shall:

1) Redraft the RRS or OP accordingly;
2) Initiate iterative comment / response cycles as needed until it again concludes that no further Substantive Changes are needed; and
3) Return the proposed RRS or OP to the WSC for disposition.

Step 8 – Convene a Standards Briefing

Once the WSC approves submitting the RRS or OP to the Ballot Pool for ballot, WECC shall dispatch notice to the SEL that a Standards Briefing will be held to discuss the content of the proposed RRS or OP prior to balloting. Notice shall be provided 15 days or more before

the Standards Briefing is to be held and shall provide, at a minimum, the following:

- Identification of the RRS or OP;
- The time and place of the Standards Briefing; and
- The location of the proposed RRS or OP and related documentation for review.

Step 9 – Form the Ballot Pool and Ballot the Standard

Any individual or entity seeking participation in the ballot of an RRS or OP shall apply to WECC for Ballot Body membership in any SVS in which it is eligible. WECC staff shall review the request and confirm eligibility to join the Ballot Body.

Decisions of the staff to approve, deny, or restrict the admission of an individual or entity to a voting sector may be appealed in accordance with the WECC Bylaws.

From the Ballot Body, a discrete Ballot Pool will be formed for each RRS or OP to be balloted under these Procedures. All members of the Ballot Body shall be provided an opportunity to opt into a Ballot Pool formed for purposes of voting on each RRS or OP. It is the Ballot Pool that votes on RRSs and OPs developed under these Procedures.

Notice that a Ballot Pool is forming will be dispatched via the SEL. That notice shall contain, at a minimum, the following information:

1) Identification of the RRS or OP;
2) The proposed action to be taken (e.g., Notice of Ballot Pool Formation / Notice of Ballot);
3) When the Ballot Pool will open;
4) When the ballot will take place;
5) How to cast a vote; and
6) The location of the proposed RRS or OP and related documentation for review.

The Ballot Pool registration window shall remain open for a period determined by WECC staff, but in no case shall the Ballot Pool registration window be open less than 15 days or more than 30 days.

Once notice of a Ballot Pool forming has been dispatched: 1) the ballot window shall commence no sooner than 15 days and no later than 45 days after that dispatch; and 2) no Substantive Changes may be made to the proposed document unless the revisions are posted for an iterative comment / response cycle and a new date is set for ballot.

Once the ballot window opens, no Ballot Body member may join or withdraw from the Ballot Pool. The WECC Director of Standards (DOS) may authorize deviations from this rule for extraordinary circumstances such as the death, retirement, or disability of a Ballot Pool member that would prevent an otherwise eligible entity from casting a vote during a given ballot window.

Voting on an RRS or OP shall be via electronic voting administered on the WECC website.

The default voting window shall be a period of 15 days; however, the window may be held open up to a maximum of 60 days to reach a quorum. During a ballot window, WECC shall not sponsor or facilitate public discussion of the standard to be balloted.

Eligible members of the Ballot Pool may cast one vote in each SVS for which they are eligible.

Participating Stakeholders may only vote on an RRS if they have applied for and been granted Participating Stakeholder status. A Participating Stakeholder is only entitled to vote on an RRS and may only vote on a WECC Criterion if the proposed WECC Criterion could result in sanction to a non-WECC Member. A Participating Stakeholder is not entitled to vote on any other OP.

Each member of the Ballot Pool casting a negative vote on an RRS or OP will be required to provide a statement explaining the reason for the negative vote. The statement should include language that would make the RRS or OP acceptable. The statement will be included in the voting record for consideration by the WSC and the Board.

A two-thirds (2/3) quorum of the Ballot Pool is required for each vote. Quorum shall be based on the total number of Ballot Pool members and shall not be based on the total number of votes cast. Abstentions and negative votes cast without an explanation shall not be counted for the purpose of determining consensus, but will be counted for purposes of obtaining a quorum.

A weighted majority vote of the Ballot Pool is required for an RRS or OP to be approved. Voting among the SVSs shall be weighted as follows:

- For each SVS with 10 or more voters, the number of affirmative votes cast shall be divided by the sum of the affirmative and negative votes cast to determine the fractional affirmative vote for that SVS.

- For each SVS with less than 10 voters, the same process shall be used to determine the fractional affirmative vote, but the fractional affirmative vote of that SVS shall be multiplied by 10 percent times the number of voters.

    - For example, for SVSs with nine voters, the fractional affirmative vote will be multiplied by 90 percent.

- The sum of the fractional affirmative votes from all SVSs divided by the weighted number of SVSs voting shall be used to determine if a weighed majority has been achieved and whether the RRS or OP has been approved. An SVS shall be considered as voting if any member of the SVS in the Ballot Pool casts either an affirmative or a negative vote. If there are more than ten voters in the SVS, the weighting used for the calculation of “weighted sectors voting” shall be 100 percent. For SVSs with less than ten voters, the weighting used for the calculation of the “weighted sectors voting” shall be 10 percent per voter.

- An RRS or OP shall be deemed approved by the Ballot Pool if the sum of fractional affirmative votes from all SVSs divided by the weighted number of voting SVSs is a majority (i.e., greater than 50 percent).

After a vote by the Ballot Pool, the WSC shall take one of the following actions.

If the Ballot Pool approves an RRS or OP, the WSC shall submit the RRS or OP to the Board for approval. The WSC shall provide voting results to the Board, including the final ballot results and any rationale supporting any negative votes cast.

Any RRS or OP that was provided to the Board for approval will be posted for Board review for at least the period mandated by the WECC Bylaws.

If the Ballot Pool rejects the RRS or OP, the SAR shall be deemed complete and all associated documents shall be archived, except as allowed in the Regulatory Directive section of these Procedures.

Step 10 – Initiate the Appeals Process – If Needed

An appeal may be brought on the basis of either a technical (reliability) concern or a due process (procedural) concern.

If the appeal is based on technical grounds, that appeal may be brought at any stage of the development process prior to the opening of a ballot window. The appeal shall be submitted to the DOS who shall place the appeal on the agenda of the next regularly scheduled WSC meeting. If the appellant does not concur with the WSC's findings, the appellant may request that the DOS forward the matter to the Board for disposition.

If the appeal is based on due process concerns, the appellant shall submit the matter to the DOS no later than 30 days after the alleged occurrence of the due process violation, but in no case shall an appeal on due process grounds be accepted more than 30 days after the RRS or OP has been approved by the Ballot Pool. The appeal shall be submitted to the DOS who shall place the appeal on the agenda of the next regularly scheduled WSC meeting. If the appellant does not concur with the WSC's findings, the appellant may request that the DOS forward the matter to the Board for disposition.

The filing of an appeal shall not halt the development process; however, the appeal shall be settled by the Board before the Board votes to approve the RRS or OP.

Step 11 – Obtain Board Approval

The Board shall consider the RRS or OP for approval no later than at its next regularly scheduled meeting after the close of the Ballot Pool window and recommendation for approval by the WSC, subject to the notice requirements in the WECC Bylaws.

Any person or entity may submit comments to the Board for the Board's consideration. The

Board shall consider:

1) All comments submitted for its consideration;
2) The WSC's recommendations and minority opinions, if any;
3) All comments that were not incorporated into the RRS or OP;
4) Voting results including, at a minimum, the final ballot results and any rationale supporting negative votes; and
5) Any other supporting documentation.

If an OP is approved by the Board, WECC shall post the final OP on its website and the SAR will be deemed complete. The effective date will be that approved by the Board.

If an RRS is approved by the Board, WECC shall forward the RRS to NERC for NERC and FERC disposition.

If the RRS or OP is not approved by the Board, the Board may either deem the SAR complete or remand the RRS or OP to the DT with specific guidance as to proposed changes.

If the RRS or OP is remanded, any Substantive Changes must be vetted in accordance with these Procedures. Under no circumstances shall the Board make Substantive Changes to the RRS or OP, except in accordance with its backstop authority as authorized by the WECC Bylaws.

Step 12 – Submit RRSs for ERO Review, FERC Approval & Implementation of WECC Regional Reliability Standards

Note: Step 12 only applies to RRSs.

All new, revised, or retired RRSs shall be submitted to NERC for NERC and FERC approval. The approval, revision or retirement of an RRS shall not be effective in the United States until approved by FERC and shall not be effective in another jurisdiction until approved by the applicable governmental authority.

Step 13 – Retire an OP

Upon determining that the subject matter of an OP is duplicated in a NERC Reliability Standard, and that retirement of the OP will not cause a reliability gap after the effective date of the associated NERC Reliability Standard, the WSC may retire a WECC OP on its own initiative without further due process.

Step 14 – Submit a Request for Interpretation

A Request for Interpretation (RI) of a document developed under these Procedures is limited to clarifying existing requirements in the approved document and may not expand

upon a requirement or provide guidance on how to implement a requirement.

The RI is initiated by submitting WECC's online SAR form. The SAR shall: 1) identify the specific document; 2) identify the requirement within that document for which an interpretation is being requested, and 3) specify the perceived lack of clarity. The SAR shall indicate the material impact to the requesting entity or others caused by the perceived lack of clarity.

The RI is processed using the same process set forth in these Procedures with the following exceptions:

- The chair of the WSC shall assemble an Interpretation Drafting Team (IDT). The IDT shall be composed of SMEs with relevant expertise to address the clarification and, to the extent possible, should include members of the original DT. The IDT shall not include any team member representing the entity that filed the RI; however, this prohibition does not preclude representatives of the filing entity from participating in the development process.

- If all of the document is to be subsumed into the new PSS RRS the PSS DT should recommend to the Standing Committee that the document be retired as of the effective date of the replacement document.

- Once an interpretation of an RRS has been approved by the Board, the interpretation shall be appended to the RRS and submitted to NERC for NERC and FERC approval. The interpretation will remain appended to the RRS until such time as the RRS is revised and the interpretation's content is addressed during the revision process. RRS interpretations shall not be effective in the United States until approved by FERC and shall not be effective in other jurisdictions until approval by the applicable governmental authority.

Supporting Processes

Expedited Process for Urgent Action

In cases requiring urgent action, such as in the development of emergency procedures, any person or entity may propose an interim RRS or OP for approval by the WECC Board. The RRS or OP must go through a process that eliminates any or all of the steps outlined previously, but only to the extent deemed necessary by the Board and only in a manner that is consistent with the WECC Bylaws.

If the Board approves the interim document, it shall establish an initial effective date for the interim document.

Within 90 days after the initial effective date of the document, the Board shall either:

1) Cause a SAR to be submitted requesting the development under these Procedures of a permanent replacement to the interim document; or

2) Shall extend the applicability of the interim document for an additional 90 days.

Renewal may occur more than once, but a good faith effort must be made to develop a permanent replacement under these Procedures.

If a SAR is submitted, the interim RRS or OP shall remain in effect until the permanent replacement RRS or OP becomes effective.

If a SAR is not submitted and the interim RRS or OP has not been extended, the interim RRS or OP shall be deemed retired.

Regulatory Directives

These Procedures acknowledge that FERC may order WECC to make specified regulatory changes to documents created under these Procedures. For the purpose of this section only, those documents are referred to as Directive Regional Reliability Standards (DRRS).

If the Board determines that these Procedures failed to result in a DRRS meeting the mandated regulatory changes, the Board shall have authority to take the following actions to ensure that the DRRS is responsive to the regulatory directive.

If the Ballot Pool approves a DRRS that does not address a regulatory directive required to be included in that document, the Board may remand the DRRS to the original DT or instruct the WSC to convene a new DT to redraft the document. The Board shall instruct the DT on the specific regulatory directive that must be contained in the redraft. Once the DRRS is redrafted it shall be reprocessed under these Procedures.

If the Ballot Pool rejects a DRRS or fails to ballot the DRRS due to failure to reach a quorum, either when first presented for ballot or during an iterative redraft as instructed by the Board, the Board shall review the DRRS, including all comments provided and all rationale accompanying any negative vote.

Upon a finding that the DRRS was rejected for reasons not related to the regulatory directive, the Board may direct WECC staff to file a new SAR with the specific narrow scope of addressing only the regulatory directive. The Board may suggest specific language for inclusion in the proposed DRRS.

Upon a finding that the DRRS was rejected based on language addressing the regulatory directive, the Board shall take the following steps to meet its regulatory obligation:

1) Review the entire record of development.
2) Require a public technical conference to be noticed and convened to determine whether the rejected DRRS is:
    - just and reasonable;
    - not unduly discriminatory or preferential;
    - in the public interest;

- helpful to reliability;
- practical;
- technically sound;
- technically feasible;
- cost-justified; and
- meets the regulatory directive (hereafter “Just and Reasonable”).

3) Determine whether the DRRS should be implemented as drafted, notwithstanding rejection by the Ballot Pool.

Upon a finding that the rejected DRRS should be implemented, the Board shall approve the DRRS and direct that it be submitted to NERC for NERC and FERC approval, as required.

Upon a finding that the rejected DRRS should not be implemented, the Board may submit the DRRS and its record of development as a regulatory compliance filing in response to the regulatory directive. The filing shall include a recommendation that the DRRS not be made effective and an explanation of the basis for that recommendation.

Maintenance of the Procedures

The WSC is charged with maintenance of these Procedures. Proposed changes to these Procedures shall first be brought to the WSC for consideration. The WSC may initiate proposed changes on its own initiative.

If it determines that a change to these Procedures should be pursued, the WSC shall draft the proposed changes and post the proposed changes to the WECC website for comment, accompanied by a notice to the SEL soliciting comments on the proposed changes.

The WSC shall consider all comments received and shall redraft the proposed changes as it deems necessary. Once the WSC approves the proposed changes, those changes shall be submitted to the Board for approval. Changes to these Procedures approved by the Board shall be submitted to NERC for NERC and FERC approval.

Maintenance of RRS and OPs Documents

The WSC shall ensure that each RRS is reviewed at least once every five years from the effective date of the most recent version of the RRS. If the review identifies needed changes, the WSC shall cause a remedial SAR to be filed. If the review does not identify needed changes, the WSC shall communicate its decision via the SEL and no further action will be required.

Review of OPs shall be conducted in accordance with internal WECC policies and procedures.

Attachment 2

Reliability Standards Development Procedures

Amended Exhibit of the Delegation Agreement Between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council

Redline Version

RELIABILITY STANDARDS
DEVELOPMENT PROCEDURES

Introduction

This document explains the WECC process for requesting, announcing, developing, revising, withdrawing and approving WECC Standards as defined below ("WECC Standards Process"). The process involves several steps:

- A request to develop a new Standard or revise an existing Standard
- Decision to proceed with development or revision of a Standard and assignment to a Drafting Team

Public (including members) notification

The Western Electricity Coordinating Council (WECC) is a Regional Entity[1] authorized through a delegation agreement between the North American Electricity Reliability Corporation (NERC) and WECC pursuant to Section 215 of the Federal Power Act. NERC delegates designated powers, rights, and responsibilities to WECC regarding the administration within the Western Interconnection of electric Reliability Standards adopted or approved by NERC and the Federal Energy Regulatory Commission (FERC).

These Reliability Standards Development Procedures (Procedures) define the process to be used by WECC for the development, revision, and retirement of Regional Reliability Standards (RRS) and various Other Projects (OP) created under these Procedures.

- These Procedures were established to create the structure for open and transparent due process in the development of WECC RRSs and OPs. These Procedures include, but are not limited to, public notice of intent to develop ~~or revise~~RRSs and OPs, a ~~Standard~~
- ~~Drafting stage~~
- ~~Posting of draft for~~ public comment
- ~~Review of all comments and public posting of decisions reached on each comment~~
- ~~Ballot Body balloting of the~~ period on the proposed ~~Standard~~
- ~~Consideration~~documents, due consideration of comments provided, and a balanced ballot of ~~any appeals~~
- ~~WECC Board of Directors (Board) decision regarding approval, disapproval or remand of proposed Standard~~
- ~~Forwarding proposed WECC Reliability Standards to the ERO~~

~~The~~ process for developing and approving WECC Standards includes:

~~1. Notification of pending Standard change before a wide audience of all "~~interested ~~and affected parties"~~stakeholders.

The ~~2. Posting Standard change drafts for all parties to review~~

[1] Unless otherwise specified, capitalized terms are defined in the NERC Glossary of Terms Used in Reliability Standards.

3. Provision for gathering and posting comments from all parties

4. Provision for an appeals process – both "due process" and "technical" appeals

The WECC Standards Committee (WSC) has the responsibility for developing and balloting WECC Standards. The WSC Chair is responsible for ensuring administration of the process and completion of all WSC responsibilities. The WSC is supported by the Standing Committees as well as Drafting Teams that draft the Standards. The WSC, with the support of a Drafting Team and Standing Committees, ensures the Draft Standard is properly reviewed consistent with WECC due process requirements, responses have been provided to comments on the Draft Standard, or the Draft Standard is revised in response to the comments. Board approval signifies that WECC has adopted the Standard. WECC staff has the role of tracking the Standard as it moves through the process and facilitating resolution of issues. In accordance with Section 8.6 of the WECC Bylaws, Participating Stakeholders may participate in Reliability Standard development by joining the Ballot Body and may vote electronically on a Draft Standard.

WECC Bylaws Controlling

It is the intention of the drafters of the WECC Standards Process that the procedures described herein Procedures shall be interpreted and applied in a manner that is consistent with the WECC Bylaws. Should any conflict arise between this WECC Standards Process the Procedures and the WECC Bylaws arise, the WECC Bylaws will control prevail.

Terms

Definitions

Ballot Body. The Ballot Body consists

That body of qualified WECC members Members and non-members that register with WECC for participation in Ballot Pools.

Ballot Pool

That pool of Ballot Body entities that have been determined eligible for registered to vote on a specific document.

Day

All references to days are calendar days. When counting the WECC Standard Voting Sectors described in this Reliability number of days, the count shall exclude the first day of the time window to be measured. If a terminus date falls on a weekend or a day that WECC is scheduled to be closed, the new terminus date shall be the day following the weekend or WECC closure day.

For example, if a 15-day period ends on a holiday the terminus date is on the following WECC business day.

Drafting Team (DT)

A team of pertinent subject matter experts (SME) that was appointed by the WECC Standards Committee (WSC) to develop the document(s) that were called for in a Standard Authorization Request (SAR) consider and respond to industry comments, participate in forums to help build consensus on draft documents, and perform other tasks as assigned by the WSC.

Electric Line of Business

The generation, transmission, distribution, or trading of electricity or the provision of related energy services in the Western Interconnection.

NERC Compliance Registry

Registry of the Bulk Electric System owners, operators, and users that are subject to approved reliability standards.

Non-Substantive Changes

A Non-Substantive Change is one that does not change the scope, applicability, intent of the document, or the actions required by affected entities.

For example, Non-Substantive Changes include, but are not limited to; correcting grammar or sentence structure, typographical or spelling errors, font and formatting, numbering, references, adding an obviously missing word, or rephrasing a statement to improve its clarity. Non-Substantive Changes do not require, but may receive posting for comments and/or revision of the document under these Procedures.

Other Projects (OP)

Any document type other than an RRS developed under these Procedures. These include, but are not limited to, WECC Criteria.

Participating Stakeholder~~Development Process and in section 8.5.5.2 of~~

Any person or entity that is not a WECC Member, but who has applied for and been granted participating stakeholder rights as defined and currently set forth in the WECC Bylaws. ~~The Ballot Body consists of the entities that may vote on Regional Criteria and~~

Regional Reliability Standard (RRS)

A requirement approved by FERC under Section 215 of the Federal Power Act, to provide for reliable operation of the Bulk Electric System in the United States. Regional Reliability

Standards, except as otherwise limited by these procedures. are specific to the Western Interconnection and shall be established using these Procedures. When approved by FERC and applicable authorities in Canada and Mexico, Regional Reliability Standards shall be made part of the body of NERC Reliability Standards and shall be enforced upon all applicable Bulk-Electric System owners, operators, and users within the WECC area, regardless of membership in the region.

Standard Authorization Request (SAR)

Ballot Pool. The Ballot Pool consists of Ballot Body entities that have opted to vote on a specific Standard. Quorum for voting on a Standard is based on the Ballot Pool.

Days. All references to days in this document refer to calendar days, except as otherwise noted in these procedures.

Draft Standard. A Draft Standard includes any proposed new Standards, revisions to existing Standards, or termination of existing Standards. Draft Standards are introduced by use of Standard Authorization Requests or the Special Procedures for Addressing Regulatory Directives, as described in these procedures.

Joint Session. The Joint Session is any collective meeting of the Standing Committees. Such meetings are generally held in conjunction with the regular meetings of the individual Standing Committees.

Participating Stakeholder. A Participating Stakeholder as defined in Section 3.33 of the WECC Bylaws.

Standard. In the context of this document, the term Standard refers to a Regional Reliability Standard or a Regional Criterion.

form titled *Standard Authorization Request (*~~**or "***~~*SAR*~~**").** The form titled~~*)* administrated by the WECC Standards~~/Regional Criteria Request Form approved~~ Department for the purpose of requesting development, revision, retirement, or interpretation of an RRS or OP.

Standards Briefing

Any meeting initiated by WECC for the purpose of ~~requesting a new Standard, a revision to an existing Standard, or termination of~~creating an ~~existing Standard.~~

Standing Committee. The Market Interface Committee (MIC), Operating Committee (OC) or Planning Coordination Committee (PCC).[2]

[2] In accordance with WECC Bylaws Section 8.5.4, Membership in WECC's Standing Committees is open to all WECC members.

~~**WECC Standards Committee.** This committee consists of one representative from each of the eight Voting Sectors described in Section 8.5.5.2 of the Bylaws~~open forum for discussion and ~~a ninth member who shall be a member of the WECC Board of Directors. The members of the WSC shall be appointed by, and serve at the pleasure of, the Board, in accordance with a charter of the WSC approved by the Board. The chair of the Board shall designate a member of the Board of Directors to serve as the chair of the WSC. The WSC is responsible for determining if a Standard Authorization Request is within the scope of WECC's activities, and overseeing the drafting, comment and voting~~explanation of an RRS or OP, generally but not exclusively held during the development process ~~for a Standard. The WSC is responsible for taking actions described in the Special Procedures for Addressing Regulatory Directives to ensure compliance with directives issued by the Federal Energy Regulatory Commission (FERC) or Mexican or Canadian regulatory authorities. The WSC shall also oversee the process for responding to requests for interpretations of Standards.~~of those documents in advance of a ballot window.

Standards Email List (SEL)

Email list(s) established and maintained by WECC for the purpose of communicating due process activity; generally, but not exclusively, for standards-related activities.

Substantive Changes

A Substantive Change is one that changes the scope, applicability, intent of the document, or the actions required by affected entities.

For example, Substantive Changes include but are not limited to:

- changes to the functional entities listed in the applicability section of the RRS or OP;
- changes to the effective date;
- adding, deleting or revising requirements, measures or explanatory narrative.

Substantive Changes to an RRS or an OP require at least one posting / comment / response cycle.

WECC Member

Any entity that has applied and been accepted for membership in WECC ~~**Standards Voting Sectors**. For purposes of voting on Standards,~~ and is current in the payment of dues.

WECC Standards Committee (WSC)

Committee established by the WECC Board of Directors (Board) for the purpose of overseeing the implementation of these Procedures pursuant to its Board-approved charter.

Overview

This document has two dominate sections. The first section describes the development steps for the Normal Process for Regional Reliability Standards and Other Projects. The second section augments the first with Supporting Processes to address exceptions such as an expedited process for urgent actions, addressing regulatory directives, and maintenance

of certain documents.

Development Steps/Table of Contents

The following development steps are included in the normal process for Regional Reliability Standards and Other Projects section:[3]

Step 1 – Submit and Validate a Standard Authorization Request 9

Step 2 – Complete SAR and Present to the WSC 10

Step 3 – Convene the Drafting Team 11

Step 4 –Begin Drafting Phase and Submit Draft to WSC 12

Step 5 – Post for Comment 13

Step 6 – Respond to Comments 15

Step 7 – Submit Proposed Draft to the WSC with a Request for Ballot 16

Step 8 – Convene a Standards Briefing 16

Step 9 – Form the Ballot Pool and Ballot the Standard 17

Step 10 – Initiate the Appeals process – If Needed 22

Step 11 – Obtain Board Approval 23

Step 12 – Submit RRSs for ERO Review, FERC Approval & Implementation of WECC Regional Reliability Standards

Step 13 – Retire an OP 24

Step 14 – Submit a Request for Interpretation 24

The following related processes are included in the Supporting Processes section:

- Expedited Process for Urgent Action
- Regulatory Directives~~members~~
- Maintenance of Procedures
- Maintenance of RRSs and OPs Documents

[3] This Table of Contents will reflect the final actual pagination after final formatting. This footnote will be deleted from the final document.

Notices

Notices required under these Procedures shall be distributed electronically via WECC's SEL(s) and deemed delivered when posted on the WECC website, except as noted in the following paragraph. Concurrent running of notice and posting periods is explicitly allowed.

WECC shall provide notice to NERC of all standards-related activities by including NERC on WECC's SEL. Inclusion of a NERC-provided email address on the related SEL shall constitute coordination of notice to NERC of standards-related activities and shall be deemed delivered upon dispatch via the SEL(s).

All WECC Members and Participating Stakeholders will be given an opportunity to receive notices provided via the SEL.

WECC Standards Committee (WSC)

The WSC manages these Procedures. The WSC protects the integrity, credibility and implementation of the Procedures while acting in accordance with the WSC Charter. Delineation of specific WSC duties, WSC composition and governance, WSC voting privileges, and other related practices, shall ~~vote~~be in ~~the following eight sectors.~~ accordance with the WSC charter as approved by the Board.

WECC Standards Voting Sectors

There are eight (8) Standards Voting Sectors (SVS) in which an entity may register to vote. The SVSs are divided into two separate categories: Registered and Non-Registered.

The Registered category is for those entities *registered* on the NERC Compliance Registry and to those Canadian and Mexican entities that perform functions that, if performed in the United States, would allow those entities to be registered for compliance in the NERC Compliance Registry. The Non-Registered category is for all others meeting the qualifications of those defined SVSs. A single entity cannot be in the Registered category and the Non-Registered category at the same time.

SVSs 1 through 5 are "Registered" SVSs.

~~1)~~ 1) Transmission Sector. ~~-~~This sector consists of Western Interconnection entities registered in the NERC ~~compliance registry~~Compliance Registry as ~~transmission owners, transmission operators, transmission service providers, or transmission planners~~Transmission Owners, Transmission Operators, Transmission Service Providers, or Transmission Planners;

~~2)~~ 2) Generation Sector. ~~-~~This sector consists of Western Interconnection entities registered in the NERC ~~compliance registry~~Compliance Registry as ~~generation owners or generation operators~~Generation Owners or Generation Operators;

~~3)~~ 3) Marketers and Brokers Sector. ~~-~~This sector consists of Western

Interconnection entities registered in the NERC ~~compliance registry~~Compliance Registry as ~~purchasing-selling entities~~Purchasing-Selling Entities.

~~4)~~ 4) Distribution Sector. ~~-~~This sector consists of Western Interconnection entities registered in the NERC ~~compliance registry~~Compliance Registry as ~~distribution providers or load-serving entities~~Distribution Providers or Load-Serving Entities;

~~5)~~ 5) System Coordination Sector. ~~-~~This sector consists of Western Interconnection entities registered in the NERC ~~compliance registry as balancing authorities, reserve sharing groups, planning authorities, resource planners, interchange authorities, and reliability coordinators. WECC may cast a vote in this sector;~~Compliance Registry as Balancing Authorities, Reserve Sharing Groups, Planning Authorities/Coordinators, Resource Planners, Interchange Authorities/Coordinators, or Reliability Coordinators.

~~6) End Use Representative Sector. This sector consists of non-registered members of WECC Member Class Four;~~

SVS 6 through 8 are "Non-Registered" SVSs.

6) End-Use Representative Sector. This sector consists of entities not on the NERC Compliance Registry, but that are WECC Members and are end users of significant amounts of electricity in the Western Interconnection, including; industrial, agricultural, commercial and retail entities as well as organizations in the Western Interconnection that represent the interests of a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public or the environment.

~~7)~~ 7) State and Provincial Representatives Sector. ~~-~~This sector consists of ~~non-registered~~ entities not on the NERC Compliance Registry, but that are WECC ~~members of~~ Members that are representatives of states and provinces in the Western Interconnection provided that such representatives will have policy or regulatory roles and do not represent state or provincial agencies and departments whose function involves significant direct participation in the market as end users or in Electric Line of Business activities.~~**WECC Member** Class Five;~~

8) Other Non-Registered WECC Members and Participating Stakeholders Sector. ~~-~~This sector consists of ~~consultants or other members of WECC Member Class Seven, or interested stakeholders who qualify for~~ (1) Participating ~~Stakeholder status but are not~~ Stakeholders as defined in the WECC Bylaws, (2) WECC Members not on the NERC Compliance Registry that are Electric Line of Business entities doing business in the Western Interconnection that do not own, control or operate transmission or distribution lines in the Western Interconnection, including power markets, independent power producers, any other entities whose primary business is the provision of energy services, and (3) those entities that are not eligible for membership in any other Standards Voting Sector and who have a substantial interest in the purposes of WECC.

8) If a single entity qualifies for more than one Registered SVS, that entity may register and vote in each Registered SVS for which it qualifies. For example, if a single entity was registered in the NERC compliance registry.Compliance Registry as a transmission owner and also a generator owner; that single entity could register and vote once in SVS 1 and once in SVS 2.

For sectors oneNon-Registered SVSs 6 through five, Western Interconnection8 represent those entities that perform functions outside the United States, that if conducted in the United States would qualify them for the NERC compliance registries included in these sectors, shall be eligible to vote in the appropriate sector(s), as may be determined by WECC staff.

Each WECC member or Participating Stakeholder shall have a vote that may be cast in each sector for which the member or stakeholder is eligible as described in Section 8.5.5.4 of the Bylaws.

Sectors one through five are the*not registered* sectors, and the three non-registered sectors are sectors six through eight. If an entity is eligible for a registered sector, then that entity may be eligible for more than one registered sector. An entity can only be in one non-registered sector. An entity cannot be in both a registered and a non-registered sector. The first five sectors (in the NERC Compliance Registry. Unlike Registered SVSs 1 through 5) shall be in the North American Electric Reliability Corporation ("NERC") compliance registry, with the exception for, entities that perform functions outside the United States that are determined eligible for these voting sectors by WECC Staffin Non-Registered SVSs 6 through 8 are only eligible to register and vote in a single SVS.

Participating Stakeholders may not vote on Regional Criteria unless the proposed Regional Criteria could result in sanctions to a non-WECC member.

Normal Process for Regional Reliability Standards and Other Projects

Step 1 – Request To Revise or DevelopSubmit and Validate a Standard Authorization Request

Requests to develop, terminate,
Development, revision or revise retirement of a Regional Reliability Standard will(RRS) or Other Project (OP) shall be submitted toinitiated by the WECC staff through the usefiling of the WECCa Standard Authorization Request ("(SAR"). Requesters may be) by any individual or organization. WECC membershipperson or entity. A SAR is not a requirement as long asfiled by completing the electronic fields of the online WECC SAR form. WECC staff shall review the requester has an interest in electric system reliability or commercial business practices inincoming SAR to ensure it is valid. Once deemed valid, the Western Interconnection.SAR shall be

immediately posted on the WECC website and notification shall be sent to the SEL.[4]

Step 2 – ~~Standard Authorization Request Validation and Submission~~**Complete SAR and Present** to the WSC

~~The SAR will be reviewed for completeness and assigned a tracking number by the~~ WECC staff shall assign a unique tracking number to each SAR. The unique tracking number shall be used to identify the SAR throughout the development and archival processes. The SAR and those documents developed in response to the SAR shall be publicly accessible on the WECC website.

WECC staff~~. Staff may~~ shall determine within 30 days of receipt whether a SAR is complete. WECC staff may assist with completing the ~~request~~SAR, or report to the WSC that the SAR is incomplete and request guidance. ~~When complete, the WECC staff will forward the SAR to the WSC. WECC staff will maintain a web-based form that tracks all SARs through the Standard development process, as well as a Standards development tracking log that is posted on the WECC website.~~

~~The WSC will confer either in person or via conference call within two weeks of receipt of a completed request to determine whether the request is within WECC's scope.~~

~~If the WSC~~

To be deemed complete, each SAR shall contain a description of the proposed RRS or OP subject matter sufficiently detailed to clearly define the purpose, scope, impacted parties, requirements and any other information relevant to the proposed RRS or OP.

Once deemed complete by WECC staff, WECC staff shall notify the WSC that the SAR has been received and is complete, and shall place the SAR on the agenda for the next scheduled WSC meeting for disposition, subject to required notice. Notice of WSC meetings and posting of WSC agendas will be provided in accordance with the WSC Charter.

The WSC shall determine whether the SAR is within the scope of WECC's authority and activities, and is appropriate for development. The WSC shall make that determination within 60 days of the date that the SAR is received by WECC, except where the SAR has been remanded, in which case the WSC shall make that determination within 30 days of receiving the curative SAR. Public comment on the SAR will be reviewed and considered by the WSC during a duly noticed WSC meeting prior to the WSC approving the SAR.

The WSC shall ensure that the SAR provides enough information that a Drafting Team (DT) will have a clear understanding of the reasons for, and nature of, the RRS or OP to be developed. The SAR author may be asked to further assist in the development or clarification of the SAR.

[4] A "valid" SAR is different than a "complete" SAR. A SAR is deemed valid by staff as a threshold review that filters out spam and unwanted nuisance documents that may be received via an open website portal. Whether a SAR is "complete" is addressed in Step 2.

The WSC may accept the SAR, in which case development proceeds to Step 3.

The WSC may remand a SAR if it determines the content of the SAR is deficient. If the SAR is deemed deficient, the WSC shall specify the deficiency identified in the SAR and suggest potential remedies as part of its remand. WECC staff will make reasonable efforts to assist the SAR author in addressing the deficiencies identified by the WSC.

The SAR author shall have 30 days from the date of remand or until the 60th day following submittal of the SAR, whichever is longer, to remedy each deficiency identified in the remand, or withdraw the SAR.

If the ~~, by majority vote, that a~~ deficiencies are remedied, WECC staff will resubmit the SAR to the WSC for disposition. If the deficiencies are not remedied within the allotted period: 1) the SAR will be deemed incomplete, 2) no further developmental action will be taken on the SAR, and 3) the SAR will be archived. The SAR author may submit a new SAR without prejudice based on the same or similar fact pattern.

The WSC may reject a SAR if it determines the SAR is outside the scope of WECC's authority or ~~inappropriate, it will prepare an~~is not appropriate to be undertaken by WECC. If a SAR is rejected, the WSC shall post its explanation ~~and post it~~ for rejection on the WECC website. ~~The party that submitted the SAR, parties subscribing to the WECC standards email list, the Standing Committees, and Board will all be notified of the posting and its location on the WECC website. If the WSC decides to reject a SAR at this stage, such~~Notification of the WSC's decision shall: 1) be communicated to the SAR author, the Board, and the Standards Email List (SEL), 2) reference the unique SAR tracking number and direct the recipient to supporting information as appropriate, and 3) be made no more than 30 days from the date of the WSC's determination. The WSC's decision to reject a SAR may be appealed to the Board ~~in accordance with Step 8.~~.

~~Upon ascertaining that a SAR is within the scope of WECC's authority and appropriate, the WSC will select and oversee a Drafting Team formed for the purpose of drafting a Draft Standard. The WSC shall ensure that the Drafting Team includes a composite of individuals having the appropriate planning, operations, and market expertise. Notification of such assignments will be posted on the WECC website and sent to all parties that subscribe to the WECC standards email list. In addition, such assignments will be simultaneously noticed to NERC. The WSC shall ensure that the SAR provides the Drafting Team and WECC a description of the Draft Standard it expects the Drafting Team to draft, and an explanation as to why the Draft Standard is needed.~~

~~Step 3 – Drafting Team Begins~~Step 3 – Convene the Drafting Team

If it accepts a SAR, the WSC may, at its discretion, expand or narrow the scope of the SAR. The WSC shall prioritize the development of the SAR in relation to other RRSs or OPs proposed for development under the Procedures, as may be required based on the volume

of requests and resources. If prioritization dictates a postponed starting date, the WSC shall either set a postponed starting date or set a review date upon which the WSC shall re-evaluate the SAR for purposes of its progress through these Procedures. In no case shall the review date be more than 180 days after the date the SAR was received.

Upon establishing a start date for the development of an RRS or OP, the WSC shall convene a DT to develop the RRS or OP required by the SAR. The WSC may either directly assign a DT or solicit team member nominations from the industry. The WSC shall approve the DT membership within 60 days of establishing a start date. The WSC may augment or modify DT membership at any time as needed.

Because the DT chair's primary responsibility is leadership and coordination, the DT chair need not be a SME in the field associated with the SAR.

Names of DT members will be posted on the associated project development website.

The WSC should provide to the DT a proposed starting date and an expected completion date.

Step 4 –Begin Drafting Phase and ~~Submits~~Submit Draft ~~Standard~~ to WSC

~~The Drafting Team will begin working on the Draft Standard following assignment by the WSC, as directed by the WSC chair. The WSC shall provide a time period for which the Drafting Team should complete the Draft Standard. The WSC chair shall designate a Drafting Team leader who shall be responsible for coordinating the Drafting Team's efforts. Notification of Drafting Team meetings will be posted on the WECC website and sent to all parties that subscribe to the WECC standards email list at least 15 calendar days prior to the meeting. In addition, notification of all Drafting Team meetings will be simultaneously noticed to NERC. These meetings will be open to interested stakeholders. The Drafting Team will facilitate interested stakeholder participation in the discussion in order to encourage understanding of the issues and consensus among the meeting participants. The Drafting Team will work to achieve a consensus recommendation. A consensus recommendation is one that strives to eliminate all well-reasoned objections, but if the Drafting Team determines that it is not possible to accommodate all such points of view, it may proceed to provide a recommendation that is supported by a majority of the Drafting Team members.~~

~~Standard requesters have the right, and are encouraged to~~
All DT meetings shall be open and publicly noticed on the WECC website.

The DT will begin working on the documents required by the SAR following assignment by the WSC. Notice of each DT meeting shall be posted on the WECC website for a minimum of 15 days prior to the meeting.

The author of the SAR may participate in the drafting process. ~~Requesters~~The author of the SAR may be ~~called on~~asked to provide additional information, supporting studies, and other information to support the requirements of the ~~Draft Standard~~proposed RRS or OP.

An RRS shall include those sections mandated by NERC, such as an applicability section, effective date, mandatory requirements, affected time horizons, measures, compliance, violation risk factors (VRF), and violation severity levels (VSL).

Each ~~All WECC Standards will follow a standard format that refers to the "Responsible Entities" included in the NERC Functional Model and includes compliance measures according to the WECC standard template. The Drafting Team will include definitions for any terms included in the Draft Standard that need to be added to the WECC glossary.~~

RRS shall promote at least one reliability principle and be consistent with all reliability principles and NERC market interface principles. Each RRS shall provide for as much uniformity as possible with reliability standards across the interconnected Bulk-Power System of the North American continent. An RRS shall be more stringent than a continent-wide reliability standard, include a regional difference that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the Bulk-Power System.

An RRS or OP may include a guidance section, background section or other narrative sections; however, these sections are not required. Incorporation of extrinsic documents into an RRS or OP should be avoided.

An RRS or OP may include new definitions of terms that need to be added to the WECC or NERC glossaries. Wherever possible, DTs are encouraged to use existing defined terms rather than create new defined terms.

In drafting the applicability section of an RRS, only those functional entities listed in the currently approved NERC Functional Model shall be used. When drafting the applicability section of an OP, use of the NERC Functional Model is not required. Development of an OP should conform to WECC internal policies and practices, unless otherwise specified herein.

In the course of its ~~review~~assignment, the ~~Drafting Team:~~ DT shall, at a minimum: ~~will review the~~

- Review any preliminary technical assessment provided ~~by~~with the ~~requester;~~ SAR;
- ~~may perform~~Perform or request additional technical studies~~, if necessary;~~ as needed;

- ~~will complete an impact assessment report as part of its evaluation to assess the potential effects of the request;~~

- ~~may prepare additional~~Prepare supporting documents to support the ~~Draft Standard~~RRS or OP as needed; and
- ~~may request~~Request from the WSC additional time to develop the ~~Draft Standard~~RRS or OP, if ~~the Drafting Team believes it is~~ necessary.~~-~~

~~The Drafting Team, upon reaching a determination, by majority vote, on the language for a Draft Standard, shall submit the Draft Standard to the WSC. The Drafting Team shall also~~

~~supply the WSC with the impact assessment report, any additional technical studies performed, and any other materials that significantly contributed to the Drafting Team's evaluation and drafting of the Draft Standard.~~

Step ~~4 – Draft Standard Posted~~5 – Post for Comment

Upon completion of each iterative draft of the RRS or OP, WECC staff shall facilitate the posting of the draft RRS or OP on the WECC website, along with supporting documents, if any, for a comment period of no less than 45 days for the first iteration and no less than 30 days for each iteration thereafter, except as allowed in the Expedited Process for Urgent Action section of these Procedures.

An implementation plan shall be included in at least one iterative posting during the development of the RRS or OP and shall be a part of the final record for consideration prior to ballot.

A notice that the comment period has been opened shall be distributed via the SEL. The notice shall include, at a minimum, the following information:

- Identification of the RRS or OP;
- What action is being taken (e.g., request for 30- or 45-day comment);
- The location of the document for review;
- How to submit comments or perform the requested action; and
- The opening and closing dates during which the solicited action shall take place. Unless otherwise posted, all posting periods close at 5:00 p.m. (Mountain).

WECC shall open a Web portal to serve as the sole means of receiving comments on the RRS or OP. Comments received via other media or received outside of the posted comment period will be accepted at the discretion of the DT. Comments may be submitted by any individual or entity, or a group of parties with a common comment. To streamline the process, if a group of parties elects to submit a common comment, those parties are encouraged to submit that common comment only once and append to the comment the names of all those individuals, entities or groups that are in support of the common position. DTs are charged to give due weight to such a joint comment and not to view the comment as having been received by a single individual or entity.

The WSC shall monitor each posting and review the posted documents to determine whether the DT remains within the scope of the SAR. At any time prior to opening a Ballot Pool, if the WSC concludes that the proposed RRS or OP is not within the scope of the SAR or does not meet other regulatory requirements or directives, the WSC shall either remand the RRS or OP to the DT with a specific explanation identifying the deficiencies that must be remedied, adjust the scope of the SAR, or retain the SAR as drafted and replace the DT.

Upon receiving the remanded RRS or OP and explanation of deficiencies, the DT shall initiate a redraft following the steps contained in these Procedures. If a new DT is assigned, the new DT shall start the development efforts at Step 4 of these Procedures.

Step 6 – Respond to Comments

The DT shall consider all comments submitted in accordance with these Procedures. If the same comment is provided more than once, the DT may provide a single response to all comments that raise the same or a similar concern.

The DT shall prepare a summary of the comments received and the changes made to the proposed RRS or OP as a result of comments received. The DT shall summarize comments that were rejected by the DT, in whole or in part, and the reason(s) that these comments were rejected. The summary, along with a response to each comment received, will be posted on the WECC website no later than the next posting of the proposed RRS or OP.

All parties submitting comments are encouraged to participate in the DT meetings during which responses to their comments are considered and drafted.

The DT should target posting its responses to the WECC website no later than 30 days after the comment window has closed. If more than 30 days are required, the DT chair shall advise the WSC chair of the DT's progress and request additional assistance as needed.

Substantive Changes

If the DT determines that comments received during any posting warrant a Substantive Change to the language of an RRS or OP, the DT shall consider each comment and redraft the RRS or OP accordingly, repeating the posting / comment / response cycle as many times as needed to address the Substantive Changes while staying within the scope of the SAR.

If at any time during the development process the DT determines that the scope of the SAR should be adjusted, the DT shall present that request to the WSC for disposition.

If at any time during the development process the DT determines that it has reached a developmental impasse, the DT shall present the issue to the WSC for disposition.

If comments received during any posting do not warrant a Substantive Change to the language of an RRS or OP, the DT shall be polled at a regularly scheduled and announced DT meeting and asked whether the RRS or OP should be forwarded to the WSC with a recommendation to ballot the document. If the DT concludes by an affirmative majority vote that the RRS or OP should be forwarded to the WSC with a recommendation for ballot, the document will be forwarded accordingly.

Non-Substantive Changes

These Procedures acknowledge that a Non-Substantive change may be discovered at any point during or after the final development of the RRS or OP.

Non-Substantive Changes to an RRS shall be handled in accordance with the NERC Standards Development Manual or its successor.

Non-Substantive Changes to an OP shall be addressed using WECC's internal policies and practices. Non-Substantive changes for OPs do not require a comment / response cycle.

Step 7 – Submit Proposed Draft to the WSC with a Request for Ballot

Upon completion of the proposed RRS or OPs, the DT shall present the proposed RRS or OPs to the WSC with a request for ballot. The WSC shall address that request no later than its next regularly scheduled meeting.

After receiving a request for ballot, the WSC shall review the RRS or OP as presented and determine whether it fulfills the requirements stated in the SAR. The WSC shall also consider whether extrinsic requirements, such as FERC orders, Board directives, or other regulatory directives are met by the content of the document.

If the WSC concludes that the proposed RRS or OP is ready for ballot, the WSC shall forward the RRS or OP to WECC staff with a request that a Ballot Pool be formed from the Ballot Body, for the specific intent of seeking approval of the proposed RRS or OP. The results of the WSC's vote to forward the RRS or OP to the Ballot Pool shall be documented. Any WSC member that opposes submittal of the RRS or OP will be encouraged to provide dissenting comments, and if possible, specific language that would make the draft document acceptable to the dissenting member. If the WSC cannot reach agreement to submit the RRS or OP to the Ballot Pool, the WSC will report to and seek guidance from the Board.

If the WSC concludes that the proposed RRS or OP is not ready for ballot because it does not fulfill the requirements of the SAR or because it fails to meet other regulatory requirements or directives, the WSC shall remand the RRS or OP to the DT with a specific explanation identifying the deficiencies that must be remedied.

Upon receiving the remanded RRS or OP and explanation of deficiencies, the DT shall:

1) Redraft the RRS or OP accordingly;
2) Initiate iterative comment / response cycles as needed until it again concludes that no further Substantive Changes are needed; and
3) Return the proposed RRS or OP to the WSC for disposition.

Step 8 – Convene a Standards Briefing

Once the WSC approves submitting the RRS or OP to the Ballot Pool for ballot, WECC shall dispatch notice to the SEL that a Standards Briefing will be held to discuss the content of the proposed RRS or OP prior to balloting. Notice shall be provided 15 days or more before the Standards Briefing is to be held and shall provide, at a minimum, the following:

- Identification of the RRS or OP;
- The time and place of the Standards Briefing; and

- The location of the proposed RRS or OP and related documentation for review.

Step 9 – Form the Ballot Pool and Ballot the Standard

Any individual or entity seeking participation in the ballot of an RRS or OP shall apply to WECC for Ballot Body membership in any SVS in which it is eligible. WECC staff shall review the request and confirm eligibility to join the Ballot Body.

Decisions of the staff to approve, deny, or restrict the admission of an individual or entity to a voting sector may be appealed in accordance with the WECC Bylaws.

From the Ballot Body, a discrete Ballot Pool will be formed for each RRS or OP to be balloted under these Procedures. All members of the Ballot Body shall be provided an opportunity to opt into a Ballot Pool formed for purposes of voting on each RRS or OP. It is the Ballot Pool that votes on RRSs and OPs developed under these Procedures.

Notice that a Ballot Pool is forming will be dispatched via the SEL. That notice shall contain, at a minimum, the following information:

1) Identification of the RRS or OP;
2) The proposed action to be taken (e.g., Notice of Ballot Pool Formation / Notice of Ballot);
3) When the Ballot Pool will open;
4) When the ballot will take place;
5) How to cast a vote; and
6) The location of the proposed RRS or OP and related documentation for review.

The Ballot Pool registration window shall remain open for a period determined by WECC staff, but in no case shall the Ballot Pool registration window be open less than 15 days or more than 30 days.

Once notice of a Ballot Pool forming has been dispatched: 1) the ballot window shall commence no sooner than 15 days and no later than 45 days after that dispatch; and 2) no Substantive Changes may be made to the proposed document unless the revisions are posted for an iterative comment / response cycle and a new date is set for ballot.

Once the ballot window opens, no Ballot Body member may join or withdraw from the Ballot Pool. The WECC Director of Standards (DOS) may authorize deviations from this rule for extraordinary circumstances such as the death, retirement, or disability of a Ballot Pool member that would prevent an otherwise eligible entity from casting a vote during a given ballot window.

Voting on an RRS or OP shall be via electronic voting administered on the WECC website. The default voting window shall be a period of 15 days; however, the window may be held open up to a maximum of 60 days to reach a quorum. During a ballot window, WECC shall not sponsor or facilitate public discussion of the standard to be balloted.

Eligible members of the Ballot Pool may cast one vote in each SVS for which they are eligible.

Participating Stakeholders may only vote on an RRS if they have applied for and been granted Participating Stakeholder status. A Participating Stakeholder is only entitled to vote on an RRS and may only vote on a WECC Criterion if the proposed WECC Criterion could result in sanction to a non-WECC Member. A Participating Stakeholder is not entitled to vote on any other OP.

Each member of the Ballot Pool casting a negative vote on an RRS or OP will be required to provide a statement explaining the reason for the negative vote. The statement should include language that would make the RRS or OP acceptable. The statement will be included in the voting record for consideration by the WSC and the Board.

A two-thirds (2/3) quorum of the Ballot Pool is required for each vote. ~~Upon receiving the Draft Standard from the Drafting Team, the WSC shall decide whether to: (i) post the Draft Standard provided by the Drafting Team for comment; (ii) further revise or modify the Draft Standard provided by the Drafting Team, then post the WSC's revision for comment; (iii) return the Draft Standard to the Drafting Team for further work, as directed; or (iv) terminate the Standard development activity in accordance with the procedures for rejecting a SAR in Step 2. A majority (greater than 50 percent) vote of the authorized membership of the WSC is required to terminate a Draft Standard at this stage. If the WSC chooses to remand the draft back to the Drafting Team, the WSC chair shall provide the Drafting Team with the committee's reason for the remand and provide further guidance, as necessary.~~ Quorum shall be based on the total number of Ballot Pool members and shall not be based on the total number of votes cast. Abstentions and negative votes cast without an explanation shall not be counted for the purpose of determining consensus, but will be counted for purposes of obtaining a quorum.

~~If the WSC chooses to present the Draft Standard for comment, the WSC shall post the initial Draft Standard on the WECC website and provide 45 days for comments. Along with the draft, the WSC will post the impact assessment report and other supporting materials. The Draft Standard will include all mandatory requirements. In addition, the Draft Standard will include measurements, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs).[5] Notice of this posting and a solicitation for comments on the draft will be sent to all WECC members and all individuals who subscribe to the WECC standards e-mail list. In addition the notification of posting and solicitation for comments will be simultaneously noticed to NERC. The WSC may request input from affected parties regarding their estimated cost to implement the Draft Standard and may use that data to amend an impact assessment report, which will be posted for comment when it becomes available.~~

~~[5] Regional Criteria, which are also to be developed under this Procedure, will not contain VRFs of VSLs which are only necessary for Standards that will be enforceable and for which violations may result in penalties.~~

Members of electric industry organizations may respond through their organizations, or directly, or both. All comments will be supplied electronically and will be posted on the WECC website.

Step 5 – WSC Deliberates on Comments

The WSC chair is responsible for ensuring that comments are addressed in a timely manner. The WSC may further employ and oversee the Drafting Team for purposes of analyzing and responding to comments. The WSC will post its response to comments on the WECC website within 30 days of the close of the comment period. All parties that submit comments are strongly encouraged to participate in WSC deliberations.

If the WSC determines, by majority vote, any technical comments including those on the draft or the impact assessment report are significant, it will repeat Steps 3 and 4 as many times as considered necessary to ensure adequate opportunity for interested stakeholder input. All interested stakeholders are strongly encouraged to submit their comments as early in the process as possible. The number of days for comment on each subsequent revision to the Draft Standard will be 30 days.

A majority vote of the WSC is required to approve submitting the recommended Draft Standard to the Ballot Body for a vote. Balloting results will be documented. All WSC member dissenting voters, as well as others participating in the WSC deliberations, will be encouraged to provide dissenting comments and, if possible, specific language that a party believes would make the Draft Standard acceptable. If the WSC vote fails to capture a simple majority to approve submittal to the Ballot Body for a vote, and there is no apparent way to reach a majority agreement, the WSC will report to and seek guidance from the WECC Board.

Step 6 – WSC Submits Draft Standard for Ballot Body Vote and Ballot Pools Are Established

The WSC's final Draft Standard will be posted on the WECC website at least 30 days prior to the commencement of the voting window and WECC members and Participating Stakeholders who have joined the Ballot Body[6] will be notified of the WSC's recommendation. The posting will include the final WSC member vote, any dissenting WSC member comments, a summary addressing comments that were not incorporated into the Draft Standard, the impact assessment report and the period of time during which the Ballot Body is scheduled to vote on the WSC's recommendation.[7]

[6] Each WECC Member and Participating Stakeholder shall be permitted to designate a person who is authorized to join Ballot Pools for Standards and to either cast a vote within those Ballot Pools or designate a proxy to cast the vote of the WECC Member or Participating Stakeholder. Each such designated person shall be provided a user name and password for use in electronically identifying that entity's authorization to act within the Ballot Body. The Ballot Body will be renewed every five years as part of WECC's section 4.9 review.

[7] The period of time the vote is scheduled shall take into account the next scheduled Joint Session of the Standing Committees.

Notice of the posting also will be sent to the Standing Committees, all Participating Stakeholders, and the standards email list. In addition, the notification of the posting for ballot will be simultaneously noticed to NERC.

After posting of the Draft Standard, the Standing Committees shall participate in at least one Joint Session addressing the Draft Standard. In addition to the Joint Session, individual Standing Committees may undertake additional discussions or webinars.

The notice shall solicit participants for the Ballot Pool for the final Draft Standard scheduled for a vote. Members of the Ballot Body choosing to vote on the Draft Standard shall respond to the WSC's solicitation for Ballot Pools within a period designated by WECC Staff. Responses from Ballot Body members shall indicate within which WECC Standards Voting Sector(s) the party chooses to vote. Where a WECC member or Participating Stakeholder is eligible for multiple WECC Standards Voting Sectors, it may vote in any or all of its eligible sectors as allowed pursuant to the Bylaws (section 8.5.5.2) and this Reliability Standards Development Process. Based on responses to the Ballot Pool solicitation, WECC staff shall form the Ballot Pool for a particular Draft Standard.

Step 7 – Ballot Pool Vote on Recommendation to Board

In accordance with Sections 8.5 and 8.6 of the WECC Bylaws, the Ballot Pool will vote on the Draft Standard. Voting shall begin at least seven (7) calendar days following the Joint Session of the Standing Committees at which the Draft Standard was considered. Voting on Draft Standards shall be via electronic voting administered by the WECC website, and shall take place over a fifteen (15) business day voting window. Each WECC member or Participating Stakeholder may cast one vote in each eligible voting sector. Voters rejecting the Draft Standard will be required to provide an explanation of their vote. Explanations will be added to the record in order to assist the WSC's and/or the Board's subsequent consideration of the Draft Standard.[4]

A weighted majority vote of the Ballot Pool is required for a Draft Standardan RRS or OP to be approved by the WECC membership and Participating Stakeholders.. Voting among the WECC Standards Voting Sectors will be SVSs shall be weighted as follows:

- For each SectorSVS with ten10 or more voters, the number of affirmative votes cast shall be divided by the sum of the affirmative and negative votes cast to determine the fractional affirmative vote for that Sector. Abstentions, incomplete votes, and non-responses shall not be counted for the purposes of determining the number of voters in the SectorSVS.

- For each SectorSVS with less than ten10 voters, the same process shall be used to determine the fractional affirmative vote, but the fractional affirmative vote of that SectorSVS shall be multiplied by ten10 percent (10%) times the number of voters. E.g.,

  - For example, for a SectorSVSs with nine voters, the fractional affirmative vote will be multiplied by ninety90 percent (90%). Abstentions, incomplete votes, and non-responses shall not be counted for the purposes of determining the number of voters in the Sector..

- The sum of the fractional affirmative votes from all ~~Sectors~~SVSs divided by the weighted number of ~~Sectors~~SVSs voting shall be used to determine if a weighed majority has been achieved~~. A Sector~~ and whether the RRS or OP has been approved. An SVS shall be considered as voting if any member of the ~~Sector~~SVS in the Ballot Pool casts either an affirmative or a negative vote. ~~-~~If there are more than ten voters in the ~~Sector~~SVS, the weighting used for the calculation of "weighted sectors voting" shall be ~~one hundred~~100 percent ~~(100%).~~. For ~~Sectors~~SVSs with less than ten voters, the weighting used for the calculation of the "weighted sectors voting" shall be ~~ten~~10 percent ~~(10%)~~ per voter. ~~Abstentions, incomplete votes, and non-responses~~

- ~~An RRS or OP~~ shall ~~not~~ be ~~counted for the purposes of determining the number of voters per Sector.~~

- ~~A Standard shall be~~deemed approved by the Ballot Pool if the sum of fractional affirmative votes from all ~~Sectors~~SVSs divided by the weighted number of voting ~~Sectors~~SVSs is a majority (i.e~~.~~., greater than ~~fifty~~50 percent ~~(50%)).~~).

~~A two-thirds (2/3) quorum of the Ballot Pool is required for each vote. Abstentions and incomplete responses will be counted in determining whether a quorum of the Ballot Pool is achieved. Quorum shall be based on total number of Ballot Pool members, and shall not be based on total number of votes cast. If necessary, the voting window may be extended by the WSC until a quorum is achieved.~~

After a vote by the Ballot Pool, the WSC ~~will~~shall take one of the following actions~~:~~.

~~(1)~~ If the Ballot Pool approves ~~a Draft Standard~~an RRS or OP, the WSC shall submit the ~~recommended Draft Standard~~RRS or OP to the ~~WECC~~ Board~~.~~ for approval. The WSC shall provide ~~the Draft Standard, any comments on which the WSC members did not agree, minority opinions of WSC members, explanations supporting votes in opposition to the Draft Standard, and the impact assessment for the Draft Standard~~voting results to the Board ~~for~~, including the final ~~approval. To be considered by the Board,~~ ballot results and any rationale supporting any ~~"no" votes by a WSC member on a Draft Standard shall be accompanied by a text explaining the "no" vote and, if possible, should provide specific language~~negative votes cast.

Any RRS or OP that ~~would make the Draft Standard acceptable. Relevant voting information from the Ballot Pool shall be submitted to the Board for its consideration in determining whether or not to approve the Draft Standard. Final Draft Standards and all materials~~was provided to the Board for approval will be posted ~~no less than 30 days prior to the Board vote.[8] The date of the expected Board vote will also be posted.~~for Board review for at least the period mandated by the WECC Bylaws.

~~[8] WECC Bylaws, Section 7.5.1 – "Except as set forth in Section 7.5.2 regarding urgent business, all regular business of the Board will occur at the Board meetings, at least twenty-one (21) days' advance notice of which has been provided…"~~

~~(2) If the Ballot Pool rejects a Draft Standard, the WSC may, by a majority vote (greater than 50 percent of the WSC membership), decide to amend or modify the initial Draft Standard or remand it back to the Drafting Team to amend or modify it. Any amended or modified Draft Standard must be resubmitted to the Ballot Pool for a vote before the WSC submits the subsequent Draft Standard to the WECC Board. If the WSC determines by majority vote (greater than 50% of the WSC members) that the modifications to the Draft Standard could be unanticipated by the Ballot Pool or may be controversial, the amended or modified Draft Standard shall be subjected to an additional Joint Session discussion prior to voting. The reasons for the modification(s) will be documented, posted, and provided to the Board. If any changes are made at the WSC meeting, the roll call of votes for and against the subsequent Draft Standard and abstentions will be recorded at the meeting, and the subsequent Draft Standard will be posted for 10 days for comments. The comments will be posted and distributed to the Ballot Pool and will be made available prior to any subsequent rounds of voting. Unless otherwise directed by the WSC, the Ballot Pool for subsequent votes on a Draft Standard shall consist of the same parties.~~

~~(3) If the Ballot Pool rejects a Draft Standard, the WSC may allow the Draft Standard to terminate.~~

If the Ballot Pool rejects the RRS or OP, the SAR shall be deemed complete and all associated documents shall be archived, except as allowed in the Regulatory Directive section of these Procedures.

Step ~~8~~ 10 – Initiate the Appeals Process – If Needed

~~Requests for reconsideration of WSC decisions may be made to the WSC. The WSC will post its findings. The subsequent rejection of such a request by the WSC may be appealed to the Board.~~

~~A Draft Standard recommended by the WSC may be appealed on either technical or due process grounds. Any due process or technical appeals must be submitted, in writing, to the WECC staff within 15 days of the date the WSC posts a recommendation.~~

~~An appeal to the Board shall be posted on the WECC website and shall be heard at the Board's next regularly scheduled meeting occurring at least 21 days after the appeal is filed.~~

~~Step 9 – Board Approval~~

~~The WECC Board of Directors will consider the proposed Draft Standard no later than at its next~~

~~meeting occurring at least 30 days after the Ballot Pool vote. The Board will consider the WSC's~~ An appeal may be brought on the basis of either a technical (reliability) concern or a due process (procedural) concern.

If the appeal is based on technical grounds, that appeal may be brought at any stage of the development process prior to the opening of a ballot window. The appeal shall be submitted to the DOS who shall place the appeal on the agenda of the next regularly scheduled WSC meeting. If the appellant does not concur with the WSC's findings, the appellant may request that the DOS forward the matter to the Board for disposition.

If the appeal is based on due process concerns, the appellant shall submit the matter to the DOS no later than 30 days after the alleged occurrence of the due process violation, but in no case shall an appeal on due process grounds be accepted more than 30 days after the RRS or OP has been approved by the Ballot Pool. The appeal shall be submitted to the DOS who shall place the appeal on the agenda of the next regularly scheduled WSC meeting. If the appellant does not concur with the WSC's findings, the appellant may request that the DOS forward the matter to the Board for disposition.

The filing of an appeal shall not halt the development process; however, the appeal shall be settled by the Board before the Board votes to approve the RRS or OP.

Step 11 – Obtain Board Approval

The Board shall consider the RRS or OP for approval no later than at its next regularly scheduled meeting after the close of the Ballot Pool window and recommendation for approval by the WSC, subject to the notice requirements in the WECC Bylaws.

Any person or entity may submit comments to the Board for the Board's consideration. The Board shall consider:

1) All comments submitted for its consideration;
2) The WSC's recommendations and minority opinions, ~~all~~if any;
3) All comments that were not incorporated into the ~~draft Standard~~RRS or ~~revision(s),~~OP;
4) Voting results including, at a minimum, the final ballot results and ~~the impact assessment report. The~~ any rationale supporting negative votes; and
5) Any other supporting documentation.

If an OP is approved by the Board, WECC shall post the final OP on its website and the SAR will be deemed complete. The effective date will be that approved by the Board.

If an RRS is approved by the Board, WECC shall forward the RRS to NERC for NERC and FERC disposition.

If the RRS or OP is not ~~amend or modify~~approved by the Board, the Board may either deem the SAR complete or remand the RRS or OP to the DT with specific guidance as to proposed changes.

If the RRS or OP is remanded, any Substantive Changes must be vetted in accordance with these Procedures. Under no circumstances shall the Board make Substantive Changes to the RRS or OP, except in accordance with its backstop authority as authorized by the WECC Bylaws.

Step 12 – Submit RRSs for ERO Review, FERC Approval & Implementation of WECC Regional Reliability Standards

Note: Step 12 only applies to RRSs.

All new, revised, or retired RRSs shall be submitted to NERC for NERC and FERC approval. The approval, revision or retirement of an RRS shall not be effective in the United States until approved by FERC and shall not be effective in another jurisdiction until approved by the applicable governmental authority.

Step 13 – Retire an OP

Upon determining that the subject matter of an OP is duplicated in a NERC Reliability Standard, and that retirement of the OP will not cause a reliability gap after the effective date of the associated NERC Reliability Standard, the WSC may retire a WECC OP on its own initiative without further due process.

Step 14 – Submit a ~~Draft Standard, except to make nonmaterial changes to the language~~Request for Interpretation

A Request for Interpretation (RI) of a ~~Standard or revision thereto. If approved, the Standard will be posted on the WECC website and all parties notified.~~
~~If~~ the Draft Standard is not approved, the Board may return the Draft Standard to the WSC for further work, or the Board may terminate the Standard activity with an appropriate notice and explanation to the SAR requester, WSC, and participants in the Ballot Pool. These Board actions will also be posted.

~~A majority vote of the Directors present at a Board meeting, as specified in Sections 7.2 and 7.4.1 of the WECC Bylaws, is required to approve the recommended Standard.~~

~~**Step 10 – ERO Review, FERC Approval and Implementation of Reliability Standards**~~

~~To the extent required under Section 215 of the Federal Power Act, 18 C.F.R. Part 39, and according to procedures established in the delegation agreement between WECC and the Electric Reliability Organization ("ERO"), the Board shall submit new Reliability Standards, revisions to existing Reliability Standards, and terminations of existing Reliability Standards for review by the ERO and approval by FERC. Upon approval by FERC, the Reliability Standards will be made part of the body of NERC reliability standards and enforced upon all applicable bulk power system owners, operators, and users within the WECC region. Parties' right to participate in the ERO and FERC review processes shall be as established in the applicable regulations and the ERO/WECC delegation agreement. Reliability~~

Standards subject to ERO review shall become effective as approved by FERC or, for entities outside of the U.S. portion of the Western Interconnection, upon approval by the applicable Canadian or Mexican authorities.

Step 11 – Implementation of Standards Not Subject to ERO/FERC/Other Approval

All new and modified Standards not subject to ERO review and FERC, Canadian or Mexican approval as provided in Step 10 shall become effective as ordered by the WECC Board. As of the effective date of such new or modified Standard, all industry participants in the Western Interconnection that such Standard is applicable to are expected to implement and abide by the Standard. Any and all parties to this Process retain the right of appeal to other authorities as the law allows.

Expedited Process for Urgent Action **Interim Standards** document developed under these Procedures

In cases requiring urgent action, such as in the development of emergency operating procedures, any Standing Committees or Participating Stakeholders may propose a new or modified interim Standard for approval by the WECC Board through a process that eliminates any or all of the steps outlined above, but only to the extent necessary, and only in a manner that is consistent with the WECC Bylaws. Such interim Standard shall be replaced by a Board-approved permanent Standard, developed using all the steps identified in this document within one year (or such additional time as may reasonably be required to complete all steps) from the date on which the WECC Board approved the interim standard. An interim Standard may be converted to a successor permanent Standard as long as any procedural steps bypassed in developing the interim Standard are completed with respect to the permanent Standard. If necessary, the Board may renew an interim Standard to allow additional time for the development of a successor permanent Standard. Renewal may occur more than once, but a good faith effort must be made to develop a successor permanent Standard.

Interpretation of Regional Standards and Regional Criteria

Any entity may request an interpretation of a Standard by sending a request through the WECC web portal identifying the Standard and requirement or requirements for which additional clarity is sought. The request shall indicate the material impact to the requesting entity or others caused by the actual or potential lack of clarity. An interpretation is limited to clarifying existing requirements in the approved Standards. Interpretationsdocument and may not be developed that expand upon a requirement or that provide guidance on how to applyimplement a requirement.

The WECC Staff shall review the request for clarity and completeness and shall work with the requestor to clarify the request or complete any missing elements of the request if needed. The WECC Staff shall forward the request to the WSC. If the WSC believes that the request is intended to change a requirement or is seeking feedback on how to apply a requirement, rather than interpret the requirement, the request shall be denied and returned to the requestor with an explanation. If denied, the requestor shall be advised of the appeals process.

The RI is initiated by submitting WECC's online SAR form. The SAR shall: 1) identify the specific document; 2) identify the requirement within that document for which an interpretation is being requested, and 3) specify the perceived lack of clarity. The SAR shall indicate the material impact to the requesting entity or others caused by the perceived lack

of clarity.

The RI is processed using the same process set forth in these Procedures with the following exceptions:

The chair of the WSC

- ~~Within 21 days of receiving the request, the WSC Chair~~ shall assemble an Interpretation Drafting Team (IDT~~)~~). The IDT shall be composed of SMEs with ~~the~~ relevant expertise to address the clarification~~. The IDT~~ and, to the extent possible, should include members ~~from~~of the original ~~Standard Drafting Team to the extent possible, and may be supplemented as deemed appropriate by the WSC Chair, but shall not contain any members~~ DT. The IDT shall not include any team member representing the entity that ~~submitted the request.~~filed the RI; however, this prohibition does not preclude representatives of the filing entity from participating in the development process.

~~As soon as practicable, but not more than 45 calendar days after the WSC assembles the IDT, the IDT shall draft a written interpretation to the Standard providing the requested clarity. The interpretation shall be posted for a 30-day formal comment period. The IDT shall then have 15 days to respond to the comments and to make any changes to the interpretation. The IDT shall reach a determination on the language for an interpretation by majority vote of the IDT. The IDT shall then return the interpretation to the WSC which shall then post the interpretation for another 30 days to give entities time to review the interpretation prior to a Ballot Pool vote. Notice of this posting will be sent to the Ballot Body, and the notice shall solicit participants for the Ballot Pool for voting on the interpretation. After posting of the interpretation, the Standing Committees shall participate in at least one Joint Session addressing the interpretation. Voting on the interpretation shall be consistent with the quorum and weighted voting procedures explained in Step 7 of these Reliability Standards Development Procedures. Use of a conference call or web meeting and electronic or email balloting is encouraged to shorten the interpretation process. If the interpretation is approved by a weighted majority of the Ballot Pool, the WSC shall forward the interpretation to the WECC Board of Directors for approval. If the Ballot Pool rejects the interpretation, the WSC shall notify the requestor. The WSC shall also ask the IDT to provide a revised interpretation.~~

- ~~Interpretations of Regional Standards shall be~~ If all of the document is to be subsumed into the new PSS RRS the PSS DT should recommend to the Standing Committee that the document be retired as of the effective date of the replacement document.

Once an interpretation of an RRS has been approved by the Board, the interpretation shall be appended to the RRS and submitted to NERC for ~~processing with a request that the interpretation be adopted by the~~ NERC ~~Board of Trustees and then filed for approval with~~ and FERC ~~and applicable Governmental Authorities in British Columbia, Alberta and Mexico.~~approval.

- ~~For~~ ~~entities operating in the United States, once the interpretation of a Regional Standard is approved by FERC, the interpretation shall become effective and shall be appended to the Standard. For entities outside of the U.S. portion of the Western Interconnection, interpretations shall become effective for these entities only upon approval by the appropriate Canadian or Mexican regulatory authority.~~ The interpretation will remain appended to the ~~Standard~~RRS until such time as the ~~Standard is revised through the normal process incorporating the clarifications provided by the interpretation~~RRS is revised and the

interpretation's content is addressed during the revision process. RRS interpretations shall not be effective in the United States until approved by FERC and shall not be effective in other jurisdictions until approval by the applicable governmental authority.

Supporting Processes

Expedited Process for Urgent Action

In cases requiring urgent action, such as in the development of emergency procedures, any person or entity may propose an interim RRS or OP for approval by the WECC Board. The RRS or OP must go through a process that eliminates any or all of the steps outlined previously, but only to the extent deemed necessary by the Board and only in a manner that is consistent with the WECC Bylaws.

If the Board approves the interim document, it shall establish an initial effective date for the interim document.

Within 90 days after the initial effective date of the document, the Board shall either:

1) Cause a SAR to be submitted requesting the development under these Procedures of a permanent replacement to the interim document; or
2) Shall extend the applicability of the interim document for an additional 90 days.

Renewal may occur more than once, but a good faith effort must be made to develop a permanent replacement under these Procedures.

If a SAR is submitted, the interim RRS or OP shall remain in effect until the permanent replacement RRS or OP becomes effective.

If a SAR is not submitted and the interim RRS or OP has not been extended, the interim RRS or OP shall be deemed retired.

Regulatory Directives
~~Special Procedures for Addressing Regulatory Directives~~

These Procedures acknowledge that FERC may order WECC to make specified regulatory changes to documents created under these Procedures. For the purpose of this section only, those documents are referred to as Directive Regional Reliability Standards (DRRS).

If the Board determines that ~~the WECC Standards Process did not~~ these Procedures failed to result in a ~~proposed Draft Standard that addresses a directive issued by the FERC or by a Mexican or Canadian~~DRRS meeting the mandated regulatory ~~authority (Applicable Regulatory Authority), hereinafter, "regulatory directive," then~~changes, the Board shall have authority to take ~~certain~~the following actions to ensure that ~~a Draft Standard~~ the DRRS is responsive to the regulatory

directive ~~is drafted, approved and/or submitted to the Applicable Regulatory Authority.[9] The Board shall have the authority to choose which one or more of the actions set out below are appropriate to the circumstances and need not take these actions in sequential steps.~~ .

~~1. Board Remand to the WSC after an Affirmative Vote of the~~ If the Ballot Pool~~. If the Board is presented with~~ approves a ~~Draft Standard~~DRRS that ~~fails to~~does not address a regulatory directive required to be included in that document, the Board may remand ~~to the WSC the proposed Draft Standard with instructions (including establishing a timetable for action).~~

~~2. Board Remand to WSC for Additional Public Consideration and Re-ballot. Upon a written finding by the Board that a Ballot Pool has failed to approve a Draft Standard that contains a provision to address a specific matter identified in a regulatory directive, the Board has the authority to remand the Draft Standard to the WSC with instruction to (i)~~ the DRRS to the original DT or instruct the WSC to convene a ~~public technical conference~~new DT to ~~discuss~~redraft the ~~issues surrounding~~document. The Board shall instruct the DT on the specific regulatory directive~~, including whether or not the Draft Standard is just, reasonable, not unduly discriminatory or preferential,~~ that must be contained in the ~~public interest, helpful to reliability, practical, technically sound, technically feasible, and cost-justified; (ii) working with WECC staff, prepare a memorandum discussing the issues, an analysis of the alternatives considered and other appropriate matters; and (iii) re-ballot the Draft Standard one additional time, with such adjustments in the schedule as are necessary complete a re-ballot of the Draft Standard within forty-five (45) days of the remand. The WSC memorandum shall be made available to the Ballot Pool in connection with the re-ballot. In any re-ballot, negative votes without comment shall be counted for purposes of establishing a quorum, but only affirmative votes and negative votes with comments related to the Draft Standard shall be counted for purposes of determining the number of votes cast and whether the Draft Standard has been approved by the Ballot Pool.~~

~~3. Affirmative Vote upon Re-ballot of Draft Standard. If the re-balloted Draft Standard achieves an affirmative majority vote of the Ballot Pool, with a quorum established, then the Draft Standard shall move to the Board for approval.~~

~~4. Negative Vote upon Re-ballot of Draft Standard. If the re-balloted proposed Draft Standard fails to achieve an affirmative majority vote of the Ballot Pool, or if a quorum~~redraft. Once the DRRS is ~~not established, then the Board has the authority to consider the Draft Standard for approval pursuant to the following:~~redrafted it shall be reprocessed under these Procedures.

~~(i) The Board~~ If the Ballot Pool rejects a DRRS or fails to ballot the DRRS due to failure to reach a quorum, either when first presented for ballot or during an iterative redraft as instructed by the Board, the Board shall ~~issue notice of its intent to consider the Draft Standard~~review the DRRS, including all comments provided and ~~shall solicit written public comment particularly focused on the technical aspects of the provisions of the Draft Standard~~ all rationale accompanying any negative vote.

~~[9] The procedures in this section, "Special Procedures for Addressing Regulatory Directives," only apply to draft Regional Reliability Standards.~~

Upon a finding that address the specific matter identified inDRRS was rejected for reasons not related to the regulatory directive, including the Board may direct WECC staff to file a new SAR with the specific narrow scope of addressing only the regulatory directive. The Board may suggest specific language for inclusion in the proposed DRRS.

Upon a finding that the DRRS was rejected based on language addressing the regulatory directive, the Board shall take the following steps to meet its regulatory obligation:

1) Review the entire record of development.
2) Require a public technical conference to be noticed and convened to determine whether or not the Draft Standardrejected DRRS is:
   - just, and reasonable,;
   - not unduly discriminatory or preferential,;
   - in the public interest,;
   - helpful to reliability,;
   - practical,;
   - technically sound,;
   - technically feasible, and ;
   - cost-justified.; and

(ii) The Board may convene a public technical conference to receive additional input on the matter.

(iii) After considering the developmental record, the comments received during balloting and the additional input received under (i) and (ii), the Board has authority to act on the Draft Standard. If the Board finds that the Draft 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 the Board has authority to approve the Draft Standard and direct that it be filed with the Applicable Regulatory Authority with a request that it be made effective. If the Board is unable to find that the proposed Draft 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 direct that the Draft Standard and complete developmental record, including the additional input received under (i) and (ii), be submitted to the Applicable Regulatory Authority, as a compliance filing in response to the order giving rise to the regulatory directive, along with a recommendation that the Draft Standard not be made effective and an explanation of the basis for the recommendation.

5. Board Approval or Rejection of a Draft Standard Prepared by the WSC or WECC Staff and Not Balloted. Upon a written finding by the Board that the WSC has failed to develop, or a Ballot Pool has failed to approve, a Draft Standard that contains a provision to address a specific matter identified in a regulatory directive, the Board has the authority to direct the WSC (with the assistance of stakeholders and WECC staff) to prepare a Draft Standard that addresses the regulatory directive, taking account of the entire developmental record pertaining to the matter. If the WSC fails to prepare such Draft Standard, the Board may direct WECC management to prepare such Draft Standard. As part of this process, the Board may convene a public technical conference to receive input on the matter. The Draft Standard shall be posted for a forty-five (45) day public comment period. After considering the entire developmental record, including any comments received during the public comment period, the Board may do one of the following:

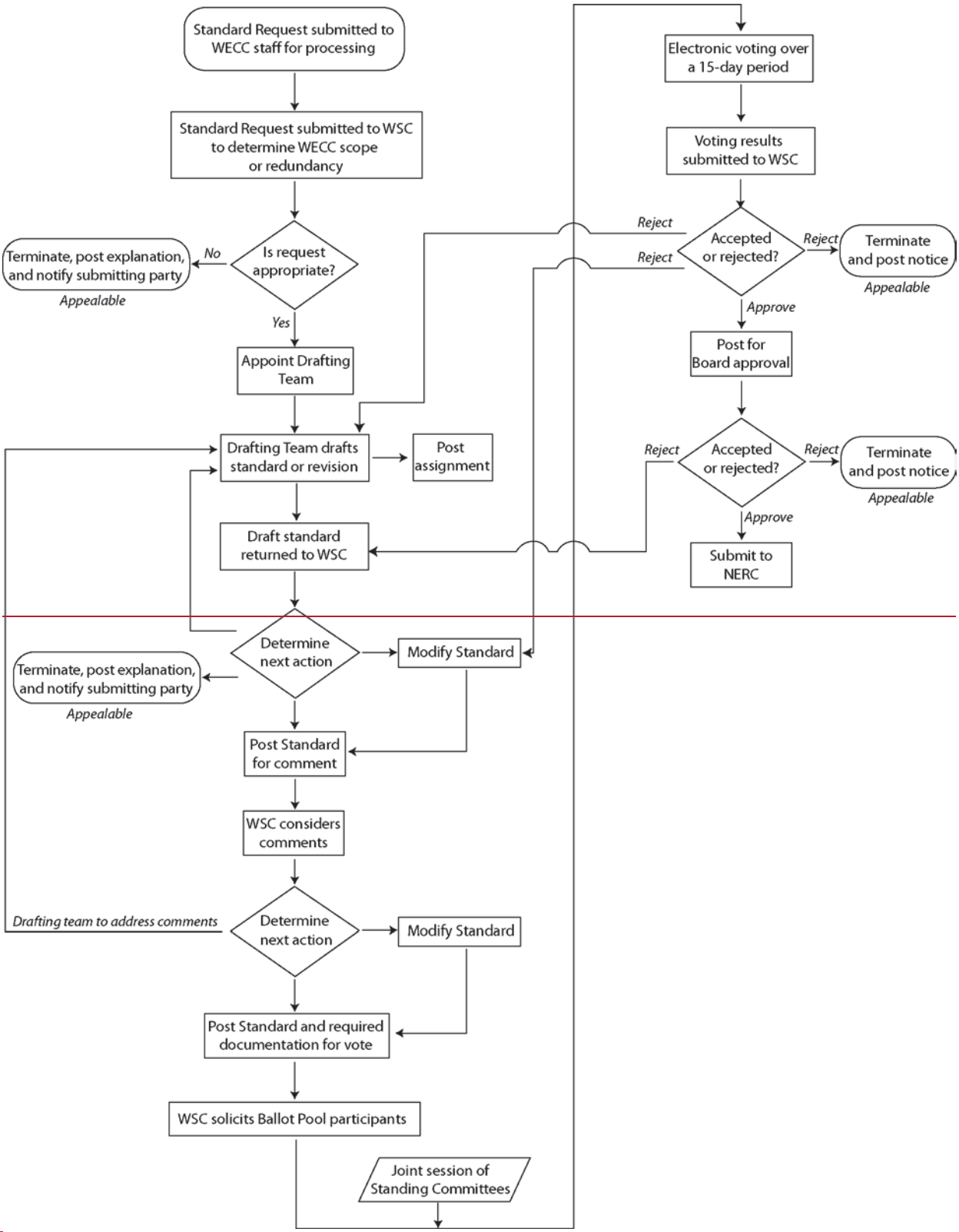
(i) The Board may find that the Draft Standard, with such modifications as the Board determines are appropriate in light of the comments received, is just, reasonable, not unduly discriminatory or preferential, and in the public interest, considering (among other things) whether it is practical, technically sound, technically feasible, cost-justified and serves the best interests of reliability of the bulk power system. In this case, the Board has the authority to approve the Draft Standard and direct that the proposed Standard be submitted to the Applicable Regulatory Authority with a request that the Draft Standard be made effective.

(ii) The Board may be unable to find that the Draft Standard 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. In this case, the Board has the authority to direct that the Draft Standard and the complete developmental record be filed as a compliance filing in response to the regulatory directive with the Applicable Regulatory Authority, with a recommendation that the Draft Standard not be made effective.

WECC shall on or before January 31st of each year file a report with the FERC on the status and timetable for addressing each outstanding directive to address a specific matter received from FERC.

Approved by the WECC Board June 22, 2011.

~~***STANDARDS DRAFTING PROCEDURES FLOWCHART***~~



- meets the regulatory directive (hereafter "Just and Reasonable").

3) Determine whether the DRRS should be implemented as drafted, notwithstanding

rejection by the Ballot Pool.

Upon a finding that the rejected DRRS should be implemented, the Board shall approve the DRRS and direct that it be submitted to NERC for NERC and FERC approval, as required.

Upon a finding that the rejected DRRS should not be implemented, the Board may submit the DRRS and its record of development as a regulatory compliance filing in response to the regulatory directive. The filing shall include a recommendation that the DRRS not be made effective and an explanation of the basis for that recommendation.

Maintenance of the Procedures

The WSC is charged with maintenance of these Procedures. Proposed changes to these Procedures shall first be brought to the WSC for consideration. The WSC may initiate proposed changes on its own initiative.

If it determines that a change to these Procedures should be pursued, the WSC shall draft the proposed changes and post the proposed changes to the WECC website for comment, accompanied by a notice to the SEL soliciting comments on the proposed changes.

The WSC shall consider all comments received and shall redraft the proposed changes as it deems necessary. Once the WSC approves the proposed changes, those changes shall be submitted to the Board for approval. Changes to these Procedures approved by the Board shall be submitted to NERC for NERC and FERC approval.

Maintenance of RRS and OPs Documents

The WSC shall ensure that each RRS is reviewed at least once every five years from the effective date of the most recent version of the RRS. If the review identifies needed changes, the WSC shall cause a remedial SAR to be filed. If the review does not identify needed changes, the WSC shall communicate its decision via the SEL and no further action will be required.

Review of OPs shall be conducted in accordance with internal WECC policies and procedures.

Attachment 3

Amended Exhibit of the Delegation Agreement Between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council

Clean Version

BYLAWS

OF

THE

WESTERN ELECTRICITY COORDINATING COUNCIL

TABLE OF CONTENTS

1. Vision and Mission. 1
   1.1 Vision.... 1
   1.2 Mission 1
2. Furtherance of WECC's Mission....1
   2.1 Activities to Carry Out WECC's Mission. 1
   2.2 Organizational Characteristics.... 3
3. Definitions....4
   3.1 Affiliate.... 4
   3.2 Annual Meeting. 4
   3.3 Applicable Regulatory Authority. 4
   3.4 Backstop Authority.... 4
   3.5 Balancing Authority. 5
   3.6 Ballot Body.... 5
   3.7 Board of Directors (Board).... 5
   3.8 Class.... 5
   3.9 Commercial Practices. 5
   3.10 Compliance Hearing Body. 5
   3.11 Delegation Agreement.... 5
   3.12 Director.... 5
   3.13 Electric Line of Business.... 6
   3.14 Electric Reliability Organization (ERO). 6
   3.15 Entity. 6
   3.16 FERC. 6
   3.17 Grid Operating Entity. 6
   3.18 International Reliability Agreement. 6
   3.19 Local Regional Entity.... 6
   3.20 Market Interface. 6
   3.21 Material External Impacts (MEI). 6
   3.22 Member.... 6

3.23 Participating Stakeholder. 7
3.24 Primary Authority. 7
3.25 Regional Criteria. 7
3.26 Regional Entity (RE). 7
3.27 Registered Entity. 7
3.28 Reliability Management System. 7
3.29 Reliability Standard. 7
3.30 Reliability Standards Development Procedures. 7
3.31 Transmission Facilities. 7
3.32 Western Interconnection. 8
4. Members and Membership. 8
4.1 Voluntary Membership. 8
4.2 Eligibility for Membership. 8
4.3 Designation of Membership Class. 9
4.4 Changes in Membership Class. 9
4.5 Affiliates and Distinct Business Entities. 9
4.6 Rights and Obligations of Membership. 10
4.7 Limitations on Member Obligations. 11
4.8 Compliance and Enforcement. 12
4.9 WECC Structure and Governance Review. 12
5. Procedures for Member Decisions. 13
5.1 Quorum and Alternative Voting. 13
5.2 General Membership Meetings. 13
5.3 Annual Member Meetings. 14
5.4 Special Member Meetings. 14
5.5 Member Class and Subclass Meetings 14
5.6 Notice of Member Meetings. 14
5.7 Open Meetings. 15
5.8 Policymaking Authority. 15
5.9 Minimum Participation Requirement. 15
6. Governance. 15

6.1 Board of Directors. 15
6.2 Composition of the Board and Board Member Qualifications. 15
6.3 Term of Office. 18
6.4 Nomination, Selection and Compensation of Directors. 18
6.5 Removal of Directors 20
6.6 Resignation. 21
6.7 Procedures for Filling Vacant Director Positions. 21
6.8 Duties of Directors 22
6.9 Powers of Directors. 22
6.10 Delegation of Board Authority. 22
7. Procedures for Board Decisions 23
7.1 Quorum. 23
7.2 Majority Vote. 23
7.3 Attendance at Board Meetings by Teleconference. 23
7.4 Board Action by Unanimous Consent. 23
7.5 Notice of Board Meetings 24
7.6 Open Meetings. 25
7.7 Board Committees. 26
8. Member Committees. 26
8.1 Purpose. 26
8.2 Standing Committees. 26
8.3 Other Committees. 28
8.4 [Repealed] 28
8.5 Procedures for Member Advisory Committee Decision-Making 28
8.6 Procedures for Committees other than the Member Advisory Committee. 33
8.7 Procedures for Developing and Voting on Reliability Standards 36
8.8 Notice of Committee Meetings 37
8.9 Open Meetings. 37
9. The Chief Executive Officer, Officers, and Employees. 37
9.1 Designation of Officers and Terms of Office. 37
9.2 Chief Executive Officer Qualifications. 38

9.3 Standards Applicable to All Employees. 38
9.4 Employment. 38
9.5 Chief Executive Officer's Duties. 38
9.6 Secretary's Duties. 39
10. Dispute Resolution. 39
11. Costs and Finances. 39
11.1 Funding of Reliability Activities. 39
11.2 Dues. 40
11.3 Funding of Non-Statutory Activities. 41
12. Amendments to these Bylaws. 41
12.1 Amendment by the Board. 41
12.2 Amendment by the Members. 41
12.3 Amendments in Response to Mandatory Membership 42
12.4 Amendments proposed by FERC. 42
13. Termination of Organization 42
14. Miscellaneous Provisions 42
14.1 Limitation on Liability 42
14.2 Indemnification. 42
14.3 No Third Party Beneficiaries. 43
14.4 Informal Inquiries for Information. 43
15. Incorporation. 43
16. Governing Law. 43
17. WECC Transition 43
17.1 Board of Directors transition. 44
17.2 Transition Exceptions 44
17.3 Member Advisory Committee transition 44

APPENDICES:

A. Board Member Standards of Conduct

B. Officers and Employees Standards of Conduct

C. WECC Dispute Resolution Procedures

BYLAWS

Of

The

WESTERN ELECTRICITY COORDINATING COUNCIL

1. Vision and Mission.

1.1 Vision.

The Western Electricity Coordinating Council ("WECC") shall seek to achieve the appropriate level of Bulk Electric System reliability at least cost considering all costs throughout the economy.

1.2 Mission

WECC is a Utah nonprofit corporation with the mission to foster and promote reliability and efficient coordination in the Western Interconnection. WECC will lead the stakeholders in the Western Interconnection to achieve appropriate system reliability, be the premier source of unbiased information, and serve as the trusted thought leader for the Western Interconnection by providing, consistent with these Bylaws: 1) impartial independent review and analysis of reliability issues impacting the Western Interconnection 2) development of electric reliability standards incorporating Western Interconnection experience and knowledge; 3) consistent and fair monitoring and enforcement activities for compliance with reliability standards; 4) event analysis and lessons-learned from system events; and 5) value for its membership through cost effective and efficient services and practices through: a) being a centralized repository of reliable information relating to the planning and operation of the Bulk Electric System in the Western Interconnection, b) coordinating system planning and modeling, c) sharing of, and providing comment on adherence to, recognized industry best practices, d) facilitating resolution of market seams and coordination issues, e) secure sharing of critical reliability data, and f) providing a robust stakeholder forum.

2. Furtherance of WECC's Mission

2.1 Activities to Carry Out WECC's Mission.

2.1.1 Compliance with the Federal Power Act. WECC will carry out responsibilities and exercise rights of a Regional Entity organized on an interconnection-wide basis pursuant to Section 215 of the Federal Power Act, including any responsibilities and rights delegated to it by the ERO pursuant to a Delegation Agreement.

2.1.2 Agreements with Canada and Mexico. WECC will carry out responsibilities and exercise rights pursuant to International Reliability Agreements with Canadian or Mexican authorities.

2.1.3 Regional Coordination. WECC will act as a coordinating entity for the entire Western Interconnection for activities of regional organizations with responsibilities for reliability and market functions.

2.1.4 Standard Setting. WECC will develop and adopt reliability, operating, and planning standards, criteria and guidelines necessary to maintain the reliable operation of the Western Interconnection's interconnected Bulk Electric System, including seeking, as appropriate, variances from standards of the ERO (or any successor organization which may be created by legislation or otherwise), as well as providing a process for regional variances.

2.1.5 Certification of Grid Operating Entities. WECC will assist in certifying Grid Operating Entities in the Western Interconnection.

2.1.6 Reliability Assessment. WECC will ensure that interconnected Bulk Electric System reliability assessments are conducted as needed. WECC will do this work in conjunction with the Regional Entities to the greatest extent possible. WECC will also facilitate coordinated reliability assessments among Regional Entities.

2.1.7 Compliance Activities. With respect to enforcement of reliability standards, WECC will:

2.1.7.1 implement the Reliability Management System in effect as of WECC's formation and as the Reliability Management System may be subsequently modified in accordance with its terms;

2.1.7.2 implement any monitoring and enforcement mechanisms delegated to it pursuant to Section 215 of the Federal Power Act and any Delegation Agreement with the ERO, or required by any International Reliability Agreement with a Canadian or Mexican authority; and

2.1.7.3 administer any other monitoring and enforcement mechanisms where WECC is designated to perform administration.

2.1.8 Coordinated Regional Planning. With respect to the coordination of regional planning activities, WECC:

2.1.8.1 will develop coordinated planning policies and procedures for the Western Interconnection, including facilitation of market-based solutions, consistent with WECC/ERO standards and FERC policy.

2.1.8.2 will review and assess Local Regional Entity planning processes to determine whether WECC planning procedures have been satisfied;

2.1.8.3 will refer planning matters back to the originating Local Regional Entity for revision or other corrective actions when the WECC Board determines that WECC planning procedures have not been satisfied; and

2.1.8.4 may perform other interconnection-wide studies as needed.

2.1.9 Coordinated Operations. With respect to coordinating reliable operating activities within the Western Interconnection, WECC will develop, coordinate and promote consistent interregional operating policies and procedures for the Western Interconnection, consistent with WECC/ERO standards and FERC policy.

2.1.10 Market Interface Issues. With respect to Market Interface issues WECC will:

2.1.10.1 facilitate development of compatible and efficient practices across the Western Interconnection; and

2.1.10.2 exercise Backstop Authority where an unresolved Market Interface issue will cause Material External Impacts by taking some or all of the following actions: 1) providing a forum for and coordinating voluntary solutions among Members; 2) recommending specific solutions for voluntary adoption by Members; and 3) if necessary, proposing solutions to an Applicable Regulatory Authority.

2.1.11 Dispute Resolution. WECC will provide a process for the timely resolution of disputes between WECC Members as set forth in Section 11.

2.2 Organizational Characteristics.

As WECC carries out activities to fulfill its mission, it will seek to develop and maintain the following characteristics:

2.2.1 dedication to serving the individuals, businesses, and other organizations that generate, transmit, distribute, market, and use electrical energy in the Western Interconnection;

2.2.2 efficiency in its administration, decision-making, policy and standards development, and dispute resolution processes;

2.2.3 the ability to maintain status as an Interconnection-wide regional reliability entity and be afforded deference and delegation by ERO (or successor organization); and

2.2.4 fair and open processes through which practices, policies, and standards are developed and implemented based on sound technical and policy analysis.

2.2.5 Promote an efficient western electric market by reducing or eliminating conflict, duplication and overlap among electric organizations in the Western Interconnection.

2.2.6 Allow access to WECC data by individuals who can demonstrate a legitimate business need for the data, provided such individuals agree to such protections and non-disclosure restrictions which may be necessary due to the nature of the data sought to be accessed and agree to pay the incremental costs of providing the data which may be requested.

3. Definitions.

The capitalized terms used in these Bylaws shall have the meanings set forth below, or if not set forth below, shall have the meanings given them in the NERC Glossary of Terms Used in NERC Reliability Standards.

3.1 Affiliate.

An Entity that directly or indirectly through one (1) or more intermediaries, controls, or is controlled by, or is under common control with, another Entity. An Entity "controls" any Entity in which it has the power to vote, directly or indirectly, 5% or more of the voting interests in such entity or, in the case of a partnership, if it is a general partner. Notwithstanding the foregoing definition, for purposes of these Bylaws: 1) electric distribution cooperatives that are member-owners of a generation and transmission cooperative are not Affiliates of the generation and transmission cooperative or of each other; 2) an entity controlled by or operating as a unit, agency, or subdivision of a local, state, provincial, or U.S. federal or Canadian or Mexican national government will not be considered an Affiliate of any other entity controlled by or operating as a unit, agency, or subdivision of a local, state, provincial, or federal government; 3) separate agencies of a single state or province, or of the U.S. federal or Canadian or Mexican national government will not be considered Affiliates of each other, regardless of any commonality of political control; 4) members of any joint powers authority, and such joint powers authority, will not be considered Affiliates of each other; and 5) members of an RTO will not be considered Affiliates of such RTO or of each other solely as a result of such membership.

3.2 Annual Meeting.

The annual membership meeting of WECC, as described in Section 5.3.

3.3 Applicable Regulatory Authority.

The FERC or any state or provincial government agency with jurisdiction to regulate or directly affect the transmission of electricity within the Western Interconnection.

3.4 Backstop Authority.

The ability, obligation, or responsibility of WECC to address an issue when the WECC Board determines that a Local Regional Entity(ies) holding Primary Authority has not resolved an issue, has created incompatible resolutions or has not acted. In each case where these Bylaws authorize WECC to exercise Backstop Authority, the provisions that authorize Backstop Authority will also specify the conditions necessary to trigger Backstop Authority and the actions that fall within WECC's exercise of Backstop Authority.

3.5 Balancing Authority.
The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

3.6 Ballot Body.
The Ballot Body consists of WECC members and non-members that have been determined eligible for the voting sectors described in the Reliability Standards Development Procedures and may, therefore, vote on Regional Criteria and Regional Reliability Standards.

3.7 Board of Directors (Board).
WECC Board of Directors, collectively, as described in Section 6.

3.8 Class.
A grouping of Members described in Sections 4.2.1 through 4.2.7 and 4.3.

3.9 Commercial Practices.
The products and practices involved in trading electricity. The term "Commercial Practices" only refers to an interaction among market entities that does not affect or require assistance from Grid Operating Entities that have grid reliability responsibilities.

3.10 Compliance Hearing Body.
The hearing body used for the purpose of providing a balanced compliance panel to conduct hearings for the resolution of disputes concerning compliance with or enforcement of Reliability Standards that may arise between WECC (acting as Compliance Enforcement Authority for the Western Interconnection) and a Registered Entity.

3.11 Delegation Agreement.
An agreement between the ERO and WECC pursuant to Section 215 of the Federal Power Act by which the ERO delegates to WECC designated powers, rights and responsibilities regarding the administration within the Western Interconnection of electric Reliability Standards adopted or approved by the ERO and the FERC.

3.12 Director.
An individual member of the WECC's Board of Directors.

3.13 Electric Line of Business.
The generation, transmission, distribution, or trading of electricity or the provision of related energy services in the Western Interconnection.

3.14 Electric Reliability Organization (ERO).
The organization certified by FERC under 18 C.F.R. §39.3, the purpose of which is to establish and enforce Reliability Standards for the Bulk-Electric System in the United States, subject to FERC review.

3.15 Entity.
Any individual, person, corporation, partnership, association, governmental body or organization of any kind.

3.16 FERC.
The Federal Energy Regulatory Commission or any successor.

3.17 Grid Operating Entity.
Any operating entity, such as a Balancing Authority, that is certified pursuant to Section 2.1.5 of these Bylaws to be responsible for reliable operation of a portion of the Western Interconnection.

3.18 International Reliability Agreement.
An agreement between WECC and any appropriate Canadian or Mexican authority related to WECC's powers, rights and responsibilities regarding the administration of electric reliability standards applicable within such authority's geographic area of the Western Interconnection.

3.19 Local Regional Entity.
A regional transmission organization or some other formally or informally constituted regional organization or group within the Western Interconnection, including but not limited to a Balancing Authority, a group of Balancing Authorities acting in concert, or a group of Entities that own or operate Transmission Facilities acting in concert. These Local Regional Entity boundaries can be reevaluated or modified over time.

3.20 Market Interface.
Market Interface involves all interactions among market entities and Grid Operating Entities related to transmission service and physical delivery.

3.21 Material External Impacts (MEI).
Significant effects on another Local Regional Entity or market within the Western Interconnection but outside of the Local Regional Entity or market adopting a policy, standard, practice or procedure, or implementing an action.

3.22 Member.

Any entity that has applied and been accepted for membership in WECC and is current in the payment of dues.

3.23 Participating Stakeholder.
Any person or entity that is not a WECC Member, but is an interested stakeholder and has applied and been granted, pursuant to Section 8.7.2, the participation and voting rights set forth in Section 8.7.1.

3.24 Primary Authority.
The ability, obligation, or responsibility of an entity to address an issue in the first instance.

3.25 Regional Criteria
The term Regional Criteria shall have the definition set forth in the NERC Rules of Procedure as may be amended from time to time.

3.26 Regional Entity (RE).
An entity having enforcement authority pursuant to 18 C.F.R. §39.8.

3.27 Registered Entity.
An owner, operator, or user of the Bulk-Electric System or the entities registered as their delegates for the purpose of compliance in the North American Electric Reliability Corporation Compliance Registry or similar Entity operating in Canada or Mexico and which could be registered in the Compliance Registry if it operated in the United States.

3.28 Reliability Management System
The contracts, separate from these Bylaws, by which Members and other parties agree to certain procedures and sanctions intended to enforce specified Reliability Practices to maintain reliable electric service throughout the Western Interconnection.

3.29 Reliability Standard.
A requirement approved by FERC under section 215 of the Federal Power Act, to provide for reliable operation of the Bulk-Electric System in the United States. Regional Reliability Standards are specific to the Western Interconnection and shall be established using the WECC Standards Development Procedures.

3.30 Reliability Standards Development Procedures.
The process for developing and approving WECC Regional Reliability Standards (or its successor) attached as Exhibit C to the Delegation Agreement between WECC and North American Electric Reliability Corporation.

3.31 Transmission Facilities.
Those facilities that are defined as "transmission facilities" by FERC for purposes of the open access requirements of Section 210 and 211 of the Federal Power Act or any facilities which would be so defined if the Member were subject to FERC jurisdiction.

3.32 Western Interconnection.

The geographic area containing the synchronously operated electric transmission grid in the western part of North America, which includes in the United States Arizona, California, Idaho, Nevada, Oregon, Utah, and Washington, as well as parts of Montana, Nebraska, New Mexico, South Dakota, Texas, Wyoming, and Colorado; parts of the Canadian Provinces of British Columbia and Alberta; and Baja California Norte, Mexico.

4. Members and Membership.

4.1 Voluntary Membership.

Except as otherwise may be required by applicable authority, membership in WECC is voluntary. A Member may withdraw upon giving the Secretary thirty (30) days' advance written notice. Notwithstanding such notice of withdrawal, all contracts, FERC orders, unpaid Member costs, and decisions of arbitration in effect or pending as of the date of the written notice of withdrawal will be followed through to completion, pursuant to these Bylaws, by the withdrawing Member; however. Nothing herein will relieve any Member withdrawing from WECC from any obligation it may have under applicable law including, but not limited to, Section 215 of the Federal Power Act. A Member that withdraws is obligated to pay any unpaid dues owed through the remainder of the fiscal year in which its withdrawal becomes effective.

4.2 Eligibility for Membership.

Subject to Section 4.5, any Entity that is an interested stakeholder or that meets the criteria for membership in the membership classes described in Sections 4.2.1 through 4.2.5 may be a Member of WECC:

4.2.1 Class 1. Electric Line of Business Entities owning, controlling or operating more than 1000 circuit miles of transmission lines of 115 kV and higher voltages within the Western Interconnection.

4.2.2 Class 2. Electric Line of Business Entities owning, controlling or operating transmission or distribution lines, but not more than 1,000 circuit miles of transmission lines of 115 kV or greater, within the Western Interconnection.

4.2.3 Class 3. Electric Line of Business Entities doing business in the Western Interconnection that do not own, control or operate transmission or distribution lines in the Western Interconnection, including power marketers, independent power producers, load serving entities, any other Entities whose primary business is the provision of energy services, and those Entities that are not eligible for membership in the other Member Classes and who have a substantial interest in the purposes of WECC.

4.2.4 Class 4. End users of significant amounts of electricity in the Western Interconnection, including industrial, agricultural, commercial and retail entities as well as organizations in the Western Interconnection that represent the interests

of a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public or the environment.

4.2.5 Class 5. Representatives of states and provinces in the Western Interconnection, provided that such representatives will have policy or regulatory roles and do not represent state or provincial agencies and departments whose function involves significant direct participation in the market as end users or in Electric Line of Business activities.

4.2.6 Sub-Class Organization. A Member Class may subdivide in up to three subclasses based on a majority desire within that class for purposes of electing Member Advisory Committee representation.

4.3 Designation of Membership Class.

A Member of WECC may not belong to more than one Class. An applicant for membership will designate the Class for which it qualifies based upon the criteria for membership set forth in Section 4.2, however any Member owning, controlling or operating Transmission Facilities or distribution facilities must belong to Class 1 or 2 unless the Board grants the Member's petition for a change in Member Class pursuant to the provisions of Section 4.4 of these Bylaws. Applications for membership will be submitted to WECC. WECC staff will review the application to verify eligibility for membership and Member Class designation. An applicant whose application has been rejected or any Member who disputes the WECC staff's determination regarding the appropriate Member Class designation may request review by the Governance Committee. If the applicant or any Member disagrees with the Governance Committee's decision, the applicant or such Member may appeal this decision to the Board.

4.4 Changes in Membership Class.

Notwithstanding any other provision of these Bylaws, upon a petition from a Member, the WECC staff (subject to review by the Governance Committee and appeal to the Board) may allow the Member to change Member Class if the interest of the Member is more closely aligned with the proposed Class than the Member's current Class.

4.5 Affiliates and Distinct Business Entities.

An Affiliate of a Member that satisfies the membership qualifications may also become a Member provided:

4.5.1 The Affiliate applying for membership and the Member disclose to the Chief Executive Officer all Affiliates that are WECC Members and the Classes to which the Affiliates belong. Every Member will promptly notify the Chief Executive Officer whenever it becomes, or ceases to be, an Affiliate of any other Member.

4.5.2 Affiliates may be members of the same Class; provided, however, a group of Affiliates within a single Class may only have one vote in any WECC forum. Except as set forth in Section 8.7.6, a group of Affiliates within a single Class may, by providing at least three (3) business days advance written notice to the

Chief Executive Officer, split their single vote equally amongst all Affiliates or designate a single Affiliate as the group's voting Member.

4.5.3 For good cause shown and with the express approval of the Board, a company or organization containing functionally distinct entities within it may obtain separate memberships for such entities; provided that such entities will be considered Affiliates.

4.5.4 The Board may adopt a policy regarding whether Members may share the benefits of membership (including the right to receive information that is only available to Members) with a non-member Affiliate.

4.6 Rights and Obligations of Membership.

Except as otherwise provided in these Bylaws or other applicable authority, Members of WECC have the following general rights and obligations:

4.6.1 The right to elect and remove Directors as described in Section 6.5;

4.6.2 The right to amend these Bylaws, and to review and rescind any Board amendment of these Bylaws, in accordance with Section 12;

4.6.3 The right to receive appropriate meeting notices, as well as reports and information produced by WECC;

4.6.4 The right to attend, participate and vote in all WECC Member meetings and the right to attend Board meetings (other than closed sessions of Board meetings) and to comment upon all matters considered in such meetings;

4.6.5 The right to be a member of, attend meetings of, and to introduce motions, debate and to vote in the deliberations of WECC committees, subject to the limitations of these Bylaws and such other reasonable limitations as the Board may adopt from time to time;

4.6.6 The right to invoke the dispute resolution provisions of these Bylaws;

4.6.7 The right to petition the Board to take any action consistent with applicable law (including Section 215 of the Federal Power Act and implementing orders and regulations), these Bylaws and the articles of incorporation and to have such petition voted upon in a reasonable and timely manner;

4.6.8 The obligation to abide by these Bylaws, decisions resulting from the dispute resolution process, and all standards or decisions of WECC, subject to the exceptions set forth in Section 4.7 and the enforcement provisions of Section 4.8.

4.6.9 The obligation to notify the Chief Executive Officer promptly of changes with respect to Affiliates as provided in Section 4.5.1 of these Bylaws; and

4.6.10 The obligation to pay in a timely manner the membership dues pursuant to Section 11.

4.6.11 The obligation to provide system data that the Board has determined is necessary for WECC functions and does not impose an undue burden on the Members; provided, however, that the Board shall adopt appropriate limitations on this obligation or procedures that protect and avoid unnecessary collection of confidential, privileged, trade secret, cybersecurity or critical energy infrastructure information or other information that the Board determines merits such protection consistent with applicable law.

4.6.12 The obligation to support surfacing minority and majority opinions or views within their Member Class, along with supporting rationale to enable the Board of Directors to make decisions based on informed judgment aligned with WECC's vision, mission and these Bylaws.

4.7 Limitations on Member Obligations.

4.7.1 The obligation of Members pursuant to Section 4.6.8 will not require any Member to take any action which the Member in good faith determines: 1) would exceed the physical capabilities of the Member's electric system (or any part of another's electric system that the Member has the legal right to cause to comply with a WECC action governed by Section 4.6.8); 2) would create serious and immediate risks to public health or safety (provided, however, that the shedding of load shall not in and of itself be deemed a serious and immediate risk to public health and safety for the purpose of this section); 3) would create an immediate risk of serious damage to facilities or equipment within its electric system or cause it to operate any of its electric facilities or equipment in an unsafe manner; 4) would cause the Member to violate or improperly implement an applicable law, regulation, rule, order, FERC license provision or other legal obligation; or 5) would conflict with any non-power requirement applicable to the Member (including without limitation any obligation under environmental laws, regulations, court and administrative decisions or biological opinions).

4.7.2 Each Member shall retain sole control of its facilities and the use thereof, and a Member shall not be required to construct or dedicate facilities for the benefit of any other Member, or be required to take action, or refrain from action, as may be deemed necessary to maintain reliable service to its own customers and/or to fulfill its obligations to third parties; provided, that a Member shall comply with duly-adopted reliability standards applicable to its system and shall comply with any directives under existing security coordination agreements. Nothing in these Bylaws is intended to preclude application of Section 210 or 211 of the Federal Power Act. The above limitations shall not be construed as altering a Member's

obligation to comply with applicable Reliability Standards or enforcement orders, or any other obligation arising under 18 C.F.R. Part 39.

4.8 Compliance and Enforcement.

The power of WECC to enforce Member obligations other than compliance with Reliability Standards and other obligations arising under 18 C.F.R. Part 39 and applicable Canadian and Mexican regulatory requirements is limited to suspension or termination of membership as set forth in this Section; provided, however, that: 1) nothing in this Section will limit the power of Members to agree to additional enforcement provisions in separate contracts (such as contracts pursuant to the Reliability Management System); 2) nothing in this Section will limit the power of WECC to propose solutions regarding Market Interface issues to any Applicable Regulatory Authority as described in Section 2.1.10; and 3) nothing in this Section will limit WECC's delegated authority under Section 215 of the Federal Power Act and 18 C.F.R. Part 39 and applicable Canadian and Mexican regulatory requirements to enforce reliability standards and perform other delegated or contractual functions within the Western Interconnection. The Board may suspend or, to the extent consistent with applicable law, terminate the membership of any Member for a material failure to meet any obligation of membership set forth in these Bylaws, including, but not limited to: 1) non-payment of dues sixty (60) days after the dues become delinquent; 2) intentionally or repeatedly violating any WECC Bylaw; 3) materially breaching or intentionally violating any FERC order or arbitration decision issued pursuant to these Bylaws; 4) willfully obstructing any lawful purpose or activity of WECC; or 5) remaining inactive as described in Section 5.9. The Board will give the affected Member not less than twenty-one (21) days prior written notice of any proposed suspension or termination, which will include the specific basis for the proposed action and, if applicable, instructions on curing the problem. Prior to terminating a membership, the Board will consider any information provided by the Member in response to the notice described herein.

4.8.1 Suspension. The suspension of a Member will not affect the Member's rights and obligations other than that the Member will not be entitled to vote at any meeting of the Members, Classes, subclasses, or any committee until the suspension is removed except that a suspended Member may participate in the WECC proposed Reliability Standards Development Procedure.

4.8.2 Termination. The termination of membership will have the same effect, and be subject to the same continuing obligations, as such Member's withdrawal pursuant to Section 4.1, except that it will be effective as of the issuance date of the notice provided pursuant to Section 4.8.

4.9 WECC Structure and Governance Review.

At least each five years, the Board of Directors will conduct a thorough assessment of whether WECC is fulfilling its purposes in a manner that is consistent with: 1) the provisions of Section 2.2 of these Bylaws; and 2) the then-current state and the expected future evolution of the electric power industry within the Western Interconnection. Unless determined otherwise by a majority vote of both the Board of Directors and the Members Advisory Committee (MAC), the initial review required under this Section 4.9 will

commence after the completion of the first full year of operation under these Bylaws as amended in June 2013 and will be done collaboratively with the MAC and to the extent practical, will be coordinated with any similar structure and governance reviews being conducted by Peak Reliability. In particular, the Board will focus on whether the standards, obligations, processes, and decisions WECC imposes on its Members are timely, fair, effective, and reasonable in view of the commercial, legal, regulatory, and economic needs and objectives of the affected Members. The Board will evaluate WECC's Board composition, Member Class structure, committee structure and activities, and staff responsibilities as they relate to the foregoing considerations. The assessment required by this Section 4.9 will be accompanied by Board recommendations for any changes the Board determines are warranted by the assessment. The assessment and recommendations prepared by the Board in accordance with this Section 4.9 will be submitted in writing to the Members at the first annual Member meeting held after they are completed.

5. Procedures for Member Decisions.

5.1 Quorum and Alternative Voting.

With the exception of voting on Regional Reliability Standards and Regional Criteria under the oversight of the WECC Standards Committee, members may conduct business and take votes only at duly noticed Member meetings. Members may not conduct any business of the membership as a whole at any meeting unless a quorum is first established.

5.1.1 Quorum. A majority of all Members, including a majority in at least three (3) Classes, will constitute a quorum for all meetings of the membership as a whole. A majority of the members of a Class or subclass will constitute a quorum for all Member Class or subclass meetings. Members participating through a designated alternative representative or through submission of an absentee ballot will be counted in determination of a quorum. Inactive Members, as defined in Section 5.9 of these Bylaws, will not be counted in determining a quorum at Member, Member Class or subclass meetings. A quorum, once established, will be deemed to continue for the balance of any Member, Member Class, or subclass meeting, except that no election of Directors may occur without a quorum being present. Members may designate an alternate representative or submit an absentee ballot in a form consistent with Section 5.1.2 for any Member, Member Class, or subclass meeting.

5.1.2 Alternate or Absentee Voting: In the event that a Member's designated voting representative cannot attend a meeting of the Membership or a Member Class meeting where Directors are being elected or amendments to these Bylaws are considered, a Member may designate an alternate voting Member representative, with two (2) days written notice to the Corporate Secretary, or a Member may cast an absentee ballot pursuant to the procedures established by the Corporate Secretary.

5.2 General Membership Meetings.

All business of the Members acting as a whole will be conducted at meetings called by advance notice to all WECC Members provided in accordance with Section 5.5. Unless stated otherwise in these Bylaws, decisions at all meetings of the Members, Member Classes, or subclasses will be by simple majority vote of the Members present or otherwise represented in accordance with these Bylaws, with each Member having one vote, unless other Bylaw provisions provide for the allocation of the Member's vote. The Chair of the Board will preside over all Members acting-as-a-whole meetings.

5.3 Annual Member Meetings.

WECC will hold an Annual Meeting of all Members at a time and place determined by the Board. At the Annual Meeting, and at other times as provided for in these Bylaws, in addition to such other actions the Members may take, Member Classes will elect Directors for vacant director positions.

5.4 Special Member Meetings.

Members may hold special meetings whenever called by the Board. The Board will call special Member meetings whenever a majority of the Members of any Class request a special meeting or at such other times as it deems appropriate. The Chair of the Board will preside over all special Member meetings.

5.5 Member Class and Subclass Meetings

An individual WECC Member Class or subclass may hold a meeting for any purpose relevant to the interests of Class or subclass Members. Such meeting will be initiated by request by one or more Class or subclass Member(s), and agreement by at least fifty percent (50%) of Class or subclass Members.

5.6 Notice of Member Meetings.

5.6.1 Annual Meeting. The Chief Executive Officer will provide at least thirty (30) days' advance notice to all Members and the Board of the date, place and time of the Annual Meeting of the Members and an agenda of the business to be conducted at such meeting.

5.6.2 Other Member Meetings. The Chief Executive Officer will provide notice of regularly scheduled and special meetings of the Members to the Members not less than fifteen (15) days before the meeting if delivered by first-class mail, or not less than ten (10) days before the meeting if the notice is delivered personally, by telephone, by facsimile, electronic mail or express mail. If mailed, such notice will be deemed given when deposited in the United States mail, with first-class postage thereon prepaid, addressed to a Member. Such notice will state the date, time and place of the meeting and the meeting agenda.

5.6.3 Public and Website Notice. Public notice of each meeting of the Members will be placed on WECC's website at least ten (10) days before such meeting. In addition, the Chief Executive Officer will provide notice in the same manner and time as set forth in Section 5.6.2 of each meeting to each member of the public

who so requests and who has provided appropriate information regarding delivery of notice.

5.7 Open Meetings.
All Membership meetings are open to observation by the public.

5.8 Policymaking Authority.
The Board of Directors may adopt policies for the interpretation and implementation of the meeting and voting procedures established in this Section 5.

5.9 Minimum Participation Requirement.
In order to be counted for quorum purposes at a meeting of the membership as a whole, Class, or subclass meeting, a WECC Member must actively participate (by attending in person, sending an alternate, or voting absentee) in at least one WECC meeting (including meetings of the Board, committees and subcommittees) each year. If the Member does not meet this minimum participation requirement, the Member will be considered an "inactive" Member until its active status is restored by participation in at least one WECC meeting (including meetings of the Board, committees and subcommittees) by attending in person, sending an alternate, or voting absentee. An inactive Member will not be counted toward establishing a quorum of the membership as a whole, of a Class, or of a subclass. An applicant for WECC membership or a WECC Member may at any time self-designate itself an inactive Member. Such designation will be effective until the Member is reinstated to "active" status. If a Member does not participate for twenty four (24) consecutive months, the Member's membership will be terminated. If a Member's membership is so terminated, reapplication for membership may be made at any subsequent time.

6. Governance.

6.1 Board of Directors.
Subject to those matters expressly requiring approval of the Membership, a Board of Directors elected by the Members will govern WECC. The Board of Directors will elect its own Chair and Vice-Chair from those individuals serving as Directors.

6.2 Composition of the Board and Board Member Qualifications.

6.2.1 The Board of Directors shall consist of nine (9) Directors. At all times, subject to temporary vacancies, the Board of Directors shall include at least three directors who have at least ten years of experience in the utility industry, preferably in the Western Interconnection, including at least one director who has transmission operations experience, at least one director who has transmission planning experience, and at least one director who has generation operations experience. At any time where the membership of the Member Advisory Committee (MAC) is modified, as may be provided in other provisions of these bylaws, to include representation for Entities of the two Canadian Provinces of British Columbia and Alberta and the Mexican State of Baja California, at least one Director, elected

subsequent to such MAC representation, shall have international experience corresponding to such geographic area(s) and/or representation in the MAC.

6.2.2 The remaining members of the Board of Directors shall be selected in an effort to ensure diversity of background and experience. Desirable categories of experience may include: regulatory or legal; accounting, finance or economics; environmental; end-user advocacy; information technology; compliance or standards; public sector; and international.

6.2.2.1 Transmission operations experience shall preferably include experience in control center operations at the senior management or officer level.

6.2.2.2 Transmission planning experience shall preferably include experience in modeling and/or planning transmission facilities, including economic and reliability modeling at the senior management or officer level.

6.2.2.3 Generation operations experience shall preferably include experience in development or operation of generation facilities, including economic and reliability modeling at the senior management or officer level.

6.2.2.4 Regulatory or legal experience shall preferably include at least one of the following types of experience: state, provincial or federal industry regulation; significant litigation experience ideally at the appellate level; evaluation of complex legal arguments; and advising clients with respect to settlements.

6.2.2.5 Accounting, finance or economic experience shall preferably include experience as a Chief Financial Officer, a Chief Account Officer, a Corporate Risk Officer, a Certified Public Accountant, or the equivalent thereof.

6.2.2.6 Environmental experience shall preferably include experience advocating environmental interests before local, state or federal agencies or boards, and/or leadership experience in representing environmental interests in relation to energy issues.

6.2.2.7 End-user advocacy experience shall preferably include experience advocating end-user economic interests before local, state or federal ratemaking agencies or boards.

6.2.2.8 Information technology experience shall preferably include experience as a senior level manager responsible for integrating information technology services with organizational needs in areas such as capacity planning, budget and finance, acquisition and deployment, operations, change management, application development, trade ally relationships, user support, data quality, security and similar areas.

6.2.2.9 Compliance or standards experience shall preferably include experience as a senior level officer or manager for corporate compliance with internally and/or externally imposed requirements, rules or standards.

6.2.2.10 Public sector experience shall preferably include experience representing the public interests with respect to energy issues.

6.2.2.11 International experience shall preferably include experience as described in the previously listed experience categories, but in the Canadian provinces of British Columbia or Alberta, or the Mexican state of Baja California.

6.2.3 Director Affiliation Restrictions. A Director may not be a full time employee of a Registered Entity. Nor may a Director be affiliated with any Member or Registered Entity operating in the Western Interconnection, nor a Director of an entity performing the function of Reliability Coordinator in the Western Interconnection.

6.2.3.1 For the purposes of this section, "affiliated" shall mean (1) an employee of, (2) a contractor for, (3) an employee of a contractor for, or (4) an equity owner of Registered Entity or Member. For purposes of determining whether a Director is "affiliated" the term "Director" shall include a spouse and/or minor child of the Director.

6.2.3.2 A Director with an equity interest in private or publicly traded companies that are end-users of electricity in the Western Interconnection but are not otherwise "affiliated" pursuant to the restrictions set forth in Section 6.2.2 shall not be considered to be "affiliated".

6.2.3.3 A Director with an equity ownership in a broadly diversified mutual fund which may from time to time include interests in one of the types of organizations described in Section 6.2.2, shall "not be considered to be "affiliated, provided that such equity interest cannot confer a controlling interest in a Member or Registered Entity within the Western Interconnection.

6.2.3.4 A Director receiving post-employment compensation, which compensation is not indexed to the success of the disbursing entity shall not be considered "affiliated".

6.2.3.5 A Director shall not be considered "affiliated" solely by having a contractual relationship with a state government that has one or more

agencies that are Members, provided that the Director cannot be affiliated with the Member agency or agencies.

6.2.3.6 A Director shall not be considered "affiliated" for being a residential or small business end-user of electricity or for being affiliated with, a member of, or a contributor to an organization that represents a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public interests or the environment, but a Director shall be considered "affiliated" if the Director is an employee of, or serves as a director, trustee, or officer or in any other policy-setting capacity with respect to any such organization.

6.2.3.7 The affiliation restrictions set forth in this Section are not all encompassing. Candidates and Board members are expected to disclose all known potential financial or relationship conflicts, including any known relationships between companies they have affiliation with and/or entities described in Section 6.2.2. Furthermore, any Nominating Committee will be expected to investigate and evaluate all potential conflicts, whether financial or otherwise.

6.2.4 In addition, the Board may provide for the Chief Executive Officer ("CEO") of WECC to be a voting, additional tenth, member of the Board through the inclusion of such a provision in the resolution the Board adopts appointing WECC's CEO. Such provision shall not permit the CEO to be a member of a Board committee or to cast either a tie-breaking vote or a vote that creates a tie. The CEO may not serve as the Chair or Vice-Chair of the Board.

6.3 Term of Office.

Directors will hold office for staggered terms of three (3) years, three Directors' terms ending each year. Each three (3) year term shall commence upon the adjournment of the portion of the Annual Member Meeting provided for in Section 5.3, in which all Members are counted for purposes of determining a quorum. Similarly, the three year terms of outgoing Directors shall end upon the adjournment of that portion of the Annual Member Meeting in which all Members are counted for purposes of determining a quorum, whether that results in a longer or shorter term than exactly three years.

6.4 Nomination, Selection and Compensation of Directors.

6.4.1 Nominating Committee. Candidates for a Director position shall be nominated by a Nominating Committee. The Nominating Committee shall consist of seven members. Three members shall be Directors, not standing for re-election, designated by the Board Chair. The remaining four Nominating Committee members shall be designated by the Member Advisory Committee and come from individuals serving on the Member Advisory Committee, with two (2) members being from Classes 1, 2, and/or 3, and two (2) members being from Classes 4 and/or 5.

6.4.1.1 If the Member Advisory Committee does not designate MAC members to serve on the Nominating Committee within 30 days of being notified of the Board Chair's designation of the three Directors to serve on the Nominating Committee, the Board Chair may designate MAC members to serve.

6.4.1.2 A Nominating Committee shall be formed each year not less than 180 days prior to the Annual Meeting. A Nominating Committee will continue to function until a replacement Nominating Committee is formed, but may not continue for a period longer than twelve (12) months from its creation, provided however, that the Board, by resolution, may authorize a Nominating Committee to function beyond twelve (12) months as the Board may determine is necessary.

6.4.2 Director Candidate Nominations.

6.4.2.1 The Nominating Committee shall develop candidate pools and make candidate nominations to the Members. The Nominating Committee may consider any qualified applicant in developing the candidate pool, and may identify applicants through the following process: (1) selecting and utilizing an independent search firm to provide the Nominating Committee with a list of qualified applicants for each Director position subject to election; (2) consider an incumbent Director who is willing to stand for reelection, including a review of such Director's tenure on the Board of Directors; (3) consider external nominations.

6.4.2.2 External parties, including but not limited to Members and Western Interconnection stakeholders, may recommend candidates (self-recommendations and third party recommendations) to the Nominating Committee for consideration, by submitting the following: the candidate's resume, a summary of the candidate's relevant experience, a disclosure statement from the candidate, and a letter of interest from the candidate. All recommendations from external parties must be submitted to the Nominating Committee within sufficient time for the Nominating Committee to evaluate the candidate prior to the notification required in Section 6.4.2.5.

6.4.2.3 The Nominating Committee shall review the qualifications of the potential candidates and put forth one nominee for each Director position up for election.

6.4.2.4 Five (5) affirmative votes of the Nominating Committee shall be necessary to put forth a nominee to the Members.

6.4.2.5 At least sixty (60) days in advance of the Annual Meeting, the Nominating Committee shall notify the Board Chair whether or not it has finalized all Director nominations. If the Committee fails to put forth a nomination for an open position, then the Board Chair may form a new Nominating Committee with different Board and Member Advisory Committee members, who shall be tasked with developing any remaining nominations for open Director positions.

6.4.2.6 Each nominee, put forth by the Nominating Committee, shall be presented for separate election by the Members.

6.4.3 Director Elections. Members will vote for each vacant Director position separately. A candidate will be elected to the Board upon majority vote of the Members as a whole in addition to a majority of the Classes (three of the five) having a majority vote from the Members of the individual Class.

6.4.4 Should a candidate fail to receive the required vote of the Members or Member Classes, the Board may:

6.4.4.1 conduct a new election of an alternate candidate put forward by the Nominating Committee, if any, or the Board may ask the Chair to establish a new Nominating Committee to recommence the nomination and election process. Where a candidate has not received the required vote of the Members and Member Classes, the director position shall remain vacant until a candidate is elected, except as provided in Section 6.7.2.

6.4.5 Annual Compensation of Directors. Every two years, or sooner if, in the discretion of the CEO, a new survey is required, the CEO shall contract with an appropriate firm to conduct a national compensation survey, which shall provide an independent review of the compensation paid independent directors. The latest survey so procured shall be used by the Nominating Committee to make an annual recommendation for the compensation of Directors for the following year. Any such recommendation shall require five (5) affirmative votes of Nominating Committee members. This recommendation shall be presented to the MAC no later than one hundred fifty (150) days prior to the Annual Meeting. The MAC shall set the compensation for the Directors at least one hundred and twenty (120) days prior to the Annual Meeting. When making this decision, the MAC shall consider the recommendation of the Nominating Committee and any other material relevant to setting Director compensation. If the Nominating Committee is unable to reach the five (5) vote majority necessary to make a compensation recommendation, the MAC shall make no changes to the compensation paid Directors for the following year.

6.5 Removal of Directors.

The Members or the Board may remove a Director before completion of the Director's term of office pursuant to the following provisions.

6.5.1 Removal by the Members. Directors may be removed only for gross negligence, violation of local, state, provincial, or federal laws, gross misconduct, or failure to meet the fiduciary obligations of Directors.

6.5.1.1 Removal of a Director will be by a vote of a majority of all the WECC Members, not just those Members voting, in addition to a majority of the Classes (three of the five) having a majority vote from the Members of the individual Class. Removal may only take place at a meeting called for that purpose by notice provided in accordance with the notice requirements for member meetings. A vote, by all Members, to consider removal of a Director will occur based upon a petition, for such an all-Member vote, supported by twenty percent (20%), each, of the Members of three of the five Member Classes.

6.5.2 Removal by the Board. The Board may remove any Director for gross negligence, violation of local, state, provincial, or federal laws, gross misconduct, or failure to meet the fiduciary obligations of Directors. Such removal will only occur upon the affirmative vote of not less than six (6) Directors.

6.6 Resignation.

Any Director may resign from their position at any time by written notice to the Board by delivery to the Chair. The acceptance of a resignation will not be required to make it effective.

6.7 Procedures for Filling Vacant Director Positions.

6.7.1 Director Vacancies. If the position of any Director becomes vacant prior to its normal term expiration, the remaining Directors may charge the Nominating Committee with selecting a successor immediately. The Nominating Committee will follow the requirements set out in Sections 6.2.1 and 6.2.2 in its selection of any successor Director. Alternatively, if less than one (1) year remains in the term of that Director, the remaining Directors may choose to leave the position vacant for the remainder of the term.

6.7.2 Holdover to Cure Procedural Vacancies. Whenever an incumbent Director is a candidate for a Director position and a vacancy would be created due to expiration of the Director's term, the Director may continue to serve, for up to an additional 12 months, until such time as an election of the Director's position can be conducted, provided the vacancy arises from a lack of quorum or other procedural inability to elect a candidate for the Director position.

6.7.3 Should the number of serving Directors fall below seven (7), the Board may appoint one or more individuals to serve as temporary Directors until such time as replacement Directors can be elected by the Members.

6.7.3.1 In appointing temporary Directors, the Board shall select individuals who meet the requirements of Section 6.2.

6.8 Duties of Directors.

The Directors will have the following duties:

6.8.1 Fiduciary Obligation to WECC: All Directors, will have a fiduciary obligation to WECC consistent with the requirements for Directors of Utah non-profit corporations. Members of the Board will at all times act in conformance with such requirements, these Bylaws and the Standards of Conduct set forth in Appendix A.

6.8.2 Preserve Non-Affiliated Status: Throughout their terms, Directors will have a duty to avoid any affiliation that is inconsistent with the qualifications for Directors in Section 6.2.2 of these Bylaws. If a Director becomes aware of any intervening disqualification, he/she must either resign or eliminate the disqualification (e.g., dispose of securities) within sixty (60) days.

6.9 Powers of Directors.

The management of all the property and affairs of WECC will be vested in the Board of Directors. The Board will hold annual elections to select a Board Chair and to fill any other Board officer positions that may be created by the Board or required by applicable law. The Board may exercise all the powers of WECC and do all lawful acts and things (including the adoption of such rules and regulations for the conduct of its meetings, the exercise of its powers and the management of WECC) as are consistent with these Bylaws and the Articles of Incorporation. The Board will give serious consideration to the Member Advisory Committee's and the Western Interconnection Regional Advisory Board's (or any successor) recommendations. The Board will respond to Member Advisory Committee and Western Interconnection Regional Advisory Board recommendations through a means which the Board determines appropriate.

6.10 Delegation of Board Authority.

The Board may delegate to the Chief Executive Officer or to any Board Committee formed pursuant to Section 7.7.3 any or all of its powers and authority except: 1) any power which it may not delegate pursuant to applicable Utah law; 2) the power to adopt any reliability standard; 3) the power to determine when to exercise the Backstop Authority of WECC; 4) the power to approve budgets; 5) the power to form committees; 6) the power to amend the Bylaws; 7) the power to elect the Chair and other officers of the Board; and 8) the power to hire, fire or set the terms of employment of the Chief Executive Officer. The Board may also delegate to any Member committee the power to make specific decisions, subject to the right of any Member to appeal any of such decisions to the Board within 30 days of the committee vote on the decision by writing a letter to the Chief Executive Officer that describes in reasonable detail the grounds for appeal, and requests that the appeal be considered by the Board at its next regularly scheduled meeting, subject to applicable notice requirements. Delegation will be by express decision and will require the affirmative vote of not less than a majority of the

Directors. Any Director may call for a vote to rescind such delegation at any time and such delegation will be rescinded if a majority of the Directors vote to do so.

6.10.1 Notice to Members. Within seven (7) days of any decision delegated pursuant to Section 6.10, except for routine decisions of the Chief Executive Officer, Members will be notified of the decision by electronic mail, posting on the WECC website and any other means determined appropriate by the Board. Routine decisions of the Chief Executive Officer will be noticed in periodic reports to the Board and Members as determined by the Board, which will be sent to Members by electronic mail and posted on the WECC website.

6.10.2 Board Review of Delegated Decisions. Decisions delegated pursuant to Section 6.10 will be reviewed by the Board at the request of any Director, provided such request is lodged with the Secretary within thirty (30) days of the notice. Whenever it determines that a matter requires an urgent decision, the Board may shorten the deadline for requests for review, provided that: 1) the notice and opportunity for review will be reasonable under the circumstances; and 2) notices to Members will always contain clear notification of the procedures and deadlines for Board review. A request for review of a decision will stay the effect of the decision pending review unless the Board in making the delegation expressly determines otherwise.

7. Procedures for Board Decisions.

7.1 Quorum.

No business will be conducted by the Board unless at least five (5) Directors are present, or six (6) Directors if the CEO is counted to determine a Board quorum.

7.2 Majority Vote.

A decision of the Board will require an affirmative vote of a majority of Directors present and not abstaining; provided that no decision of the Board shall be made with fewer than three (3) affirmative votes, or four (4) affirmative votes if the CEO is counted to determine a Board quorum. Directors may not vote by proxy or by absentee ballot, but Directors may participate in Board meetings by telephone as provided in Section 7.3 of these Bylaws.

7.3 Attendance at Board Meetings by Teleconference.

Any or all of WECC's Directors may participate in any meeting of the Board by telephone conference or any other means of communication that enable all Directors participating in the meeting to simultaneously hear one another. Every Director participating in a meeting in the manner described in the preceding sentence will be deemed to be present in person at that meeting.

7.4 Board Action by Unanimous Consent.

7.4.1 Action Without a Meeting. Unless WECC's Articles of Incorporation or applicable law provides otherwise, action required or permitted to be taken at a

meeting of the Board may be taken without a meeting through one or more written consents describing the action taken. Any Board action taken by written consent must be signed by all Directors in office at the time the action is taken. Such actions must be noticed to Members in accordance with Section 7.5 and Members must be given an opportunity to comment prior to the Board taking such actions through electronic mail, comments on the website or other appropriate means. The required notice of such meeting may generally describe the arrangements (rather than the place) for the holding of the meeting. All other provisions herein contained or referred to will apply to such meeting as though it were physically held at a single place. All Board actions by written consent must be filed with WECC's Board meeting minutes. Action taken under this Section is effective when the last Director signs the consent, unless the consent specifies an earlier or later effective date. Any action by written consent has the same effect as a meeting vote and may be described as such in any document.

7.4.2 Waiver of Procedures. For any specific action at any noticed meeting of the Board, and under exigent or unusual circumstances, the Board by unanimous vote of those present may waive any procedural requirement applicable to Board decision-making, including any requirement for notice of a specific potential action, except for the following: 1) the requirement for notice of the time and place of the meeting pursuant to Section 7.5; 2) the quorum and voting requirements of Sections 7.1 and 7.2; and 3) any non-procedural limitation on the power of the Board to make a decision, including, but not limited to, those restrictions in Sections 6.10 (limiting the power to delegate) and 12.1 (limiting the power to amend the Bylaws). Whenever such action is taken, a statement describing the action, the exigent or unusual circumstances, the specific procedure waived, the basis for the waiver and the votes of all Directors present shall be posted on the website and communicated in writing or by e-mail to all Members within five (5) days.

7.5 Notice of Board Meetings.

7.5.1 Regular Meetings. Except as set forth in Section 7.5.2 regarding urgent business, all regular business of the Board will occur at the Board meetings, at least twenty-one (21) days' advance notice of which has been provided by the Chief Executive Officer to all Directors and all Members. Notice will include an agenda that will identify those matters on which a vote will be taken at the meeting. The foregoing requirement shall not preclude the Board from taking an action that is different from the specific proposed action identified in the agenda, as long as the relevant subject matter has been reasonably identified in the agenda. The Directors will establish a regular meeting schedule that will be made available to the Members. The schedule will include not less than two meetings of the Board annually.

7.5.2 Special Meetings. Whenever the Chair of the Board or any three (3) Directors find that there is urgent business requiring Board action before the next regular Board

meeting, a special meeting of the Board may be called. Such special meetings will be held upon as much written notice to each Board Member and all Members as is possible under the circumstances, which will not be less than three (3) days. However, this notice of special meetings may be waived if: 1) the waiver is by a writing signed by a quorum of Board members; and 2) as much notice of the meeting as practicable has been given to WECC Members via e-mail and posting on the WECC website.

7.5.3 Public and Website Notice. Public notice of each meeting of the Board will be placed on WECC's website at least ten (10) days before such meeting (or such lesser time as provided pursuant to Section 7.5.2). In addition, the Chief Executive Officer will provide notice of each meeting by first-class mail, facsimile or electronic mail to each member of the public who so requests and who has provided appropriate information regarding delivery of notice.

7.6 Open Meetings.

Except as provided in Section 7.6.1, all regular and special meetings of the Board will be open to observation by any Member and any member of the public.

7.6.1 Closed Session. Notwithstanding the provisions of Section 7.6, upon an affirmative vote of two-thirds (2/3) of the Directors present, the Board may meet in closed session: 1) to consider the employment, evaluation of performance, or dismissal of an employee of WECC and to deliberate regarding decisions the Board may be called upon to make regarding the nomination, qualification, appointment, or removal of a member of the Board of Directors; 2) to discuss pending or proposed litigation and to receive confidential attorney-client communications from legal counsel; and 3) to receive and discuss any information that is privileged, trade secret, cybersecurity, critical energy infrastructure information (as defined by the FERC), protected from public disclosure by law or that the Board determines should be confidential in order to protect a legitimate public interest.

7.6.1.1 Attendance by an Affected Director. Closed sessions of the Board may not be attended by a Director under the following circumstances: 1) where the qualifications or performance of the Director or the Director's spouse or children are being discussed; 2) where the Director is employed by an entity that is or is likely to become a party to the litigation being discussed; and 3) where the Director or the Board determines that the Director would have a serious and substantial conflict of interest by becoming privy to confidential attorney-client or trade secret information that is to be presented to the Board in closed session.

7.6.1.2 Announcement of Closed Session. Before adjourning into closed session, the Chair of the Board will announce the purpose of the closed session in a manner that provides the public an understanding of the general subject matter to be discussed but which does not reveal sensitive or personal

information. The Board will not discuss additional items outside the scope of this description.

7.6.1.3 Confidentiality of Closed Session. All Directors and others present will maintain the confidentiality of discussions and decisions made in closed session. The Board will appoint a secretary for closed session to keep a minute book for the purpose of recording the subject matter discussed in closed session and any actions taken in closed session. After a closed session has ended, the Board Chair shall provide the public a general description of the business conducted during the closed session, without breaching the confidentiality of the information used in the session.

7.7 Board Committees.

7.7.1 Governance Committee. The Chair will appoint a Governance Committee that shall: oversee implementation and amendment of these Bylaws and address such other issues pertinent to Governance as the Board may choose to delegate to it. The Chair will designate one of the appointed Directors to be the Chair of the Governance Committee.

7.7.2 Nominating Committee. Constituted as described in Section 6.4.1 of these Bylaws.

7.7.3 Other Board Committees. The Board may appoint such Board committees as it deems necessary from time to time to carry out its business affairs. In appointing such committees, the Board will specify their purpose, membership, voting, notice and meeting procedures and such other direction as the Board may deem appropriate. The Board may appoint one or more Members or other persons to participate in Board committees as full voting members or as non-voting advisory members.

7.7.4 Standards of Conduct for Board Committee Members. Members of Board committees shall comply with the Board Member Standards of Conduct set forth in Appendix A.

8. Member Committees.

8.1 Purpose.

WECC will have committees composed of its Members to advise and make recommendations to the Board. Such committees will include both standing committees required by these Bylaws and such other committees as the Board may choose to create.

8.2 Standing Committees.

WECC will have the following standing committees:

8.2.1 Member Advisory Committee. This committee is comprised of Member representatives elected by the Member Classes, or subclasses, as set forth herein.

8.2.1.1 The committee shall advise the Board on any matters the Board requests the committee to evaluate or consider; and advise the Board on matters as the committee deems appropriate.

8.2.1.2 The committee's Chair or designee will attend the Board's meetings to provide advice, clarifications or respond to Directors' questions. The Board Chair and committee Chair shall develop guiding principles and procedures as necessary, to ensure open, effective, and efficient dialog between the MAC and Board. Such guiding principles and procedures may be amended by the Board and committee's Chairs.

8.2.2 WECC Standards Committee. This committee will oversee the process for responding to requests for Regional Reliability Standards and Regional Criteria in accordance with the Reliability Standards Development Procedures. The WECC Standards Committee is responsible for determining if a request for a Regional Reliability Standard or a Regional Criteria is within the scope of WECC's activities, and for overseeing the drafting, comment and voting process for a Regional Reliability Standard or Regional Criteria. The WECC Standards Committee shall also oversee the process for responding to requests for interpretations of Regional Reliability Standards and Regional Criteria. The WECC Standards Committee shall consist of one member from each of the WECC Standards Voting Sectors set forth in the Reliability Standard Development Procedures, and a member of the WECC Board who shall act as chair of this committee. The WECC Board shall approve a Charter for the WECC Standards Committee that describes the WECC Standards Committee membership selection process.

8.2.3 Planning Coordination Committee. This committee will advise and make recommendations to the Board on all matters within the jurisdiction of WECC pertaining to maintaining reliability through evaluating generation and load balance and the adequacy of the physical infrastructure of the interconnected Bulk Electric System within the Western Interconnection.

8.2.4 Operating Committee. This committee will advise and make recommendations to the Board on all matters within the jurisdiction of WECC pertaining to maintaining reliability through the operation and security of the interconnected Bulk Electric System in the Western Interconnection.

8.2.5 Market Interface Committee. This committee will advise and make recommendations to the Board on the development of consistent Market Interface practices and compatible commercial practices within the Western Interconnection. It will consider matters pertaining to the impact of WECC's reliability standards, practices, and procedures on the commercial electricity

market in the Western Interconnection, and facilitate analysis of the impact of electricity market practices on electric system reliability.

8.3 Other Committees.

8.3.1 The Board may create such other committees as it may desire from time to time. The Board will specify the functions, duties and responsibilities of any such committee at the time of its creation. The Board will also specify the membership rules, quorum requirements, voting levels and meeting and notice requirements at the time of creation. Any changes in the membership rules, quorum requirements, or voting levels of a committee, once established by the Board, will require a seventy-five percent (75%) vote of the Board to alter. The specific function or sunset date for a committee will be designated by the Board at the time of the committee's creation. The committee will terminate its activities upon the completion of its function or the expiration of the date set by the Board.

8.4 [Repealed]

8.5 Procedures for Member Advisory Committee Decision-Making.

8.5.1 Member Advisory Committee (MAC). The committee shall be comprised of three representatives from each of the five (5) Member Classes, for a total of fifteen (15) members.

8.5.1.1 The Board, by resolution, may create up to three additional representative positions on the MAC, to include representation for Entities of the Canadian Provinces of British Columbia, and/or Alberta, and/or the Mexican State of Baja California. The Board resolution shall set forth the terms through which Canadian or Mexican representatives shall be selected and serve.

8.5.2 MAC Member Elections. At the Annual Members Meeting, each Member Class shall conduct elections to elect Class member representatives for the committee. As set forth herein, each Class may subdivide into up to three subclasses for purposes of electing a Class' MAC members.

8.5.2.1 Committee member terms. Each committee member will serve a three year term. Terms shall be staggered such that one of each Class' representative committee member's terms ends each year. Class committee members may have term limits as determined appropriate by the Class or subclass electing such committee member.

8.5.2.2 Subclasses. Each Class will determine the need for diversity within the Class (e.g., geographic, stakeholder issues, etc.) which may lead to the establishment of subclasses. A Class may subdivide into up to three

subclasses. Each Class shall determine to establish or discontinue its subclasses, if any, by majority vote of the members in the Class.

8.5.2.3 Committee member nominations and elections. Only members of each Class, or subclass, if applicable, may nominate and vote on candidates for election as a MAC member representative for their respective Class or subclass.

8.5.2.3.1 A Class or subclass candidate need not be a member of the Class or subclass, neither an employee of a Class or subclass member.

8.5.2.3.2 A quorum of a majority of the members of a Class or subclass must be present in order to elect a MAC member for the Class or subclass; election shall be by simple majority of votes cast.

8.5.2.3.3 Where there are more candidates for election than positions to fill, absentee ballots shall allow voters to order the candidates by order of preference so that their wishes may be honored in case a runoff is required. Absentee ballots shall be counted in the first ballot based on the top choice, or the top two or three choices if more than one seat is being filled. In any runoff election, absentee ballots shall be counted based on the highest preferences indicated for the candidates who remain in the runoff election.

8.5.2.3.4 Other nomination and election procedures, beyond those contained in these bylaws, may be proposed for a Class or subclass. Contingent upon their approval, by the General Counsel, for their submission to Members, they may be adopted for implementation by majority vote of the Member Class or subclass.

8.5.3 MAC Member Vacancy by Resignation or Removal

8.5.3.1 Resignation. At any time, any MAC member may resign from their position by providing written notice of resignation to the MAC Chair. Such notice shall be effective as of the date the notice is submitted to the MAC chair.

8.5.3.2 Removal. The MAC or the Member Class or subclass which elected a MAC member may remove the MAC member prior to completion of the Mac member's term of office as set forth herein:

8.5.3.2.1 Removal by the MAC. The MAC may remove any MAC member for gross negligence, gross misconduct, violation of local, state, provincial, or federal law, or gross failure to carry

out the duties of a MAC member. Such removal will only occur after the affirmative vote of at least two-thirds (2/3) of the MAC members.

8.5.3.2.2 Removal by the Electing Class or Subclass. The electing Member Class or subclass may remove any MAC member representing that respective Class or subclass. Such removal will occur after the affirmative vote of a majority of the Members of the electing Class or subclass.

8.5.3.3 Vacancy. Whenever a MAC vacancy occurs, the MAC Chair shall conduct a proper and effective election, allowing for a reasonable period to select candidates and to organize such an election.

8.5.3.3.1 Whenever a MAC vacancy occurs, the MAC Chair shall, as promptly as feasible, conduct an election consistent with these Bylaws for the Member Class or subclass from which the vacancy arose, allowing for a reasonable period to select candidates and to organize such an election.

8.5.3.3.2 Until an election can be held, the MAC Chair may appoint an interim MAC member to fill the vacancy as may be required to meet the MAC quorum requirements of 8.5.8. The appointee shall serve until an effective election can be held. Any interim appointment must come from Members of the same Class or subclass from which the vacancy arose.

8.5.4 MAC officers. At the Annual Meeting, after incoming MAC members have been duly elected by the Member Classes or subclasses, if applicable, the MAC will elect the MAC Chair and MAC Vice-Chair from the MAC members. The Chair and Vice-Chair must represent different Classes, and shall serve one year terms, measured from the Annual Meeting to the next Annual Meeting. In the event of the resignation or removal of the Chair or Vice-Chair, the MAC members shall, at their next regular or special meeting, whichever is sooner, elect a new MAC Chair or MAC Vice-Chair, respectively.

8.5.5 MAC Member Duties. All MAC members shall have a duty to represent the interests of their Member Class or subclass. All MAC members shall maintain regular contact with the members of their Member Class as issues are considered by the MAC, and shall make reasonable good faith efforts to present and discuss both majority and minority opinions from their Member Class on matters before the MAC.

8.5.6 Regular and Special Meetings.

8.5.6.1 Regular meetings. All regular business of the MAC shall occur at MAC meetings which are noticed pursuant to Section 8.5.7. The MAC shall meet in person not less than two times per year, including once in conjunction with the Annual Meeting. The MAC shall establish a regular meeting schedule, which will be made available to the Members and Directors electronically, and available to the public through posting on the WECC website.

8.5.6.2 Special Meetings. Whenever the MAC Chair finds, or upon request to the MAC Chair from any five (5) MAC Members, that there is urgent business requiring MAC consideration or action prior to the next regularly scheduled meeting, then a special meeting shall be called with notice given in accordance with Section 8.5.7.

8.5.7 Notice.

8.5.7.1 Regular Meetings. All regular meetings of the MAC shall require at least twenty-one (21) days written notice to the MAC members, the Directors, and the Members. Such notice shall specify the time and place of the meeting, and an agenda of the business to be conducted including those matters upon which a vote will be taken. Notice of regular MAC meetings shall be effective upon electronic distribution, and shall be posted to the WECC website within one (1) business day of electronic distribution.

8.5.7.2 Special Meetings. Any special meetings of the MAC shall require at least ten (10) days written notice to the MAC members, the Directors, and the Members. Such notice shall specify the time and place of the meeting, and an agenda of the business to be conducted, including those matters upon which a vote will be taken. Notice of special MAC meetings shall be effective upon electronic distribution, and shall be posted to the WECC website within one (1) business day of electronic distribution.

8.5.8 Quorum. No business shall be conducted by the MAC unless a majority of the MAC members is present, including at least one MAC member from each Member Class which elects MAC members (not including subclass designations).

8.5.9 Majority Vote. A decision of the MAC shall be upon a simple majority vote of committee members voting unless otherwise required in other bylaw provisions.

8.5.10 Remote Participation at MAC Meetings. Any or all of the MAC members may participate in any meeting of the MAC electronically or by telephone, or by any other means of communications which enables the MAC members to simultaneously hear one another. Every MAC member participating in a meeting in this manner will be deemed to be present in person at the meeting.

8.5.11 Reporting to the Board. The MAC Chair, or designee, shall provide a report to the Board at each Board meeting detailing the business carried out by the MAC, and advising the Board of MAC recommendations on matters as set forth in Section 8.2.1 herein. In the event that there are dissenting MAC member opinions regarding a matter on which the MAC is advising or providing recommendations to the Board, the MAC Chair, or designee, shall present dissenting opinions and rationales in conjunction with the respective MAC advice or recommendations.

8.5.12 Open Meetings. Except as provided in Section 8.5.13, all regular and special meetings of the MAC will be open to observation by any Member, Director, and/or any member of the public.

8.5.13 Closed Session. Notwithstanding the provisions of Section 8.5.12, after a quorum has been established at any MAC meeting and upon an affirmative vote of two-thirds (2/3) of the MAC members present, the MAC may close an open meeting and reconvene in closed session in the following instances: (1) to receive and/or discuss confidential attorney-client privileged information from WECC's counsel; or (2) to receive and discuss any other information which is privileged, confidential, proprietary, trade secret, or otherwise protected from public disclosure by law.

8.5.13.1 Attendance by an Affected MAC Member. Closed sessions of the MAC may not be attended by a MAC member under the following circumstances: (1) when the qualification or performance of the MAC member is being discussed; (2) when the MAC member is employed by an entity that is or is likely to become a party to the litigation or legal issue being discussed; or (3) when the MAC Chair determines that the MAC member would have a conflict of interest by becoming privy to the privileged or confidential information that is to be presented to or discussed by the MAC in closed session.

8.5.13.2 Attendance by Directors. Any member of the Board may attend a closed session of the MAC unless the topic considered by the MAC concerns the Director.

8.5.13.3 Announcement and Adjournment of Closed Session. Prior to adjourning to a closed session, the MAC Chair will announce the purpose of the closed session in a manner that provides the public an understanding of the general subject matter to be discussed, but which does not reveal privileged, confidential or otherwise sensitive personal information. The closed session then shall be limited in scope to the publicly stated purpose of the closed session. After the closed session has ended, the MAC Chair shall provide the public a general description of the business conducted during the closed session, without breaching the confidentiality of the information used in the session.

8.5.13.4 Confidentiality of Closed Session. All MAC members and any others present at a closed session shall maintain the confidentiality of the information, discussions, and decisions made in closed session. Unless otherwise required, all MAC members and closed session attendees shall execute an appropriate confidentiality agreement provided by WECC's General Counsel. The MAC Chair will appoint a secretary for the closed session to take minutes of the closed session, which shall be delivered to the WECC Corporate Secretary. Minutes of the closed session will be maintained confidential by the Corporate Secretary.

8.5.14 MAC Committees. The MAC may appoint such subcommittees and work groups as it deems necessary from time to time to carry out its business affairs. In appointing such subcommittees or work groups, the MAC will specify, in a charter, their purpose, membership, voting, notice and meeting procedures, and other such direction as the MAC deems appropriate. The MAC may appoint one or more MAC members or other persons to participate in MAC subcommittees or work groups as full voting members or as non-voting advisory members.

8.5.15 MAC meetings and activities will be self-funded by Members with respect to labor and travel expenses. However, WECC and WECC staff will provide facilitation and coordination support, including payment for the expenses of meeting facilities. A MAC member may seek reimbursement, from WECC, for reasonable and actual travel expenses arising from attendance at MAC meetings, consistent with WECC employee travel expense reimbursements, where such MAC member's travel expenses are not reimbursed by any Member or other source.

8.6 Procedures for Committees other than the Member Advisory Committee.

8.6.1 Reports to Board of Directors. Action by a committee will be in the form of a recommendation for Board action except in those instances in which the Board has, by resolution, specifically delegated to a committee the power to take action subject to an appeal to the Board by any Member. The recommendation of a committee must be forwarded to the Board for its action along with any minority or dissenting reports filed with the committee Chair or Vice-Chair.

8.6.2 Subcommittees, Task Forces and Ad Hoc Groups. Any Board or member committee may create such subcommittees, task forces or other ad hoc groups ("subcommittee") as it deems appropriate to carry out the committee's responsibilities consistent with these Bylaws and the direction of the Board. The composition, responsibilities and procedures of such groups shall be specified by the committee as appropriate; provided, however that: 1) the committee may only delegate to such subcommittee responsibilities that are within the scope of the committee's responsibilities pursuant to these Bylaws and direction of the Board; and 2) the subcommittee may only make recommendations to the committee. A committee may create a subcommittee without prior approval of the Board;

provided, however, that the committee shall promptly inform the Board in writing and at the next Board meeting regarding the creation of the subcommittee. The notification to the Board shall include a charter for the subcommittee that describes how members of the subcommittee will be selected, the duties of the subcommittee, and whether the committee has established a sunset date for review of (1) the need for the subcommittee and (2) the charter of the subcommittee.

8.6.3 Committee Officers. The Board will appoint the Chair and Vice-Chair of each committee. The Committee Chair or Vice-Chair will preside over all meetings of the committee and will report recommendations of the committee to the Board of Directors. The Chair and Vice-Chair will be responsible for informing the Board regarding minority opinions and other information required by the Board along with overall committee recommendations. Whenever the committee elects to form a subcommittee to represent regions or address specific tasks, the Chair (or in the absence of the Chair, the Vice-Chair) will have the power to appoint the members of such subcommittee from both members of the committees and non-members. Upon resignation of the Committee Chair, the Vice Chair shall serve as Chair until the Board appoints a replacement. Upon resignation of the Vice Chair, the Chair may appoint a temporary Vice Chair to serve until the Board appoints a replacement. Upon resignation of both the Chair and Vice Chair, the Chair of the Board may appoint one or more temporary replacements to serve until the Board appoints permanent replacements.

8.6.4 Committee Membership. Except as provided in Sections 8.2.2 and 8.6.4.1, any Member of WECC may designate one representative as its committee member to any standing committee or other committee. The WECC Member will have one vote at any committee meeting through that committee member. Any number of other persons may attend a committee meeting, but such persons will have no right to vote without a prior designation of representation by a WECC Member..

8.6.4.1 Dual Representation for Functionally-Separated Members. A Member which has distinct and functionally-separated interests as both a transmission provider and a transmission customer may designate two representatives as committee members to any standing committee, one to represent each functionally separate interest. Each such committee member will have one vote. The privilege granted by this Section is subject to revocation by the Board on a case-by-case basis or generally whenever the Board finds, upon petition from any Member or its own motion, that such dual representation creates unfairness or imbalance within a committee.

8.6.5 Committee Voting and Classes.

8.6.5.1 Classes. For purposes of voting, committees, excluding the WECC Standards Committee and the Member Advisory Committee, will have three classes of membership:

8.6.5.1.1 Transmission Provider Members;

8.6.5.1.2 Transmission Customer Members; and

8.6.5.1.3 States and Provincial Members (Member Class 5).

8.6.5.2 Voting. Except as provided in Section 4.5.2, each committee member will have one vote. In order for a recommendation to be made to the Board, such recommendation must receive a simple majority vote of both: 1) committee members present and voting from the Transmission Provider Class; and 2) committee members present and voting from Transmission Customer Class. The Board will adopt voting and record-keeping procedures to ensure that committee voting is conducted consistent with these Bylaws. This requirement will also apply where decision making power has been delegated to a committee pursuant to Section 6.9.1.

8.6.5.2.1 State and Provincial Votes. The position of the state and provincial Class committee members must be recorded, but the failure of a proposed recommendation or decision to obtain a simple majority vote of the state and provincial committee members will not prevent the recommendation or decision from being posted for due process comment or sent to the Board of Directors.

8.6.6 Notice and Review of Committee Recommendations and Decisions (Due Process). Committee recommendations or decisions delegated to a committee pursuant to Section 6.9.1 will be subject to the due process provisions of this Section. Following a committee's development of a proposed recommendation or decision, the committee will post the proposed recommendation or decision on the WECC website for review and comment by other WECC Members, and other interested parties. The committee will provide all Members e-mail notification of the posting and will allow at least thirty (30) days for comment on the proposal. The committee will consider all such additional input before reaching its final recommendation or decision. If the committee's recommendation or decision changes significantly as a result of comment received, the committee will post the revised recommendation or decision on the website, provide e-mail notification to Members and provide no less than ten (10) days for additional comment before reaching its final recommendation or decision. Upon reaching its final recommendation or decision, the committee will forward it to the Board. Whenever it determines that a matter requires an urgent decision, the Board may shorten any time period set forth in this Section, provided that: 1) notice and opportunity for comment on recommendations or decisions will be reasonable under the circumstances; and 2) notices to Members will always contain clear notification of the procedures and deadlines for comment.

8.7 Procedures for Developing and Voting on Reliability Standards.

8.7.1 Rights and Obligations of WECC Members and Participating Stakeholders. All WECC Members and Participating stakeholders are entitled to participate in the development of and to vote on Reliability Standards, Regional Criteria or revisions, subject to any applicable obligations, limitations and conditions set forth in these Bylaws, and in accordance with the WECC Reliability Standards Development Procedures.

8.7.1.1 Participation. The right to participate in Reliability Standards and Regional Criteria development and voting includes the right to request the development or revision of a Reliability Standard, the right to receive notice of, attend and participate in related WECC discussions, the right to review information relevant to a Reliability Standard or revision, the right to provide written comments on a proposed Reliability Standard, Regional Criteria, or revision, the right to participate in voting on a Reliability Standard, Regional Criteria, or revision and the right to file an appeal requesting review of any decision on a Reliability Standard, Regional Criteria, or revision.

8.7.2 Voting. The procedures and conditions for voting by WECC Members and Participating Stakeholders are set forth in the Reliability Standards Development Procedures.

8.7.3 Board Authority to Address Regulatory Directives. The Board shall have backstop authority to address regulatory directives as described in the Reliability Standards Development Procedures.

8.7.4 Participating Stakeholder Application Process. Any person or entity that is an interested stakeholder may apply to WECC for Participating Stakeholder status and, upon WECC's acceptance of such application, acquire the participation and voting rights set forth above in Section 8.7.1. WECC staff, under the direction of the CEO, will process applications and make the initial determination of eligibility for Participating Stakeholder status. Denial of Participating Stakeholder status may be appealed to the WECC Governance Committee and, if denied by the Governance Committee, to the WECC Board. A person or entity's Participating Stakeholder status will be maintained so long as the Participating Stakeholder continues to meet the requirements set forth in Section 3.24 and participates in at least one WECC meeting per year at which a Reliability Standard or revision is discussed. In the event a person or entity's Participating Stakeholder status lapses due to failure to meet the above minimum participation requirement, the person or entity may restore Participating Stakeholder status by re-applying for Participating Stakeholder status and attending a WECC meeting at which a Reliability Standard is discussed.

8.7.5 WECC Standards Voting Sectors. WECC staff shall confirm eligibility for the WECC Standards Voting Sectors set forth in the Reliability Standards Development Procedures. Decisions of the staff to approve, deny, or restrict the admission of an entity to a voting sector may be appealed to the Governance Committee. Decisions of the Governance Committee to affirm or reverse such decisions of staff may be appealed to the Board.

8.7.6 WECC staff shall require Ballot Body members to identify their affiliations with other Ballot Body members. Affiliates within a single Standards Voting Sector may only have one vote in that Standards Voting Sector. Affiliates within a single Standards Voting Sector must designate a single Affiliate as the group's Ballot Pool member to vote in that Standards Voting Sector.

8.8 Notice of Committee Meetings.

8.8.1 Standing Committees. The committee Chair, with the assistance of the Chief Executive Officer, will ensure that not less than ten (10) days' notice of all standing committee meetings is posted on the WECC website and is also provided to: 1) members of the committee; 2) Participating Stakeholders (if the meeting concerns development or approval of a Reliability Standard or revision); and 3) any WECC Member or member of the public requesting notice. A committee may take up any matter at a duly noticed meeting including matters not expressly identified in the notice; provided, however, that a final recommendation to the Board must be made in accordance with Section 8.6.1.

8.8.2 Other Committees. Notice of other committee meetings will be provided in the manner adopted for such notice by the affected Members and in accordance with the requirements of Section 8.8.1.

8.9 Open Meetings.

All committee meetings of WECC will be open to any WECC Member, Director and for observation by any member of the public, except as set forth in these bylaws or in policies on closed sessions that the Board may adopt for the purpose of preventing public disclosure of information that the Board might more appropriately discussed in closed session.

9. The Chief Executive Officer, Officers, and Employees.

9.1 Designation of Officers and Terms of Office.

WECC will have a Chief Executive Officer, a Secretary, and any other officers specified by the Board from time to time. The Chief Executive Officer will also hold the title of President of WECC if applicable law requires WECC to have a President. Each officer will be appointed by the Board and will serve for the term of office specified in the Board action appointing the officer and until his or her successor is appointed. Any two or more offices may be held by the same person except the offices of Chief Executive Officer and Secretary.

9.2 Chief Executive Officer Qualifications.

The Chief Executive Officer will be a person with senior management level experience and knowledge of bulk power electric transmission systems reliability, planning and operations.

9.3 Standards Applicable to All Employees.

A person may not be an officer or employee of WECC if: 1) the person is also the employee of or has a contractual relationship with any Entity, or any Affiliate of any Entity, that is eligible for membership in WECC; or 2) the person has a financial interest that, in the judgment of the Board or the Chief Executive Officer, creates the fact or appearance of bias, undue influence or lack of objectivity regarding any action or decision of WECC. The Board will adopt Standards of Conduct for officers and employees setting forth their duty of care, duty of loyalty, duty to avoid conflicts of interest and related matters intended to promote their neutrality, objectivity and professionalism. Upon adoption, such standards shall be attached hereto as Appendix B.

9.3.1 Exemptions from the disqualification criteria found in Section 9.3 are as follows:

9.3.1.1 Status as a residential electricity customer will not disqualify a person from employment with WECC.

9.3.1.2 A candidate for Chief Executive Officer or employee of WECC will not be disqualified for owning shares in a mutual fund because the mutual fund owns an interest in a Member or an Affiliate of a Member.

9.3.1.3 The disqualification standards described in Section 9.3 will not apply to disqualify a candidate who is receiving payments from a pension plan of a Member or an Affiliate of a Member in a form other than securities of such Member or Affiliate if the pension plan payments bear no relationship to the economic performance of the Member or Affiliate.

9.3.2 If an officer or employee receives a gift or inheritance of securities in any Member or Affiliate, he/she must resign or dispose of such securities within six (6) months of the date of receipt. Within six (6) months of the time a new Member is added in which an officer or employee owns securities, the officer or employee will resign or dispose of those securities.

9.4 Employment.

The Chief Executive Officer will be employed by the Board of Directors and will serve at the Board's pleasure. Any contract of employment with a Chief Executive Officer will permit the Board to dismiss the officer with or without cause.

9.5 Chief Executive Officer's Duties.

Subject to the Board's direction, the Chief Executive Officer or his/her designees will have the following duties, among others:

9.5.1 Execute policies at the direction of the Board and be responsible to the Board for the performance of the WECC functions described in Section 2;

9.5.2 Hire and fire staff within the constraints of the annual budget;

9.5.3 Perform administrative duties, such as preparing annual budgets for the approval of the Board, making employment decisions and ensuring conformance with regulatory requirements;

9.5.4 Develop and implement employment policies and standards of conduct; and

9.5.5 Accept or reject membership applications in accordance with the criteria of these Bylaws.

9.6 Secretary's Duties.

9.6.1 Maintain Member and Affiliates Lists. The Secretary will maintain continuously updated lists of all Members and Affiliates.

9.6.2 Maintain Official Records. The Secretary will keep minutes of all WECC Board and Member meetings and will receive and maintain minutes of committee meetings and all other official records of WECC. Within five (5) business days after any vote taken by Members, the Board, a Class or any committee, the Secretary will provide notice to all Members and Participating Stakeholders (if applicable) of the results of such a vote through postings on the website, email and/or other means of communication.

9.6.3 Maintain Website. The Secretary will oversee the creation, maintenance, and updating of the WECC's website and the information published through it.

10. Dispute Resolution.

Except as may be otherwise provided herein, and subject to the conditions set forth in Appendix C, Section A.1, disputes between Members and/or WECC will be resolved pursuant to the WECC Dispute Resolution Procedures set forth in Appendix C. Matters subject to the jurisdiction of the WECC Compliance Hearing Body are not subject to the procedures in Appendix C.

11. Costs and Finances.

11.1 Funding of Reliability Activities.

11.1.1 U.S. Statutory Funding. WECC shall fund all activities undertaken pursuant to Section 215 of the Federal Power Act in accordance with the funding provisions and procedures of that law and related FERC regulations and orders. The Board shall approve a budget for such activities in time for submission to the ERO and

to the FERC for approval of such funding in accordance with applicable requirements.

11.1.2 International Funding. WECC shall fund reliability activities undertaken in accordance with any agreements it enters into with Canadian or Mexican Entities. Specifically:

(a) Subject to (b), in the event that a Canadian or Mexican Entity seeks membership in the WECC, that Entity may elect to negotiate an agreement with WECC that provides the terms upon which that Entity will become a Member and, among other things, participate in and/or fund WECC. In such a case and unless agreed otherwise, the Canadian or Mexican Entity shall not be a Member of WECC and shall not have an obligation to fund activities undertaken by the WECC until the terms of such agreement are executed.

(b) Section 11.1.2(a) shall not apply to any Canadian or Mexican Entity that is a Member as of the date of the approval of these WECC Bylaws. Existing Canadian or Mexican Members shall continue as Members in accordance with the terms and conditions of their membership as of the date of the approval of the WECC Bylaws, including the terms and conditions of any agreements in place as of the date of the approval of these WECC Bylaws. Nothing in the Section precludes existing Canadian or Mexican Members from negotiating an agreement with WECC that modifies the terms of its participation in and funding of WECC at any time.

11.1.3 Equitable Allocation of Funding. In adopting budgets for the costs of reliability activities, the Board shall endeavor to achieve an equitable allocation as between funding through Sections 11.1.1 and 11.1.2 based upon the net energy to load and other relevant factors consistent with applicable law, the Delegation Agreement and any International Reliability Agreements.

11.2 Dues.

The Board may require Members and Participating Stakeholders to pay nominal annual dues consistent with applicable FERC requirements (or those of International Reliability Agreements as applicable) to cover reasonable costs of membership and/or participation in standards development that are not funded through Sections 11.1.1 or 11.1.2. Initial dues of a Member or Participating Stakeholder will be submitted with a completed application for membership or Participating Stakeholder status and will be for the prorated share of the full annual amount based on the Member's or Participating Stakeholder's actual months of membership or participation in the calendar year. In determining nominal dues, the Board may consider all relevant factors including, but not limited to, the ability of different classes of membership or Participating Stakeholders to pay such dues. The Board may also reduce, defer or eliminate the dues obligation of an individual Member or Participating Stakeholder for good cause shown.

11.3 Funding of Non-Statutory Activities.

To the extent that WECC elects to fund any activities not eligible for funding pursuant to Sections 11.1.1 and 11.1.2, it shall do so through the use of service fees, charges or dues applicable to the persons or entities that voluntarily participate in such activities. Participation in or funding of such activities shall not be a condition of membership in WECC.

12. Amendments to these Bylaws.

These Bylaws may be amended by either the Board or by the Members in accordance with the following procedures.

12.1 Amendment by the Board.

Except for those provisions described below, the Board may approve an amendment of the Bylaws after providing not less than thirty (30) days' notice of the proposed amendment to all Members. Approval of such an amendment requires the affirmative votes of not less than two-thirds (2/3) of the Directors in office. Such amendment will become effective sixty (60) days after its approval by the Board (1) unless the vote is appealed to the Members prior to the sixtieth day, or (2) subsequent regulatory approval is required. A Member appeal shall be sufficient to hold implementation of an amendment if a majority of any Class files a petition with the Secretary seeking appeal of such amendment. If such an appeal is received, the membership will vote on whether to rescind the Board approved amendment at the next Annual Meeting unless the Board calls a special meeting of the Members beforehand. An appeal will only be successful if a majority of all Members and a majority (three of five) of Member Classes vote to rescind the amendment. If the appeal vote is not successful, then the amendment will be deemed approved as of the day of the failed Membership vote. If subsequent regulatory approval is required for the amendment, then the amendment shall be effective upon the effective date of such approval.

12.1.1 Notwithstanding the foregoing, both Board and Member approval is required to amend provisions of these Bylaws concerning Sections 1.1 and 1.2; Section 4.2; Sections 6.2 through 6.8, inclusive; Section 7.2; Section 10; Sections 12.1 through 12.4, inclusive; Appendix C, and any other sections as may be required by Utah law. In such case, the Board shall first vote on the proposed amendment. If approved by the Board by the majority specified in Section 12.1 necessary to attain Board approval, the amendment must then be noticed to Members at least sixty (60) days prior to the Annual Meeting or a Special Member Meeting at which the Member vote will occur. The amendment will then be approved if approved by two thirds (2/3) or more of the Members who vote upon such amendment.

12.2 Amendment by the Members.

Upon petition filed with the Secretary by any Member or Director, at any Annual Meeting the Members may amend any provision of these Bylaws; provided: 1) the proposed amendment has first been presented to the Board and not adopted (this provision will not apply to amendments which the Board is prohibited from adopting); 2) Members have received not less than sixty (60) days' notice of the proposed amendment,

the reasons there for and a statement of the Board's position regarding it; and 3) the amendment receives the affirmative votes of not less than two-thirds (2/3) of all Members and a majority of Member Classes.

12.3 Amendments in Response to Mandatory Membership.
If at any time, pursuant to legislation or otherwise, membership becomes mandatory for some or all Members, upon the request of the affected Member(s) the Board will consider amendments to these Bylaws appropriate to such mandatory membership.

12.4 Amendments proposed by FERC.
FERC, upon its own motion or upon complaint, may propose an amendment to these Bylaws pursuant to 18 C.F.R. § 39.10(b).

13. Termination of Organization.

WECC may be terminated upon a vote of a majority of the Members in accordance with the provisions of Utah law, the Federal Power Act and the requirements of the Delegation Agreement and applicable International Reliability Agreements. Immediately upon such a vote, the Board will, after paying all debts of WECC, distribute any remaining assets in accordance with the requirements of Utah law, the Internal Revenue Code and these Bylaws.

14. Miscellaneous Provisions.

14.1 Limitation on Liability.
It is the express intent, understanding and agreement of the Members that the remedies for nonperformance expressly included in Section 4.8 hereof shall be the sole and exclusive remedies available hereunder for any nonperformance of obligations under these Bylaws. Subject to any applicable state or federal law which may specifically limit a Member's ability to limit its liability, no Member, its directors, members of its governing bodies, officers or employees shall be liable to any other Member or Members or to third parties for any loss or damage to property, loss of earnings or revenues, personal injury, or any other direct, indirect, or consequential damages or injury which may occur or result from the performance or nonperformance of these Bylaws, including any negligence, gross negligence, or willful misconduct arising hereunder. This Section 14.1 of these Bylaws applies to such liability as might arise between Members under these Bylaws. This Section 14.1 does not apply to parties to the Agreement Limiting Liability Among Western Interconnected Systems ("WIS Agreement") with respect to matters covered by the WIS Agreement and does not apply to any liability provision in any other agreement.

14.2 Indemnification.
WECC shall indemnify and hold harmless its Directors, officers, employees, agents and advisors against any and all damages, losses, fines, costs and expenses (including attorneys' fees and disbursements), resulting from or relating to, in any way, any claim, action, proceeding or investigation, instituted or threatened, arising out of or in any way relating to any action taken or omitted to have been taken (or alleged to have been taken or omitted to have been taken) by such person in connection with actions on behalf of WECC, and against any and all damages, losses, fines, costs and expenses (including attorneys' fees and disbursements) incurred in connection with any settlement of any

such claim, action, proceeding or investigation unless such action of such person is determined to constitute fraud, gross negligence, bad faith or willful misconduct with respect to the matter or matters as to which indemnity is sought.

14.3 No Third Party Beneficiaries.

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

14.4 Informal Inquiries for Information.

Nothing in these Bylaws shall preclude: 1) a Member from making an informal inquiry for information outside of the procedures outlined in Section 4.6.11 hereof to another Member and 2) that other Member from responding voluntarily to that informal inquiry, provided, however, that any such response to an informal inquiry for information shall not be binding upon that other Member and shall be used by the Member making the informal inquiry for informational purposes only.

15. Incorporation.

WECC shall organize itself as a non-profit corporation pursuant to the laws of the state of Utah regarding non-profit corporations under the name "Western Electricity Coordinating Council." All Members agree to take no actions that would contravene the ability of WECC to maintain its status as a non-profit corporation existing pursuant to the Utah Act. The Board shall adopt these Bylaws as the Bylaws of WECC as a non-profit corporation.

WECC is intended to qualify as an organization described in Section 501(c)(4) of the Internal Revenue Code. No part of any net earnings of WECC shall inure to the benefit of any Member or individual. Upon liquidation, to the extent consistent with the Internal Revenue Code and Utah law, any monies remaining from assessments paid by Members for the costs of WECC shall be rebated to Members in proportion to their payments. Any remaining assets of WECC shall be transferred to another organization exempt from tax under Section 501(a) of the Internal Revenue Code, or government agency, promoting the same purposes as WECC, as designated by the Board.

16. Governing Law.

Unless otherwise agreed, if any conflict of law arises under these Bylaws among the Members, the laws of the United States of America shall govern, as applicable. The venue for any legal action initiated under these Bylaws shall be the city and state (or province) in which the headquarters of WECC is located.

17. WECC Transition

The provisions of this Section shall apply to that period of time and activities associated with the transition of WECC from a hybrid Board of Directors to an independent Board of Directors with a Member Advisory Committee.

17.1 Board of Directors transition.

17.1.1 The transition of WECC governance from a hybrid Board to an independent Board of Directors will be effective upon the effective date of Federal Energy Regulatory Commission approval of Section 6.1 establishing an independent Board ("Effective Date"). The non-affiliated directors of WECC, whose terms extend past the Effective Date, so willing to continue to serve, shall form part of the initial cadre of independent Directors. These continuing Directors shall be entitled to serve the remainder of their respective three-year terms of office.

17.2 Transition Exceptions

The nomination, election and term of additional independent Directors shall be in conformance with the requirements of these bylaws, as amended, except:

17.2.1 The requirement that the Nominating Committee notify the Board Chair of the committee's nominations sixty (60) days prior to an Annual Meeting shall not apply.

17.2.2 Appointments of Member Advisory Committee members to the Nominating Committee shall be made such that no one class can occupy more than one seat at a time and cannot have a representative on the committee more than two years in a row.

17.2.3 Director positions of non-affiliated directors of WECC, whose terms extend beyond the Effective Date, but whose directors resign or indicate they will resign prior to the Effective Date, will be filled through the same nomination and election process used to select additional independent directors as provided above.

17.2.4 Those Directors first elected as a result of this transition from a hybrid to an independent Board will draw lots to determine their term length determined to achieve the staggered terms required by Section 6.3.

17.2.5 The nomination and election of a number of additional Directors needed to seat the entire Independent Board as described in section 6.4 as of the Effective Date may occur prior to the Effective Date. While the nomination and election of an individual to a director position may occur prior to the Effective Date, such nomination and election shall have the full force and effect of these bylaws after the Effective Date.

17.3 Member Advisory Committee transition

17.3.1 Initial Formation. When there is a meeting where Members vote to amend the WECC bylaws to provide for a Member Advisory Committee (MAC), the MAC will initially be constituted through elections conducted in conjunction with the same meeting.

17.3.2 Election of the initial MAC member representatives shall be as provided in these bylaws, as amended, except:

17.3.3 Where what had been the Class Seven membership category is combined with the Class Three membership category, Class Seven Members will indicate, prior to the meeting, whether they intend to continue participation in WECC as a member of the newly combined Class Three category. Entities so indicating will be considered members of Class Three for purposes of the initial formation of the MAC and shall be entitled to participate in elections for Class Three member representatives of the MAC.

17.3.4 Member Classes will not be allowed to subdivide into subclasses for purposes of electing class representative MAC members at the meeting where the MAC is initially formed and where initial MAC member elections are conducted.

17.3.5 The terms of each Class' three (3) initial Class representative members on the MAC shall be allocated, by the drawing of lots, such that the intended staggered terms for MAC members will be obtained, with one of a Class' initial MAC member representatives serving an initial term of one year, another two years, and another three years.

APPENDICES

A. Board Member Standards of Conduct

B. Officers and Employees Standards of Conduct

C. WECC Dispute Resolution Procedures

Appendix A
Standards of Conduct for
Members of the WECC Board of Directors

By accepting appointment to the Board of Directors (the "Board") of the Western Electricity Coordinating Council ("WECC"), a Director agrees to abide by the duties required of corporate directors and trustees. Utah law (and similar law in other states) imposes quasi-fiduciary duties of care and loyalty on all corporate directors or trustees, including directors and trustees of nonprofit corporations. For as long as he or she remains a member of the Board of Directors of WECC, a Director will abide by the following standards of conduct.

I. Duty of care. The Directors of a corporation are bound to use due care and to be diligent in respect to the management and administration of the affairs of the corporation. This duty of care is generally thought to have two components: the time and attention devoted to corporate affairs and the skill and judgment reflected in business decisions.

A. Each Director will regularly attend Board of Directors meetings, digest the materials sent to him or her, participate in Board discussions and make independent inquiries as needed.

B. In voting on any matter before the Board or otherwise acting in his or her capacity as a Director, each Director will:

1. make reasonable inquiry to inform himself or herself of the nature and consequences of the matter or action at issue;

2. exercise, at a minimum, the degree of care, skill, and diligence that an ordinarily prudent business person would exercise under similar circumstances; and

3. act in a manner the Director, in the exercise of his or her independent judgment, believes to be in the best interests of WECC and the membership of WECC, taken as a whole.

C. In exercising the duty of care described in paragraphs IA and B above, a Director has the right to rely on statements by the persons immediately in charge of business areas of WECC, to rely on professionals and experts (such as engineers, accountants and lawyers) and to rely on committees of WECC, unless facts or circumstances appear which would prompt further concerns of the ordinarily prudent person.

II. Duty of loyalty. The duty of loyalty imposes on a Director the obligation to remain loyal to WECC, acting at all times in the best interests of WECC and its Members as a whole and unhampered by any personal pecuniary gain. This duty does not preclude a Director from being employed in a competing or related business so long as the Director acts in good faith and does not interfere with the business of WECC.

A. Each Director will carry out his or her duties as a Director in good faith.

B. Each Director will refrain from using any influence, access, or information gained through his or her service as a Director to confer any improper personal benefit (financial or otherwise) upon himself or herself, any family member, or any person living in the Director's household.

C. Each Director will refrain from using any influence, access, or information gained through his or her service as a Director to confer an improper benefit (financial or otherwise) on any organization:

1. for which the Director serves as an officer, director, employee, consultant, or in any other compensated or management position; or

2. in which the Director or any family member or person living in the Director's household has a material financial interest (whether as a shareholder, partner, or otherwise).

D. To the extent permitted by law, each Director will maintain the confidentiality of:

1. any confidential or proprietary information of WECC disclosed or available to the Director;

2. any confidential or proprietary information of WECC Member(s) to which the Director has access by virtue of his or her status as Director; and

3. any confidential or proprietary information of third parties that has been provided to WECC or the Board on condition of confidentiality.

E. Conflicts of Interest. Because conflicts of interest may arise from time to time, specific guidelines are provided. In general, conflicts of interest involving a Director are not inherently illegal nor are they to be regarded as a reflection on the integrity of the Board or of the Director. It is the manner in which the Director and the Board deal with a disclosed conflict that determines the propriety of the transaction.

Directors of nonprofit corporations may have interests in conflict with those of the corporation. The duty of loyalty requires that a Director be conscious of the potential for such conflicts and act with candor and care in dealing with these situations.

The following are guidelines for Directors with actual or potential conflicts of interest:

1. Each Director has a responsibility to recognize potential conflicts of interest and to be guided when acting as a Director by his or her independent judgment of what is in the best interests of WECC and the membership of WECC, taken as a whole. If any Director has questions about whether a conflict of interest exists, he or she may make inquiry to the Chief Executive Officer of WECC for advice.

2. Potential conflicts of interest may arise because of a Director's private, individual interests (personal conflicts of interest) or because of relationships the Director may have with other organizations or interest groups (organizational conflicts of interest). Current or past employment or other compensation-based relationships with one or more WECC Members are examples of potential organizational conflicts of interest. Whether a potential conflict of interest is personal or organizational, in all cases involving WECC affairs a Director's conflicting interests are subordinate to those of WECC and the membership of WECC, taken as a whole.

3. Personal conflicts of interest.

   a. Personal conflicts of interest exist if a Director, a member of the Director's family, or a person sharing the Director's household: 1) has a material financial interest in a matter or transaction that comes before the Board for action; or 2) stands to receive a benefit (in money, property, or services) from a transaction involving WECC to which the person is not legally entitled.

   b. In cases of personal conflicts of interest, the affected Director's obligations are to:

      (1) disclose to the Board, before the Board acts with respect to that matter, the material facts concerning the Director's personal conflict of interest; and

      (2) refrain from voting, and from attempting to influence the vote of any other Director(s), in those matters in which the Director has a personal conflict of interest.

4. Organizational conflicts of interest.

   a. An organization has a "direct" conflict of interest if a decision by the Board would confer material benefits on that organization that other WECC Members would not share, or impose material detriments or costs on that organization that other WECC Members would not share. The fact that many if not all Members are affected to some extent by Board decisions on core issues such as standards, new transmission lines and their ratings, does not create or constitute a "direct" conflict of interest.

   b. It is not a "direct" conflict of interest for a Director to be associated with an organization or an interest group that may stand to benefit from decisions made or actions taken by the Board, so long as the Director does not attempt to use his or her position as a Director to confer special

benefits on associated organizations or interest groups when other WECC Members would not share in those benefits.

c. In cases of potential "direct" organizational conflicts of interest, the affected Director's obligations are to:

(1) disclose to the Board, before the Board acts with respect to the matter, the material facts concerning the organizational conflict of interest; and

(2) refrain from voting and from attempting to influence the vote of any other Director(s) with respect to the proposed action or decision.

Appendix B
Officers and Employee
Standards of Conduct

By accepting employment with the Western Electricity Coordinating Council ("WECC"), an Employee agrees to abide by these Standards of Conduct. For the purpose of these Standards, an Employee includes each and all officers, employees and substantially full-time consultants and contractors of WECC.

I. Duty of care. The Employees of WECC are bound to use due care and to be diligent in respect to the management and administration of the affairs of the corporation. This duty of care is generally thought to have two components: the time and attention devoted to corporate affairs and the skill and judgment reflected in business decisions.

Employees shall not have any outside employment that limits in any way their ability to fulfill their employment responsibilities to WECC. If an Employee has any question about whether outside employment is consistent with this standard, they should consult with their supervisor.

II. Duty of loyalty. The duty of loyalty imposes on an Employee the obligation to remain loyal to the WECC, acting at all times in the best interests of WECC and its Members as a whole and unhampered by any personal pecuniary gain. WECC expects all Employees to avoid adversely affecting the public's confidence in the integrity and reputation of WECC. Any conduct or activities of any Employee should be capable of being justified and withstanding public scrutiny.

A. Each Employee will carry out his or her duties as an Employee in good faith, with integrity and in a manner consistent with these Standards and all applicable laws governing WECC.

B. Each Employee will refrain from using, or creating the appearance of using, any influence, access, or information gained through his or her service as an Employee to confer any improper personal benefit (financial or otherwise) upon himself or herself, or Family Member.[1] Employees shall not accept gifts or entertainment that would tend to affect, or give the appearance of affecting, the performance of their duties; provided, however, that Employees may accept de minimus food or entertainment or non-cash gifts received as part of a social or special occasion in amounts not to exceed $1000 per source per year.

C. Each Employee will refrain from using, or creating the appearance of using, any influence, access, funds or information gained through his or her service as an Employee to confer an improper benefit (financial or otherwise) on any organization. The obligation to avoid the appearance of impropriety shall apply in particular to any organization:

1 For purposes of these Standards, a Family Member includes a spouse, domestic partner, child of the Employee, or a relative living in the same home as the Employee.

1. for which the Employee is serving or has in the past served as an officer, director, employee, consultant, or in any other compensated or management position; or

2. in which the Employee, or Family Member has a material financial interest known to the Employee (whether as a shareholder, partner, or otherwise).

D. Employees shall not use their WECC position, WECC funds or WECC resources to support any political party, candidate or proposition except as expressly authorized by the Board.

E. To the extent permitted by law, each Employee shall maintain the confidentiality of:

1. any confidential or proprietary information of WECC disclosed or available to the Employee;

2. any confidential or proprietary information of WECC Member(s) to which the Employee has access by virtue of his or her status as Employee; and

3. any confidential or proprietary information of third parties that has been provided to WECC or the Board on condition of confidentiality.

F. Conflicts of Interest. The following conflicts of interest policy shall apply to all WECC Employees. Conflicts of interest may arise from time to time. In general, conflicts of interest involving an Employee are not inherently illegal, nor are they to be regarded as a reflection on the integrity of WECC or of the Employee. It is the manner in which the Employee and WECC deal with a disclosed conflict that determines the propriety of the transaction. The following are guidelines for Employees with actual or potential conflicts of interest:

1. In general, personal conflicts of interest exist if an Employee, or a Family Member, has a material financial interest in a matter or transaction that comes before WECC for action, or stands to receive a benefit (in money, property, or services) from a transaction involving WECC to which the person is not legally entitled. For purposes of determining whether stock constitutes a material financial interest, see Paragraph F(6) below.

2. Organizational conflicts of interest exist if an Employee, or a Family Member, has a relationship with an organization or interest group that would cause a reasonable person to believe such Employee's judgment, loyalty, or objectivity might be influenced in a way that is adverse to the interests of WECC.

3. Where there is any question about potential conflicts of interest, the Employee shall disclose to the Chief Executive Officer as soon as possible and prior to when WECC takes action with respect to that matter, the material facts concerning the Employee's personal conflict of interest, and refrain from participating in, or from

attempting to influence the action of any Directors or Employee(s) of WECC regarding those matters in which the Employee has a conflict of interest.

4. No Employee may be an employee, director of, or consultant to or provide services to or be associated in any way with any WECC Member without full disclosure to, and written consent of, the Chief Executive Officer. To the extent that an Employee becomes aware that a Family Member is or will in the future be engaged in activity described in this Paragraph F(4), the Employee shall promptly notify the Chief Executive Officer, who shall review all the material facts and determine whether they constitute a conflict of interest pursuant to Paragraphs F(1) and F(2), above.

5. No Employee shall participate in any electric energy transaction other than for ordinary personal use except to the extent necessary to, and consistent with, the functions of WECC. Participation in an energy transaction includes, but is not limited to, purchasing, selling, marketing, or brokering of electricity, ancillary services, electricity transmission or electricity distribution. To the extent that an Employee becomes aware that a Family Member is or will in the future be engaged in activity described in this Paragraph F(5), the Employee shall promptly notify the Chief Executive Officer who shall review all the material facts and determine whether they constitute a conflict of interest pursuant to Paragraphs F(1) and F(2), above.

6. All Employees shall promptly disclose to the CEO and the Chair of the Board any direct or indirect financial interest in excess of $5,000 (including the direct or indirect ownership of securities) held by the Employee or a Family Member living with the Employee[2] in any Electric Line of Business entity as defined in Section 3.15 of the Bylaws doing business in the Western Interconnection. Upon such disclosure, the CEO and the Chair of the Board shall determine whether such financial interest constitutes a conflict of interest, or the appearance thereof, in light of the duties of the Employee, the ability to divest such financial interest without undue hardship and the totality of the circumstances. In response to such disclosure, the CEO and the Chair may impose such remedies as are reasonable under the circumstances and consistent with section 9.3 of the Bylaws. Such remedies may include, but are not limited to, restrictions on the Employee's duties or involvement in certain matters, transfer of the Employee to another position, broader disclosure of the financial interest, voluntary or mandatory divestiture of the interest (in whole or in part) or other remedies. Pursuant to section 9.3.2 of the Bylaws, if an Employee (not a Family Member) receives a gift or inheritance of securities of a Member of WECC, or if a new Member joins WECC in which the

2 Nothing in this section shall require an Employee to investigate the financial interests of Family Members not living with the Employee. However, to the extent known to the Employee, the financial interests of a Family Member not living with the Employee may create a potential conflict of interest (or appearance thereof) subject to Sections II(B) and/or II(F)(1) of these standards, in which case disclosure pursuant to Section II(F)(3) is appropriate.

Employee (not a Family Member) holds securities, the Employee must resign or divest such securities within six months thereafter. For the purposes of this section, none of the following shall constitute a direct or indirect financial interest:

a. An interest that exists through diversified mutual funds;

b. An interest that exists for six months following receipt of a gift or inheritance of securities of a Market Participant or acceptance of employment with WECC, whichever is later (provided that employees of the WSCC shall have two years from WECC organizational meeting to divest securities in their possession as of that date);

c. An interest that exists through a pre-existing participation in a qualified defined benefits pension plan or health benefits plan of a Market Participant so long as the benefits under such plan do not vary with the economic performance or value of the securities of such Market Participant.

Appendix C

WECC Dispute Resolution Procedures

C. DISPUTE RESOLUTION.

C.1 Obligation To Comply with Dispute Resolution Procedures. If any dispute concerning one or more issues identified in Section C.2 below arises between a Member and one or more other Members, or between one or more Members and WECC, all of the parties to the dispute shall, to the extent permitted by law, be obligated to comply with the dispute resolution procedures specified in these Bylaws (except to the extent all of the parties to the dispute may agree otherwise as provided in Section C.4 below). Only Members and WECC have the right to invoke the provisions of this Appendix C and, except where all affected parties have separately agreed otherwise with respect to a particular dispute, only Members and WECC are obligated to carry out the dispute resolution procedures set forth herein. Any dispute subject to the provisions of this Appendix C to which WECC is made a party shall be subject to the additional requirements specified in Section C.3 below if the dispute is initiated by a party other than WECC. To the extent permitted by law (and except as otherwise permitted by the provisions of Section C.6.3), no party to a dispute subject to the provisions of this Appendix C may pursue any other available remedy with respect to the dispute until all of the parties to the dispute have fully complied with the dispute resolution procedures specified herein, *provided, however,* that if any party to a dispute subject to the provisions of this Appendix C refuses to comply with the dispute resolution procedures specified herein, all other parties to the dispute shall subsequently be relieved of any further obligation to comply with these dispute resolution procedures before pursuing other remedies in connection with that dispute.

C.2 Issues Subject to Dispute Resolution Procedures. Any dispute between or among the parties identified in Section C.1 above (that the parties to the dispute do not resolve through negotiations between or among themselves) shall be subject to the dispute resolution procedures set forth in this Appendix C if the dispute concerns: (i) the application, implementation, interpretation, or fulfillment of any guidelines, criteria, policies, procedures, or Bylaws of WECC or the North American Electric Reliability Council (or any successor organization); or (ii) any matter specified in Section C.6.2 below; except that any matter that is subject to the jurisdiction of the WECC Compliance Hearing Body is not subject to the requirements of this Appendix C. Notwithstanding the foregoing provisions of this Section C.2, however, neither WECC nor any Member shall be obligated to comply with the dispute resolution procedures of these Bylaws if: (a) the dispute is between two or more Members (or WECC), all of which, at the time of the dispute, are parties to the WECC Reliability Management System Agreement and the matter is within the scope of the dispute resolution procedures set forth in that agreement; or (b) the dispute is between two or more Members, all of which, at the time of the dispute, are parties to a separate agreement or treaty or where an applicable tariff, rate schedule, or other legal obligation of one of the parties provides for the parties to resolve the dispute in a manner other than in accordance with the provisions of this Appendix C of the Bylaws.

C.3 Limitations on Members' Rights To Make WECC a Party to a Dispute. In addition to the other provisions of this Appendix C of the Bylaws, any dispute (other than a dispute initiated by WECC) to which WECC is made a party shall be subject to the limitations set forth in Sections C.3.1 and C.3.2 below.

C.3.1 Bases for Using Dispute Resolution Procedures To Challenge WECC Action. Subject to any limitation set forth in these Bylaws or in applicable statute, regulation or FERC order, one or more Members may use the dispute resolution procedures specified in this Appendix C to challenge any final action of WECC only on one or more of the following bases: (i) the action is contrary to applicable law or regulation; (ii) the action is contrary to WECC's Articles of Incorporation or these Bylaws (including WECC's purposes as set forth in those documents); (iii) the action was taken in violation of applicable procedures of WECC governing that action; or (iv) the action encompasses a decision in which there was plain error material to the decision. For purposes of this Appendix C, action taken by WECC shall be deemed final if: (a) the action has been taken or adopted or approved or accepted by WECC's Board of Directors (other than by a motion specifically providing that the action is conditional or will have temporary application not to exceed six months); (b) all conditions specified to make any conditional action of WECC's Board of Directors effective have been fulfilled; or (c) the action has been taken or adopted or approved or accepted by a committee, subcommittee, task force, or other group or person acting under authority of WECC without any provision making the action subject to further approval or adoption or acceptance by the Board of Directors. Nothing contained in this Appendix C shall limit any rights any Member (or any other party) may have under applicable law or regulation to initiate or participate in an administrative or legal action to which WECC is made a party in accordance with applicable provisions of law or regulation.

C.3.2 Obligation to Bear WECC's Share of Facilitator Costs. If one or more Members initiate a dispute under this Appendix C to challenge an action of WECC, the Member(s) initiating the challenge shall be obligated to bear all of the costs of facilitators' services incurred to comply with the requirement of Section C.5 below, except to the extent WECC agrees to pay a share of the costs of facilitators' services.

C.4 Ability to Modify Dispute Resolution Procedures by Agreement. Any provision of the dispute resolution procedures set forth in this Appendix C may be modified, waived, or omitted by agreement of all of the parties to the dispute. Parties to a dispute subject to these provisions are obligated to comply with its procedures unless all of the parties to the dispute agree to do otherwise. The manner in which the dispute resolution procedures set forth in this Appendix C may be varied include (by way of example and not as limitation): the manner of selecting a facilitator or arbitrator; the procedures or time lines to be followed during mediation or arbitration; the grounds or forum or right to appeal an arbitrator's decision; the manner of allocating fees and costs associated with the dispute; whether the parties are obligated to proceed to arbitration if the dispute is not resolved through mediation; and whether a decision rendered through arbitration is binding on the parties. In addition, any dispute that does not fall within the scope specified in Section C.2 above may be resolved according to the procedures set forth in Appendix C of these Bylaws if all of the parties to the dispute agree to do so.

C.5 Mediation.

C.5.1 Notice to Other Parties and WECC's Chief Executive Officer. To initiate the dispute resolution process with respect to a dispute governed by the provisions of

this Appendix C, the Member or WECC that has elected to initiate the dispute shall deliver to all other parties to the dispute and to WECC's Chief Executive Officer (whether or not WECC is a party to the dispute) written notice invoking the dispute resolution procedures set forth in this Appendix C (a "Dispute Notice").

C.5.1.1 The Dispute Notice shall: (i) include a brief, general description of the matter(s) in dispute; (ii) include a complete list of all other Members the party submitting the Dispute Notice intends to make a party to the dispute; and (iii) state whether or not WECC is to be made a party to the dispute.

C.5.1.2 Within five business days of receiving a Dispute Notice, any party to the dispute may elect to deliver a brief supplemental description of the dispute to WECC's Chief Executive Officer.

C.5.1.3 Within 10 business days of receiving an initial Dispute Notice, WECC's Chief Executive Officer shall: (a) publish (or cause to be published) in WECC's newsletter or on its electronic bulletin board a notice containing a list of the parties to the dispute and a summary of the descriptions of the matter(s) in dispute provided by the parties to the dispute; and (b) deliver to each party to the dispute a copy of WECC's then-current standing list of qualified facilitators, knowledgeable in the matters addressed by WECC (as approved by the Board of Directors).

C.5.1.4 No person may be listed on WECC's standing list of qualified facilitators unless the person has agreed to: (i) disclose, at any time the

person is selected to serve as a facilitator under this Appendix C, any personal or financial interest the facilitator may have with respect to the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the facilitator's immediate family members); (ii) disclose any relationship the facilitator may have with any party to the dispute that is not permitted under Section C.5.2 below; and (iii) abide by all applicable provisions of these Bylaws, including restrictions on disclosure of matters discussed and information exchanged during mediation as provided in Section C.5.3 below.

C.5.2 Selection of a Facilitator. Within 10 calendar days after the delivery of a Dispute Notice, the parties to the dispute shall select a neutral facilitator by mutual agreement. If the parties to the dispute cannot agree on a facilitator within 10 calendar days after delivery of a Dispute Notice, the facilitator shall be selected from WECC's standing list of qualified facilitators as follows: The parties to the dispute shall take turns striking names from WECC's standing list of qualified facilitators until there is only one name remaining. (The parties to the dispute shall draw lots to determine the order in which they take turns striking names.) The last person whose name remains on the list shall serve as the facilitator. No facilitator other than a facilitator chosen by agreement of all the parties to the dispute may (i) have a personal or financial interest in the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the facilitator's immediate family

members); or (ii) be (or have an immediate family member who is) a past or present director, commissioner, officer, employee, consultant, agent, or other representative of any of the parties to the dispute. If the facilitator selected through the process of striking names specified above is disqualified under the preceding sentence, the facilitator whose name was stricken last shall serve in his or her place. In addition, if WECC is a party to a dispute initiated by one or more Members, turns striking names from the standing list of qualified facilitators shall alternate between WECC on the one hand and all other parties to the dispute on the other.

C.5.3 Mediation Process. The facilitator and representatives of all of the parties to the dispute shall meet within 14 calendar days after the facilitator has been selected and attempt in good faith to negotiate a resolution to the dispute. Each party's representative designated to participate in the mediation process must have the authority to settle the dispute (or, at a minimum, be authorized to negotiate on behalf of the party and make recommendations with respect to settlement of the dispute if final authority to approve a settlement is reserved to a party's board, executive committee, commission, or other governing body). At the parties' initial meeting with the facilitator, the facilitator shall, after soliciting input from the parties to the dispute, set the schedule for further meetings among the parties to the dispute (subject to the 60-day maximum mediation period specified in Section C.5.6 below). The parties to the dispute shall comply with the schedule set by the facilitator and attempt in good faith at every meeting to negotiate a resolution to the dispute. To the extent permitted by law, neither the facilitator nor any party to the dispute may publicly disclose, rely on, or introduce as evidence in any subsequent arbitration, FERC proceeding, Canadian Regulatory

Authority proceeding, proceeding before a Mexican Regulatory Authority, appeal, or litigation concerning the same or any related dispute: (i) any views expressed or suggestions made by another party to the dispute with respect to a possible settlement of the dispute; (ii) admissions made by another party to the dispute in the course of the mediation proceedings; (iii) proposals made or views expressed by the facilitator; or (iv) the fact that another party to the dispute has or has not indicated willingness to accept a proposal for settlement made by the facilitator. In those cases in which a party to a dispute subject to the provisions of this Appendix C of the Bylaws is a membership organization (including WECC, if applicable), nothing in the preceding sentence shall prohibit that organization from reasonably communicating with its members and governing body to share general information about the dispute, such as the parties, status, disputed issues, and positions of each of the parties with respect to the disputed issues.

C.5.4 Referral for Resolution. With the consent of all parties to the dispute, a resolution may include referring the matter to a technical body (such as a technical advisory panel of WECC) for resolution or an advisory opinion, to arbitration, directly to FERC or, in a dispute involving a Canadian Member, directly to the appropriate Canadian Regulatory Authority, or, in a dispute involving a Mexican Member, directly to the appropriate Mexican Regulatory Authority.

C.5.5 Mediation Participation by WECC Staff When WECC Not a Party. If, during the course of mediation to which WECC is not a party, the facilitator or any party to the dispute wishes to solicit the views of WECC concerning the application, implementation, interpretation, or fulfillment of any guidelines, criteria, standards, policies, or procedures of WECC, the facilitator may request or permit the submission of WECC staff views only if: (i) any participation by WECC staff

takes place exclusively in the presence of all parties to the dispute; (ii) participating WECC staff members agree to be equally available upon request to all parties to the dispute; and (iii) participating WECC staff members agree to comply with the restrictions on disclosure contained in Section C.5.3.

C.5.6 Mediation Deemed at Impasse After 60 Days. If the parties to the dispute have met and negotiated in good faith in accordance with the schedule set by the facilitator but have not succeeded in negotiating a resolution of the dispute within 60 calendar days after the first meeting with the facilitator pursuant to Section C.5.3 above, the parties to the dispute shall be deemed to be at impasse and, except as otherwise provided in Section C.5.6.2 below, shall also be deemed to have fulfilled their obligations under Section C.1 of these Bylaws to fully comply with the dispute resolution provisions before pursuing any other available remedy. If any party participating in the mediation process is subject to a contractual or statutory limitations period with respect to the matter in dispute, and the limitations period will expire before the 60-day period for mediation under this Section C.5.6 is completed, then the parties shall be deemed at impasse on the seventh calendar day preceding the expiration of the shortest applicable limitations period.

C.5.6.1 Disputes Not Subject to Provisions of Section C.6.2. Unless the matter in dispute is subject to the provisions of Section C.6.2 below, at any time after the parties to the dispute are deemed at impasse, the dispute may be submitted to binding arbitration in accordance with the procedures set forth in Section C.7 of these Bylaws (but only by agreement of all of the parties to the dispute). If the matter in dispute is subject to the provisions of Section C.6.2 below, the parties' obligations with respect to submitting the matter to binding arbitration under Sections C.6 and C.7 of these Bylaws shall be as specified in Section C.5.6.2 below. In

all other cases, if the parties to the dispute do not agree to submit the dispute to binding arbitration in accordance with the procedures set forth in Section C.7 of these Bylaws, any party to the dispute may at any time thereafter pursue any other remedy available under regulation, law, or equity (subject to the restrictions on disclosure set forth in Section C.5.3 above).

C.5.6.2 Disputes Covered by Section C.6.2. If the parties to a dispute concerning a matter subject to the provisions of Section C.6.2 either: (i) are deemed at impasse after attempting to resolve the matter through mediation as provided in Sections C.5.1 through C.5.6 above; or (ii) have agreed to submit the matter directly to binding arbitration without attempting to resolve the matter through mediation as provided in Sections C.5.1 through C.5.6 above, the parties to the dispute shall submit the matter to binding arbitration in accordance with the procedures set forth in Sections C.6 and C.7 of these Bylaws.

C.5.7 Costs of Facilitator's Services. Except as otherwise provided under Section C.3.2, the costs of the facilitator's services shall be born equally by all parties to the dispute unless the parties to the dispute agree otherwise, but the parties also intend that the costs of mediation should be taken into account in any resolution proposed through the mediation process.

C.5.8 Notice to WECC of Completion of Mediation. Within 10 calendar days after either: (i) reaching a negotiated resolution through the mediation process set forth in Section C.5; or (ii) reaching deemed impasse in accordance with Section C.5.6 above, the parties to the dispute shall jointly deliver to WECC's Chief Executive Officer a written notice briefly describing the outcome of the mediation process. Promptly after receiving written notice describing the outcome of a mediation conducted in accordance with Section C.5, WECC's Chief Executive Officer shall

publish (or cause to be published) in WECC's newsletter or on its electronic bulletin board a brief description of the outcome of the mediation, together with a list of all of the parties to the dispute.

C.6 General Provisions Relating to Binding Arbitration.

C.6.1 Matters for Which Binding Arbitration is Elective. Except with respect to any dispute that concerns one or more matters specified in Section C.6.2 below, the binding arbitration procedures set forth in Section C.7 may be invoked only by agreement of all of the parties to the dispute to be arbitrated and are solely for the convenience of WECC and its Members. If a dispute governed by this Appendix C does not concern a matter specified in Section C.6.2 below, a party to the dispute shall be deemed to have fulfilled its obligations to comply with Appendix C of these Bylaws (irrespective of whether the parties to the dispute agree to proceed with binding arbitration) to the extent that either: (i) that party has fully performed the obligations set forth in Sections C.1 through C.5.8; or (ii) all of the parties to the dispute have agreed to a different process for resolving the dispute and the agreed-upon process has been fully carried out.

C.6.2 Matters for Which Binding Arbitration Is Obligatory. If a dispute is governed by Appendix C of these Bylaws and is not resolved through the process of mediation in accordance with Sections C.5.1 through C.5.6 above, the parties shall be obligated to submit the matter to binding arbitration in accordance with the procedures set forth in Section C.7 (subject to the limitations on the arbitrator's authority set forth in Section C.6.3 below) if the dispute concerns one or more of the following matters:

C.6.2.1 a decision of WECC's Board of Directors or a Committee of the Board acting on the recommendation of, or on a matter within the jurisdiction of, the Operating Transfer Capability Policy Group ("OTCPG") or successor;

C.6.2.2 a transmission path rating, or a modification to a transmission path rating, assigned to one or more transmission paths operated by a Member (or jointly operated by more than one Member);

C.6.2.3 transmission access, pursuant to Sections 10.1.2, 10.1.3, and 10.5; or

C.6.2.4 any matter that, by vote of both WECC's Board of Directors and WECC's Membership, is designated as a matter to be subject to the provisions of Section C.6.2 of these Bylaws, provided that any matter submitted to WECC's Membership pursuant to this provision must be approved by at least the number of votes required to amend these Bylaws under Section 13.2.

C.6.3 Limitations on Arbitrator's Authority with Respect to Matters Specified in Section C.6.2. Unless all of the parties to a dispute agree otherwise, an arbitrator rendering a decision with respect to any matter specified in Section C.6.2 above shall have no authority to consider or award remedies for past economic harm or damages of any kind, including without limitation actual or direct damages; indirect, consequential, or incidental damages; or exemplary or punitive damages. Nothing in this Section C.6.3 shall: (i) limit any rights that a party to a dispute concerning a matter specified in Section C.6.2 above may have to pursue legal claims for damages or other economic remedies after the arbitrator has rendered

his or her decision on that matter (within the scope of his or her authority under this Section C.6.3); or (ii) limit an arbitrator's authority under Section C.8 below to shift costs or impose monetary sanctions for "good cause" (as that term is defined in Section C.8).

C.6.4 Arbitration Decisions Not To Modify Underlying Rights and Obligations. Unless all of the parties to a dispute agree otherwise, the resolution through binding arbitration of any dispute governed by this Appendix C shall not have the effect of increasing, decreasing, or otherwise modifying WECC's or any Member's obligation to abide by, or ability to enforce or impose penalties or sanctions with respect to, any guidelines, criteria, standards, policies, procedures, decisions, or Bylaws of WECC or any limitation on the foregoing, whether established by law; regulation; judicial, executive, or administrative order, decree, or decision; tariff; contract; course of performance; treaty; or otherwise.

C.6.5 Laws Relating to Binding Arbitration. WECC and its Members recognize that some Members may be subject to laws (including without limitation United States federal or state laws, Canadian or provincial laws, or Mexican laws) that limit or define those Members' ability to agree in advance to be subject to binding arbitration. If a Member has the right or obligation under applicable law to refuse to submit to binding arbitration in connection with any dispute that would otherwise be subject to binding arbitration under Section C.6.2 of these Bylaws, that Member shall not be obligated to comply with the binding arbitration procedures set forth in Sections C.6 and C.7. Any Member subject to any law or other legally binding authority that may limit (or permit the Member to limit) its

obligation to comply with the provisions requiring binding arbitration under Sections C.6 and C.7 or to fully comply with a valid arbitrator's decision rendered in accordance with this Appendix C shall provide notice to this effect to all other disputing parties and WECC's Chief Executive Officer upon initiation of any dispute involving that Member if the dispute is subject to Section C.6.2. Upon receiving a notice under Section C.6.5, any other party to the dispute shall thereafter be relieved of any obligation to comply with the provisions Sections C.6 and C.7 in connection with that dispute, except to the extent that the Member giving notice agrees to be fully bound by procedures governing and results of any arbitration proceeding. If there are more than two parties to a dispute covered by the preceding sentence, however, then all parties to the dispute other than the party giving notice under Section C.6.5 shall make good faith efforts to establish a mutually acceptable approach for resolving among themselves whatever aspects of the dispute can reasonably be resolved through the procedures set forth in this Appendix C without the participation of the party giving notice under Section C.6.5. If any Member fails to submit to binding arbitration, or fails to abide by a valid arbitrator's decision rendered in accordance with this Appendix C, that Member shall thereafter have no right to enforce any of the provisions of Section C.6.2 (concerning obligations to submit specified disputes to binding arbitration) against any other Member or WECC until such time as the WECC Board of Directors, or a delegate designated by the Board, determines that it is appropriate to restore the Member's ability to enforce the provisions of Section C.6.2.

C.6.6 Consistency with Laws, Regulatory Jurisdiction and Orders, Etc. Nothing contained in this Appendix C and no arbitrator's decision rendered in accordance with Section C.7 shall be construed to require or shall otherwise operate to cause any Member or WECC to incur any obligation or take any action that is contrary to: (i) any applicable law or regulation; (ii) any applicable authority, order, decree, rule, or decision of a regulatory, judicial, administrative, executive, or other governmental body having jurisdiction over one or more of the matters or parties subject to this Appendix C or covered by an arbitrator's decision; or (iii) any applicable rate schedule, tariff, treaty, or valid, pre-existing contractual obligation with which any party subject to this Appendix C or covered by an arbitrator's decision is legally obligated to comply.

C.7 Arbitration Procedures.

C.7.1 Notice to WECC of Initiation of Binding Arbitration. Within 10 calendar days after all of the parties to a dispute have agreed (or become obligated under Section C.6.2 above) to submit the dispute to binding arbitration under Sections C.6 and C.7, the parties to the dispute shall deliver written notice to WECC's Chief Executive Officer (an "Arbitration Notice").

C.7.1.1 The Arbitration Notice shall: (i) include a brief, general description of the issues to be arbitrated; and (ii) identify all parties who have agreed (or become obligated) to submit the dispute to binding arbitration under Sections C.6 and C.7.

C.7.1.2 Within five business days of receiving an Arbitration Notice, WECC's Chief Executive Officer shall: (a) publish (or cause to be published) in

WECC's newsletter or on its electronic bulletin board a notice containing a list of the parties to the arbitration and the parties' brief, general description of the issues to be arbitrated; and (b) deliver to each party to the dispute a copy of WECC's then-current standing list of qualified arbitrators, knowledgeable in matters addressed by WECC (as approved by the Board of Directors).

C.7.1.3 No person may be listed on WECC's standing list of qualified arbitrators unless the person has agreed to: (a) disclose, at any time the person is selected to serve as a arbitrator under this Appendix C, any personal or financial interest the arbitrator may have with respect to the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the arbitrator's immediate family members); (b) disclose any relationship the arbitrator may have with any party to the dispute that is not permitted under Section C.7.2 below; (c) assemble a complete record of the arbitration process and the materials received as evidence by the arbitrator if any of the parties to the dispute elect to appeal or contest the arbitrator's decision; and (d) abide by all applicable provisions of and procedures specified by Sections C.6 and C.7.

C.7.2 Selection of an Arbitrator. Within 10 calendar days after all of the parties to a dispute have agreed (or become obligated) to submit the dispute to binding arbitration under Sections C.6 and C.7, the parties to the dispute shall select an arbitrator by mutual agreement. If the parties cannot agree on an arbitrator within

10 calendar days after agreeing to arbitrate their dispute, the arbitrator shall be selected from WECC's standing list of qualified arbitrators as follows: The parties to the dispute shall take turns striking names from WECC's standing list of qualified arbitrators until there is only one name remaining. (The parties to the dispute shall draw lots to determine the order in which they take turns striking names.) The last person whose name remains on the list shall serve as the arbitrator. No arbitrator other than an arbitrator chosen by agreement of all the parties to the dispute may (i) have a personal or financial interest in the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the arbitrator's immediate family members); or (ii) be (or have an immediate family member who is) a past or present director, commissioner, officer, employee, consultant, agent, or other representative of any of the parties to the dispute. If the arbitrator selected through the process of striking names specified above is disqualified under the preceding sentence, the arbitrator whose name was stricken last shall serve in his or her place.

C.7.3 Initial Statements and Proposed Arbitration Decisions. Within 10 calendar days after the selection of an arbitrator under Section C.7.2 above, each party to the dispute shall submit a statement in writing to all other parties to the dispute and to the arbitrator. Each disputing party's statement shall set forth in reasonable detail the nature of the dispute, the issues to be arbitrated, and the party's reasonable, good faith proposal for resolving the dispute. As provided in Section C.5.3 above, to the extent permitted by law, no party to an arbitration conducted under

Sections C.6 and C.7 shall publicly disclose, rely on, or introduce as evidence in any arbitration, FERC proceeding, Canadian Regulatory Authority proceeding, proceeding before a Mexican Regulatory Authority, appeal, or litigation concerning the same or any related dispute any information required to be kept confidential by the terms of Section C.5.3.

C.7.4 Procedural Matters. The arbitrator shall determine discovery procedures, how evidence shall be taken, what written submittals may be made, and other such procedural matters, taking into account the complexity of the issues involved, the extent to which factual matters are disputed and the extent to which the credibility of witnesses is relevant to a resolution. Each party to the dispute shall produce all evidence determined by the arbitrator to be relevant and material to the issues presented. If such evidence involves proprietary or confidential information, the party submitting the evidence shall petition the arbitrator for a protective order, and to the extent the arbitrator determines there is good cause the arbitrator shall issue an appropriate protective order and all parties to the dispute shall comply with the protective order. The arbitrator may elect to resolve the arbitration matter solely on the basis of written evidence and arguments.

C.7.5 Out-of-Court Sworn Testimony. At the request of any disputing party, the arbitrator shall have the discretion to allow that party to examine witnesses through sworn out-of-court testimony (referred to in the United States as "deposition" and in Canada as "discovery") to the extent the arbitrator deems the evidence sought to be relevant and appropriate. In general, out-of-court witness examinations shall be limited to a maximum of three per party and shall be held

within 30 calendar days after the making of a request. Each witness examination shall be limited to a maximum of three hours' duration. The arbitrator shall have the discretion to permit the number and duration of examination sessions allowed under this Section C.7.5 to be increased, and to extend the 30-day time limit, upon request for good cause shown. All objections are reserved for the arbitration hearing except for objections based on privilege and proprietary or confidential information.

C.7.6 Intervention by Other Parties. Unless all of the parties to the dispute agree otherwise, no one (whether a Member, WECC, or any other entity or person) that is not a party to a dispute at the initiation of arbitration under Sections C.6 and C.7 shall have the right to intervene in the arbitration. Any party wishing to intervene in an arbitration under Sections C.6 and C.7 may petition the arbitrator for permission to intervene, provided that the petition is submitted to the arbitrator not more than 30 calendar days after notice of the arbitration is posted by WECC's Chief Executive Officer in accordance with Section C.7.1. The arbitrator shall have the discretion to permit a party to intervene if the arbitrator determines that the party petitioning to intervene has a direct and substantial interest in the outcome of the arbitration. In exercising his or her discretion concerning a requested intervention, the arbitrator shall also consider any additional complexity or delay that may be caused by allowing the intervention and also any other remedies available to the party requesting intervention. Any party that is granted the privilege of intervening in an arbitration under Sections C.6 and C.7 shall be permitted to intervene subject to the same terms, conditions,

limitations, rights, and obligations of all other parties to the dispute, including without limitation the binding effect of arbitrator's decision, limitations on rights of appeal, the obligation to share equally in the costs of the arbitrator, and the obligation to be subject to the provisions of Section C.8.

C.7.7 Consideration of WECC Criteria, Etc. The Arbitrator shall give due consideration to the reliability criteria, standards, guidelines, policies, and procedures of WECC and the North American Electric Reliability Council (or any successor organization) to the extent they are relevant to resolution of the matter(s) in dispute. If the arbitrator's decision will include interpretation of any of WECC's reliability criteria, standards, guidelines, policies, and procedures, (and WECC is not a party to the arbitration), the arbitrator shall, before rendering his or her decision, consult with WECC (subject to the provisions of Section C.7.10 below) concerning the interpretation of WECC's applicable reliability criteria, standards, guidelines, policies, and procedures.

C.7.8 Evidence and Rebuttal. The arbitrator shall consider all issues material to the matter(s) in dispute. The arbitrator shall take evidence submitted by the parties to the dispute in accordance with procedures established by the arbitrator and may request additional information the arbitrator deems material to the resolution of the dispute. With the consent of all parties to the dispute, the arbitrator's request for additional information may include the opinion of any individual or organization with recognized expertise in the matter(s) in dispute, subject to the following conditions: (i) any verbal communication with an expert consulted by the arbitrator must take place exclusively in the presence of all parties to the

dispute and copies of any written communications must be provided to all parties to the dispute; (ii) any expert consulted by the arbitrator must agree to be equally available upon request to all of the parties to the dispute; (iii) any expert consulted by the arbitrator must agree to comply with the restrictions on disclosure contained in Section C.5.3; and (iv) all parties to the dispute shall be afforded a reasonable opportunity to question the expert and to rebut any additional information submitted by the expert at the request of the arbitrator.

C.7.9 Arbitrator's Decision. The arbitrator shall make all reasonable efforts to complete hearings (if applicable) and submissions of written evidence not more than 90 calendar days after receiving initial statements submitted under Section C.7.3 above. As soon as practicable, but in no event more than 30 calendar days after the completion of hearings and evidence submittals, the arbitrator shall render his or her final decision for resolving the dispute. By agreement of all of the parties to the dispute or at the discretion of the arbitrator for good cause, the foregoing deadline for delivery of the arbitrator's decision may be extended. The arbitrator's decision shall be based on the arbitrator's good faith determination of a resolution that will: (i) be consistent with any laws, rules, and regulations applicable to the matter(s) in dispute; (ii) be consistent with any valid pre-existing agreements among the parties to the dispute that bear on the matter(s) in dispute; (iii) not require any party to the dispute to take action that is not in compliance with any of WECC's reliability criteria, standards, guidelines, policies, and procedures; and (iv) best serve to promote or maintain reliable operation of the interconnected Bulk Electric System of the Western Interconnection, without

imposing inequitable burdens or benefits on any of the parties to the dispute or others that may be affected by implementation of the arbitrator's decision. The arbitrator shall deliver to each of the parties to the dispute, along with his or her decision, a written statement including specific findings of fact, conclusions of law (if applicable), and an explanation of the arbitrator's basis for rendering his or her decision. Subject to any protective order that may have been issued under Section C.7.4 above, WECC's Chief Executive Officer shall publish (or cause to be published) in WECC's newsletter or electronic bulletin board a brief summary of the arbitrator's decision. An arbitrator's decision that is not appealed shall not be deemed to be precedential in any other arbitration related to a different dispute.

C.7.10 WECC Staff Participation in Arbitration When WECC Not a Party. If, during the course of binding arbitration conducted under Sections C.6 and C.7 (in which WECC is not a party) the arbitrator or any party to the dispute wishes to solicit the views of WECC staff concerning the application, implementation, interpretation, or fulfillment of any guidelines, criteria, standards, policies, or procedures of WECC, the arbitrator may request or permit the submission of WECC staff views only with the consent of all of the parties to the dispute and only if: (i) any participation by WECC staff takes place exclusively in the presence of all parties to the dispute; (ii) participating WECC staff members agree to be equally available upon request to all parties to the dispute; and (iii) participating WECC staff members agree to comply with the restrictions on disclosure contained in Section C.5.3.

C.7.11 Compliance and Costs. Unless one or more of the parties to the dispute initiates and notifies all other parties to the dispute that it has initiated a process to contest or appeal the arbitrator's decision under Sections C.9 through C.13, upon the decision by the arbitrator, the parties to the dispute shall, within the time frame specified by the arbitrator, and, subject to Section C.6.6 above, take whatever action is required to comply with the arbitrator's decision to the extent the arbitrator's decision does not require regulatory action. To the extent the arbitrator's decision affects jurisdictional rates, terms and conditions of service, or facilities or otherwise requires local, state, federal, or provincial approval or regulatory action, or a FERC filing or a Canadian Regulatory Authority filing by a Canadian Member or a Mexican Regulatory Authority filing by a Mexican Member, the affected Member (or WECC, if WECC is the party with the obligation to seek regulatory action) shall, within the time frame specified by the arbitrator, submit the arbitrator's decision or an appropriate filing to implement the arbitrator's decision and support the appropriate authority's acceptance or approval of the arbitrator's decision or implementation filing, except in cases where any party to the dispute has given notice of its intent to contest or appeal the arbitrator's decision. All costs associated with the arbitration (not including costs associated with attorney and expert witness fees incurred by the parties to the dispute) shall be divided equally among the parties to the dispute unless: (i) all of the parties to the dispute agree to an alternate method of allocating costs; or (ii) in rendering his or her decision, the arbitrator exercises his or her discretion

under Section C.8 below to assess fees, costs, or other monetary sanctions against one or more of the parties to the dispute for good cause.

C.7.12 Entry of Judgment. At any time after an arbitrator has rendered his or her decision in an arbitration conducted under Sections C.6 and C.7 (provided that the time provided for initiating an appeal under Sections C.11.1 and C.12 below has expired and no appeal or other means of contesting the arbitrator's decision has been initiated), judgment on the decision rendered by the arbitrator may be entered by any court of competent jurisdiction (subject to the provisions of Sections C.6.3, C.6.4, and C.6.6 above). If the award is against the United States, a party to the arbitration may apply to the United States District Court for the district in which the principal office of the applicable United States department or agency is located for an order confirming the award pursuant to 5 U.S.C. § 580.

C.8 Arbitrator's Discretion to Shift Costs or Impose Sanctions for Cause. Each party to any dispute submitted to arbitration under Sections C.6 and C.7 shall bear its own costs and fees associated with representation and participation in the arbitration process, and shall share equally in the arbitrator's fees except that the arbitrator shall have the discretion, to the extent permitted by law, to require one or more of the parties to the dispute to pay part or all of the costs and fees (including without limitation attorneys' and arbitrator's fees) of one or more other parties to the dispute, or to impose monetary sanctions on some other basis that is reasonable under the circumstances, for good cause. As used in this Section C.8, "good cause" means conduct involving serious abuse of or failure to comply with the dispute resolution process set forth in this Appendix C, willfully undertaken to harass or delay other parties to the dispute or to substantially impede the

arbitrator's ability to render a decision consistent with the provisions set forth in Section C.7.9.

C.9 Rights to Appeal Arbitration Decisions. Except to the extent otherwise provided by applicable United States state or federal law, applicable Canadian or provincial law, or applicable Mexican law, a party to a dispute resolved by arbitration under Sections C.6 and C.7 may appeal or contest the arbitrator's decision only on one or more of the bases specified in Section C.9.1 below and only in accordance with the procedures set forth in Sections C.9.2 through C.13.

C.9.1 Grounds for Appealing Arbitration Decisions. A party to a dispute resolved by arbitration under Sections C.6 and C.7 may contest or appeal the arbitrator's decision only on the basis that: (i) the arbitrator's decision is contrary to applicable law or regulation (including without limitation the FPA or FERC's then-applicable standards or policies, or comparable types of provisions that may apply under applicable Canadian, provincial, Mexican, or other laws and regulations); (ii) the arbitrator's decision is demonstrably arbitrary and capricious and without support in the record assembled during the arbitration; (iii) the arbitrator failed to afford one or more parties to the dispute an opportunity for a fair and meaningful hearing; (iv) the arbitrator engaged in serious misconduct in connection with the arbitration; (v) the arbitrator exceeded the authority conferred upon him or her under this Appendix C or as otherwise established by agreement of all the parties to the dispute; or (vi) the arbitrator's decision is contrary to the provisions of Section C.6.6.

C.9.2 Matter and One or More Parties to Dispute Subject to FERC Jurisdiction. If (i) the subject matter of a dispute arbitrated under Sections C.6 and C.7 is within the jurisdiction of FERC, and (ii) the conditions specified in Section C.12.1 or C.12.2 are satisfied, the rights of the parties to contest or appeal the arbitrator's decision shall be as set forth in Sections C.10 and C.12 below (subject also to the provisions of Section C.9.1 above). Notwithstanding the foregoing, nothing herein shall be construed or operate to require any Canadian or Mexican party or any other party that is not a "public utility" within the meaning of the FPA to make any filing with FERC under Sections 205 or 206 of the FPA.

C.9.3 All Parties and Matters in Dispute Subject to Jurisdiction of a Canadian Regulatory Authority. If all of the parties to an arbitrated dispute are subject to the jurisdiction of a particular Canadian Regulatory Authority, and if all matters in dispute are also subject to the jurisdiction of the same Canadian Regulatory Authority, any disputing party may appeal an arbitrator's decision to that Canadian Regulatory Authority, where such Canadian Regulatory Authority has jurisdiction to hear the appeal, or to the appropriate Canadian court. Any appeal to a Canadian Regulatory Authority or Canadian court shall be subject to the provisions set forth in Sections C.10 and C.11 below.

C.9.4 All Parties and the Matter in Dispute Subject to Jurisdiction of a Mexican Regulatory Authority. If all of the parties to an arbitrated dispute are subject to the jurisdiction of a particular Mexican Regulatory Authority, and if all matters in dispute are also subject to the jurisdiction of the same Mexican Regulatory Authority, any disputing party may appeal an arbitrator's decision to the

appropriate Mexican Regulatory Authority, subject to the provisions set forth in Sections C.10 and C.11 below.

C.9.5 Appeal to Court. If none of the preceding provisions concerning appealing or contesting an arbitrator's decision before FERC, a Canadian Regulatory Authority, or a Mexican Regulatory Authority apply to an arbitrated dispute, any party to an arbitrator's decision rendered in accordance with the provisions of Sections C.6 and C.7 may appeal the arbitrator's decision to a court of competent jurisdiction as provided under Section C.13 below.

C.10 Appealing or Contesting Arbitrator's Decision to FERC or a Presiding Authority. Subject to the conditions specified in Sections C.9.1 through C.9.5 above, any disputing party may appeal or contest an arbitrator's decision to FERC or an appropriate Presiding Authority as follows:

C.10.1 Record on Appeal. Except as otherwise provided in Section C.10.3 below, any appeal or action to contest an arbitrator's decision to FERC or a Presiding Authority shall be based solely upon the record assembled by the arbitrator. All parties to arbitrations conducted under Sections C.6 and C.7 intend that: (i) the FERC or other Presiding Authority should afford substantial deference to the factual findings of the arbitrator; (ii) the portion, if any, of the arbitrator's decision relating to issues not of first impression (i.e., matters previously decided by the FERC or other Presiding Authority or a court of competent jurisdiction in cases involving comparable facts and circumstances) should be afforded appropriate deference by the FERC or other Presiding Authority; and (iii) the

portion, if any, of the arbitrator's decision relating to issues of first impression should be afforded no deference by the FERC or other Presiding Authority.

C.10.2 No Expansion of Record on Appeal. Except as otherwise provided in Section C.10.3 below, no Member, non-Member, or WECC that has been a party to an arbitration under Sections C.6 and C.7 shall seek to expand the factual record before FERC or a Presiding Authority beyond that assembled by the arbitrator.

C.10.3 Exceptions to Limitations on Record on Appeal. If the arbitrator fails to assemble a complete record of the evidence submitted with respect to an arbitrated decision that is appealed pursuant to Sections C.9 through C.13, the parties to the appeal shall, notwithstanding the provisions of Sections C.10.1 and C.10.2 above, have the right to supplement the arbitrator's record before FERC or the Presiding Authority with any materials received into evidence by the arbitrator but omitted from the record assembled by the arbitrator. If an arbitrator's decision is appealed under Section C.9.1(iii) or (iv) above on the grounds that the arbitrator improperly excluded evidence so as to materially prejudice the outcome of the arbitration with respect to one or more of the parties to the dispute, any party to the appeal may submit the evidence asserted to be improperly excluded, but only as a basis to request that FERC or the Presiding Authority vacate the arbitrator's decision and remand the matter to the arbitrator (or, if FERC or the Presiding Authority determines that the arbitrator engaged in serious misconduct, to a newly selected arbitrator) for reconsideration of the matter with inclusion of the improperly excluded evidence. If an arbitrator's decision is appealed under Section C.9.1(iv)

above on the grounds of serious misconduct by the arbitrator, any party to the appeal may offer new evidence relating to the arbitrator's alleged misconduct.

C.11 Procedures for Appeals to Presiding Authority. If any party to an arbitration under Sections C.6 and C.7 desires to appeal an arbitrator's decision to an appropriate Presiding Authority, it shall provide written notice to that effect to all other parties to the arbitration, the arbitrator, and WECC's Chief Executive Officer within 14 calendar days following the date of the arbitrator's decision. If notice of appeal is timely provided:

C.11.1 Within 30 calendar days after the date of the appealing party's first notice of appeal, the party providing notice of appeal shall file its statement of position regarding the appeal with the Presiding Authority, together with the complete evidentiary record of the arbitration and a copy of the arbitrator's decision. The statement of position shall state that the appeal requested has been the subject of an arbitration pursuant to this Agreement.

C.11.2 Within 30 calendar days after the date of the appealing party's first notice of appeal, any other party that was a party to the arbitration may file its statement of position regarding the appeal with the Presiding Authority.

C.11.3 Copies of all materials filed with the Presiding Authority by any party during the course of an appeal shall be delivered to all other parties to the arbitration and to WECC's Chief Executive Officer.

C.11.4 Implementation of the arbitrator's decision shall be deemed stayed pending an appeal unless and until, at the request of a disputing party, the Presiding Authority issues an order shortening or extending the stay of implementation.

C.11.5 WECC's Chief Executive Officer shall publish (or cause to be published) a summary of each appeal in WECC's newsletter or electronic bulletin board.

C.11.6 The Members and WECC intend that any Presiding Authority's order resulting from an appeal under Sections C.9 and C.11 shall be subject to judicial review pursuant to laws governing the Presiding Authority and the matter in dispute that provide for judicial review of Presiding Authority action.

C.12 Procedures for Contesting or Appealing Arbitrator's Decision Before FERC. If any party to a dispute arbitrated under Sections C.6 and C.7 elects, subject to the limitations set forth in Sections C.9.1 through C.9.5 above, to contest or appeal an arbitrator's decision before FERC, the party so electing shall provide written notice to that effect to all other parties to the arbitration, the arbitrator, and WECC's Chief Executive Officer within 14 calendar days following the date of the arbitrator's decision. The provisions contained in Sections C.10.1, C.10.2, and C.10.3 above shall apply with respect to the record of the arbitration submitted to FERC. In addition, the following provisions shall apply:

C.12.1 FERC Filing by Prevailing Party. If the arbitrator's decision requires the prevailing party to take action that must have FERC approval or involves the provision of FERC-jurisdictional service by the prevailing party, the prevailing party shall file the arbitrator's decision or make an appropriate filing with FERC to implement the arbitrator's decision. Provided that it has given notice as required under Section C.12 above, any non-prevailing party may contest the prevailing party's filing in accordance's with FERC's applicable rules and regulations.

C.12.2 Complaint to FERC by Prevailing Party. If the arbitrator's decision requires a non-prevailing party to take action that must have FERC approval or involves the provision of FERC-jurisdictional service by any non-prevailing party, then, if the non-prevailing party has given notice as required under Section C.12 above, the prevailing party may submit the arbitrator's decision to FERC in the form of a complaint.

C.13 Appeal to Court. If none of the provisions that govern appealing or contesting an arbitrator's decision before FERC, a Canadian Regulatory Authority, or a Mexican Regulatory Authority as set forth in Sections C.9.2, C.9.3, or C.9.4 above apply, any disputing party may appeal an arbitrator's decision to any court of competent jurisdiction, subject to the conditions specified in Section C.9.1 above. Except as otherwise provided in Section C.10.3 above (substituting the words "court of competent jurisdiction" for "FERC or the Presiding Authority"), any appeal to a court shall be based solely upon the record assembled by the arbitrator, and no Member, non-Member, or WECC who is a party to an arbitration under Sections C.6 and C.7 shall seek to expand the factual record before the court beyond that assembled by the arbitrator.

Appendix of Additional Definitions Relating to
Alternative Dispute Resolution Provisions

Arbitration Notice has the meaning specified in Section C.7.1 of these Bylaws.

Canadian Regulatory Authority. The agency or agencies established under the laws of Canada or the applicable Provinces of Canada and having jurisdiction over facilities, interconnections, transmission rates, charges, terms, and conditions of service of a Canadian Member.

Dispute Notice has the meaning specified in Section C.5.1 of these Bylaws.

FERC. The Federal Energy Regulatory Commission or a successor agency.

FPA. The Federal Power Act (16 U.S.C. §§ 824 *et. seq.*), as it may be amended from time to time.

Mexican Regulatory Authority. The agency or agencies established under the laws of Mexico or the applicable states of Mexico and having jurisdiction over facilities, interconnections, transmission rates, charges, terms, and conditions of service of a Mexican Member.

Presiding Authority. As used in Sections C.10 and C.11, the term "Presiding Authority" has the following meanings: with respect to an appeal to an appropriate Canadian Regulatory Authority, "Presiding Authority" means the presiding Canadian Regulatory Authority or Canadian court with jurisdiction to hear the appeal; and with respect to an appeal to an appropriate Mexican Regulatory Authority, "Presiding Authority" means the presiding Mexican Regulatory Authority or Mexican court with jurisdiction to hear the appeal.

Attachment 4

Bylaws -

Amended Exhibit of the Delegation Agreement Between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council - B

Redline Version

BYLAWS

OF

THE

WESTERN ELECTRICITY COORDINATING COUNCIL

TABLE OF CONTENTS

1. Vision and Mission. 1

1.1 Vision. 1

1.2 Mission 1

2. Furtherance of WECC's Mission 1

2.1 Activities to Carry Out WECC's Mission. 1

2.2 Organizational Characteristics. 3

3. Definitions 4

3.1 Affiliate. 4

3.2 Annual Meeting. 4

3.3 Applicable Regulatory Authority. 4

3.4 Backstop Authority. 4

3.5 Balancing Authority. 5

3.6 Ballot Body. 5

~~3.7 Ballot Pool.~~ ..... ~~5~~

3.~~8~~7 Board of Directors (Board). 5

3.~~9~~8 Class 5

3.~~10~~9 Commercial Practices. 5

3.1~~1~~0 Compliance Hearing Body. 5

3.1~~2~~1 Delegation Agreement. 5

3.1~~3~~2 Director. ..... 6~~5~~

3.1~~4~~3 Electric Line of Business. 6

3.1~~5~~4 Electric Reliability Organization (ERO). 6

3.1~~6~~5 Entity. 6

3.1~~7~~6 FERC. 6

3.1~~8~~7 Grid Operating Entity. 6

3.1~~9~~8 International Reliability Agreement. 6

3.~~20~~19 Local Regional Entity. 6

3.~~21~~20 Market Interface. 6

3.212 Material External Impacts (MEI). 76
3.223 Member. 76
3.234 Participating Stakeholder. 7
3.245 Primary Authority. 7
3.256 Regional Criteria. 7
3.267 Regional Entity (RE). 7
3.278 Registered Entity. 7
3.289 Reliability Management System. 7
3.2930 Reliability Standard. 7
3.301 Reliability Standards Development Procedures. 87
3.312 Transmission Facilities. 87
3.323 Western Interconnection. 8
4. Members and Membership. 8
4.1 Voluntary Membership. 8
4.2 Eligibility for Membership. 8
4.3 Designation of Membership Class. 9
4.4 Changes in Membership Class. 9
4.5 Affiliates and Distinct Business Entities. 9
4.6 Rights and Obligations of Membership. 10
4.7 Limitations on Member Obligations. 11
4.8 Compliance and Enforcement. 12
4.9 WECC Structure and Governance Review. 132
5. Procedures for Member Decisions. 13
5.1 Quorum and Alternative Voting. 13
5.2 General Membership Meetings. 143
5.3 Annual Member Meetings. 14
5.4 Special Member Meetings. 14
5.5 Member Class and Subclass Meetings 14
5.6 Notice of Member Meetings. 14
5.7 Open Meetings. 15

5.8 Policymaking Authority. 15
5.9 Minimum Participation Requirement. 15
6. Governance. 15
6.1 Board of Directors. 16
6.2 Composition of the Board and Board Member Qualifications. 165
6.3 Term of Office. 18
6.4 Nomination, Selection and Compensation of Directors. 198
6.5 Removal of Directors 210
6.6 Resignation. 21
6.7 Procedures for Filling Vacant Director Positions. 21
6.8 Duties of Directors 22
6.9 Powers of Directors. 22
6.10 Delegation of Board Authority. 23
7. Procedures for Board Decisions 23
7.1 Quorum. 23
7.2 Majority Vote. 24
7.3 Attendance at Board Meetings by Teleconference. 243
7.4 Board Action by Unanimous Consent. 243
7.5 Notice of Board Meetings 25
7.6 Open Meetings. 25
7.7 Board Committees. 26
8. Member Committees 27
8.1 Purpose. 276
8.2 Standing Committees 276
8.3 Other Committees. 28
8.4 [Repealed] 28
~~8.4 Assessment of Standing Committee Activities. ..... 28~~
8.5 Procedures for Committee Decision-Making. 29
8.6 Procedures for Committees other than the Member Advisory Committee. 343
8.7 Procedures for Developing and Voting on Reliability Standards 386
8.8 Notice of Committee Meetings 4037

8.9 Open Meetings. 4037
9. The Chief Executive Officer, Officers, and Employees. 4137
9.1 Designation of Officers and Terms of Office. 4137
9.2 Chief Executive Officer Qualifications. 4138
9.3 Standards Applicable to All Employees. 4138
9.4 Employment. 4238
9.5 Chief Executive Officer's Duties. 4238
9.6 Secretary's Duties. 4239
10. Dispute Resolution. 4239
11. Costs and Finances. 4339
11.1 Funding of Reliability Activities. 4339
11.2 Dues. 4340
11.3 Funding of Non-Statutory Activities. 4441
12. Amendments to these Bylaws. 4441
12.1 Amendment by the Board. 4441
12.2 Amendment by the Members. 4541
12.3 Amendments in Response to Mandatory Membership. 4542
12.4 Amendments proposed by FERC. 4542
13. Termination of Organization. 4542
14. Miscellaneous Provisions. 4542
14.1 Limitation on Liability. 4542
14.2 Indemnification. 4642
14.3 No Third Party Beneficiaries. 4643
14.4 Informal Inquiries for Information. 4643
15. Incorporation. 4643
16. Governing Law. 4643
17. WECC Transition. 4743
17.1 Board of Directors transition. 4744
17.2 Transition Exceptions 4744
17.3 Member Advisory Committee transition 4844

APPENDICES:

A. Board Member Standards of Conduct

B. Officers and Employees Standards of Conduct

C. WECC Dispute Resolution Procedures

BYLAWS

Of

The

WESTERN ELECTRICITY COORDINATING COUNCIL

1. Vision and Mission.

1.1 Vision.

The Western Electricity Coordinating Council ("WECC") shall seek to achieve the appropriate level of Bulk Electric System reliability at least cost considering all costs throughout the economy.

1.2 Mission

WECC is a Utah nonprofit corporation with the mission to foster and promote reliability and efficient coordination in the Western Interconnection. WECC will lead the stakeholders in the Western Interconnection to achieve appropriate system reliability, be the premier source of unbiased information, and serve as the trusted thought leader for the Western Interconnection by providing, consistent with these Bylaws: 1) impartial independent review and analysis of reliability issues impacting the Western Interconnection 2) development of electric reliability standards incorporating Western Interconnection experience and knowledge; 3) consistent and fair monitoring and enforcement activities for compliance with reliability standards; 4) event analysis and lessons-learned from system events; and 5) value for its membership through cost effective and efficient services and practices through: a) being a centralized repository of reliable information relating to the planning and operation of the Bulk Electric System in the Western Interconnection, b) coordinating system planning and modeling, c) sharing of, and providing comment on adherence to, recognized industry best practices, d) facilitating resolution of market seams and coordination issues, e) secure sharing of critical reliability data, and f) providing a robust stakeholder forum.

2. Furtherance of WECC's Mission

2.1 Activities to Carry Out WECC's Mission.

2.1.1 Compliance with the Federal Power Act. WECC will carry out responsibilities and exercise rights of a Regional Entity organized on an interconnection-wide basis pursuant to Section 215 of the Federal Power Act, including any responsibilities and rights delegated to it by the ERO pursuant to a Delegation Agreement.

2.1.2 Agreements with Canada and Mexico. WECC will carry out responsibilities and exercise rights pursuant to International Reliability Agreements with Canadian or Mexican authorities.

2.1.3 Regional Coordination. WECC will act as a coordinating entity for the entire Western Interconnection for activities of regional organizations with responsibilities for reliability and market functions.

2.1.4 Standard Setting. WECC will develop and adopt reliability, operating, and planning standards, criteria and guidelines necessary to maintain the reliable operation of the Western Interconnection's interconnected Bulk Electric System, including seeking, as appropriate, variances from standards of the ERO (or any successor organization which may be created by legislation or otherwise), as well as providing a process for regional variances.

2.1.5 Certification of Grid Operating Entities. WECC will assist in certifying Grid Operating Entities in the Western Interconnection.

2.1.6 Reliability Assessment. WECC will ensure that interconnected Bulk Electric System reliability assessments are conducted as needed. WECC will do this work in conjunction with the Regional Entities to the greatest extent possible. WECC will also facilitate coordinated reliability assessments among Regional Entities.

2.1.7 Compliance Activities. With respect to enforcement of reliability standards, WECC will:

2.1.7.1 implement the Reliability Management System in effect as of WECC's formation and as the Reliability Management System may be subsequently modified in accordance with its terms;

2.1.7.2 implement any monitoring and enforcement mechanisms delegated to it pursuant to Section 215 of the Federal Power Act and any Delegation Agreement with the ERO, or required by any International Reliability Agreement with a Canadian or Mexican authority; and

2.1.7.3 administer any other monitoring and enforcement mechanisms where WECC is designated to perform administration.

2.1.8 Coordinated Regional Planning. With respect to the coordination of regional planning activities, WECC:

2.1.8.1 will develop coordinated planning policies and procedures for the Western Interconnection, including facilitation of market-based solutions, consistent with WECC/ERO standards and FERC policy.

2.1.8.2 will review and assess Local Regional Entity planning processes to determine whether WECC planning procedures have been satisfied;

2.1.8.3 will refer planning matters back to the originating Local Regional Entity for revision or other corrective actions when the WECC Board determines that WECC planning procedures have not been satisfied; and

2.1.8.4 may perform other interconnection-wide studies as needed.

2.1.9 Coordinated Operations. With respect to coordinating reliable operating activities within the Western Interconnection, WECC will develop, coordinate and promote consistent interregional operating policies and procedures for the Western Interconnection, consistent with WECC/ERO standards and FERC policy.

2.1.10 Market Interface Issues. With respect to Market Interface issues WECC will:

2.1.10.1 facilitate development of compatible and efficient practices across the Western Interconnection; and

2.1.10.2 exercise Backstop Authority where an unresolved Market Interface issue will cause Material External Impacts by taking some or all of the following actions: 1) providing a forum for and coordinating voluntary solutions among Members; 2) recommending specific solutions for voluntary adoption by Members; and 3) if necessary, proposing solutions to an Applicable Regulatory Authority.

2.1.11 Dispute Resolution. WECC will provide a process for the timely resolution of disputes between WECC Members as set forth in Section 11.

2.2 Organizational Characteristics.

As WECC carries out activities to fulfill its mission, it will seek to develop and maintain the following characteristics:

2.2.1 dedication to serving the individuals, businesses, and other organizations that generate, transmit, distribute, market, and use electrical energy in the Western Interconnection;

2.2.2 efficiency in its administration, decision-making, policy and standards development, and dispute resolution processes;

2.2.3 the ability to maintain status as an Interconnection-wide regional reliability entity and be afforded deference and delegation by ERO (or successor organization); and

2.2.4 fair and open processes through which practices, policies, and standards are developed and implemented based on sound technical and policy analysis.

2.2.5 Promote an efficient western electric market by reducing or eliminating conflict, duplication and overlap among electric organizations in the Western Interconnection.

2.2.6 Allow access to WECC data by individuals who can demonstrate a legitimate business need for the data, provided such individuals agree to such protections and non-disclosure restrictions which may be necessary due to the nature of the data sought to be accessed and agree to pay the incremental costs of providing the data which may be requested.

3. Definitions.

The capitalized terms used in these Bylaws shall have the meanings set forth below, or if not set forth below, shall have the meanings given them in the NERC Glossary of Terms Used in NERC Reliability Standards.

3.1 Affiliate.

An Entity that directly or indirectly through one (1) or more intermediaries, controls, or is controlled by, or is under common control with, another Entity. An Entity "controls" any Entity in which it has the power to vote, directly or indirectly, 5% or more of the voting interests in such entity or, in the case of a partnership, if it is a general partner. Notwithstanding the foregoing definition, for purposes of these Bylaws: 1) electric distribution cooperatives that are member-owners of a generation and transmission cooperative are not Affiliates of the generation and transmission cooperative or of each other; 2) an entity controlled by or operating as a unit, agency, or subdivision of a local, state, provincial, or U.S. federal or Canadian or Mexican national government will not be considered an Affiliate of any other entity controlled by or operating as a unit, agency, or subdivision of a local, state, provincial, or federal government; 3) separate agencies of a single state or province, or of the U.S. federal or Canadian or Mexican national government will not be considered Affiliates of each other, regardless of any commonality of political control; 4) members of any joint powers authority, and such joint powers authority, will not be considered Affiliates of each other; and 5) members of an RTO will not be considered Affiliates of such RTO or of each other solely as a result of such membership.

3.2 Annual Meeting.

The annual membership meeting of WECC, as described in Section 5.3.

3.3 Applicable Regulatory Authority.

The FERC or any state or provincial government agency with jurisdiction to regulate or directly affect the transmission of electricity within the Western Interconnection.

3.4 Backstop Authority.

The ability, obligation, or responsibility of WECC to address an issue when the WECC Board determines that a Local Regional Entity(ies) holding Primary Authority has not resolved an issue, has created incompatible resolutions or has not acted. In each case where these Bylaws authorize WECC to exercise Backstop Authority, the provisions that authorize Backstop Authority will also specify the conditions necessary to trigger Backstop Authority and the actions that fall within WECC's exercise of Backstop Authority.

3.5 Balancing Authority.
The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

3.6 Ballot Body.
The Ballot Body consists of WECC members and non-members that have been determined eligible for the voting sectors described in ~~8.6.5.2~~the Reliability Standards Development Procedures and may, therefore, vote on Regional Criteria and Regional Reliability Standards.

~~**Ballot Pool.**~~
~~A Ballot Pool consists of a self-selected set of members of the Ballot Body who join the Ballot Pool for a given Regional Criterion or Regional Reliability Standard during a designated window of opportunity provided by WECC either prior to balloting or prior to the close of balloting.~~

3.7 Board of Directors (Board).
WECC Board of Directors, collectively, as described in Section 6.

3.8 Class.
A grouping of Members described in Sections 4.2.1 through 4.2.7 and 4.3.

3.9 Commercial Practices.
The products and practices involved in trading electricity. The term "Commercial Practices" only refers to an interaction among market entities that does not affect or require assistance from Grid Operating Entities that have grid reliability responsibilities.

3.10 Compliance Hearing Body.
The hearing body used for the purpose of providing a balanced compliance panel to conduct hearings for the resolution of disputes concerning compliance with or enforcement of Reliability Standards that may arise between WECC (acting as Compliance Enforcement Authority for the Western Interconnection) and a Registered Entity.

3.11 Delegation Agreement.
An agreement between the ERO and WECC pursuant to Section 215 of the Federal Power Act by which the ERO delegates to WECC designated powers, rights and

responsibilities regarding the administration within the Western Interconnection of electric Reliability Standards adopted or approved by the ERO and the FERC.

3.12 Director.
An individual member of the WECC's Board of Directors.

3.13 Electric Line of Business.
The generation, transmission, distribution, or trading of electricity or the provision of related energy services in the Western Interconnection.

3.14 Electric Reliability Organization (ERO).
The organization certified by FERC under 18 C.F.R. §39.3, the purpose of which is to establish and enforce Reliability Standards for the Bulk-Electric System in the United States, subject to FERC review.

3.15 Entity.
Any individual, person, corporation, partnership, association, governmental body or organization of any kind.

3.16 FERC.
The Federal Energy Regulatory Commission or any successor.

3.17 Grid Operating Entity.
Any operating entity, such as a Balancing Authority, that is certified pursuant to Section 2.1.5 of these Bylaws to be responsible for reliable operation of a portion of the Western Interconnection.

3.18 International Reliability Agreement.
An agreement between WECC and any appropriate Canadian or Mexican authority related to WECC's powers, rights and responsibilities regarding the administration of electric reliability standards applicable within such authority's geographic area of the Western Interconnection.

3.19 Local Regional Entity.
A regional transmission organization or some other formally or informally constituted regional organization or group within the Western Interconnection, including but not limited to a Balancing Authority, a group of Balancing Authorities acting in concert, or a group of Entities that own or operate Transmission Facilities acting in concert. These Local Regional Entity boundaries can be reevaluated or modified over time.

3.20 Market Interface.
Market Interface involves all interactions among market entities and Grid Operating Entities related to transmission service and physical delivery.

3.21 Material External Impacts (MEI).
Significant effects on another Local Regional Entity or market within the Western Interconnection but outside of the Local Regional Entity or market adopting a policy, standard, practice or procedure, or implementing an action.

3.22 Member.
Any entity that has applied and been accepted for membership in WECC and is current in the payment of dues.

3.23 Participating Stakeholder.
Any person or entity that is not a WECC Member, but is an interested stakeholder and has applied and been granted, pursuant to Section 8.7.2, the participation and voting rights set forth in Section 8.7.1.

3.24 Primary Authority.
The ability, obligation, or responsibility of an entity to address an issue in the first instance.

3.25 Regional Criteria
~~A WECC Board Approved document created to establish requirements to address NERC "fill-in-the-blank" reliability standards necessary to implement, to augment, or to comply with NERC or Regional Reliability Standards and any other documents that may precipitate attendant monitoring and compliance through the Compliance Monitoring and Enforcement Program in the United States, or by programs established by the Applicable Governmental Authority in Canada and Mexico, as applicable. New and revised Regional Criteria shall be established using the WECC Standards Development Procedures.~~ The term Regional Criteria shall have the definition set forth in the NERC Rules of Procedure as may be amended from time to time.

3.26 Regional Entity (RE).
An entity having enforcement authority pursuant to 18 C.F.R. §39.8.

3.27 Registered Entity.
An owner, operator, or user of the Bulk-Electric System or the entities registered as their delegates for the purpose of compliance in the North American Electric Reliability Corporation Compliance Registry or similar Entity operating in Canada or Mexico and which could be registered in the Compliance Registry if it operated in the United States.

3.28 Reliability Management System
The contracts, separate from these Bylaws, by which Members and other parties agree to certain procedures and sanctions intended to enforce specified Reliability Practices to maintain reliable electric service throughout the Western Interconnection.

3.29 Reliability Standard.
A requirement approved by FERC under section 215 of the Federal Power Act, to provide for reliable operation of the Bulk-Electric System in the United States. Regional

Reliability Standards are specific to the Western Interconnection and shall be established using the WECC Standards Development Procedures.

3.30 Reliability Standards Development Procedures.
The process for developing and approving WECC Regional Reliability Standards (or its successor) attached as Exhibit C to the Delegation Agreement between WECC and North American Electric Reliability Corporation.

3.31 Transmission Facilities.
Those facilities that are defined as "transmission facilities" by FERC for purposes of the open access requirements of Section 210 and 211 of the Federal Power Act or any facilities which would be so defined if the Member were subject to FERC jurisdiction.

3.32 Western Interconnection.
The geographic area containing the synchronously operated electric transmission grid in the western part of North America, which includes in the United States Arizona, California, Idaho, Nevada, Oregon, Utah, and Washington, as well as parts of Montana, Nebraska, New Mexico, South Dakota, Texas, Wyoming, and Colorado; parts of the Canadian Provinces of British Columbia and Alberta; and Baja California Norte, Mexico.

4. Members and Membership.

4.1 Voluntary Membership.
Except as otherwise may be required by applicable authority, membership in WECC is voluntary. A Member may withdraw upon giving the Secretary thirty (30) days' advance written notice. Notwithstanding such notice of withdrawal, all contracts, FERC orders, unpaid Member costs, and decisions of arbitration in effect or pending as of the date of the written notice of withdrawal will be followed through to completion, pursuant to these Bylaws, by the withdrawing Member; however. Nothing herein will relieve any Member withdrawing from WECC from any obligation it may have under applicable law including, but not limited to, Section 215 of the Federal Power Act. A Member that withdraws is obligated to pay any unpaid dues owed through the remainder of the fiscal year in which its withdrawal becomes effective.

4.2 Eligibility for Membership.
Subject to Section 4.5, any Entity that is an interested stakeholder or that meets the criteria for membership in the membership classes described in Sections 4.2.1 through 4.2.5 may be a Member of WECC:

4.2.1 Class 1. Electric Line of Business Entities owning, controlling or operating more than 1000 circuit miles of transmission lines of 115 kV and higher voltages within the Western Interconnection.

4.2.2 Class 2. Electric Line of Business Entities owning, controlling or operating transmission or distribution lines, but not more than 1,000 circuit miles of transmission lines of 115 kV or greater, within the Western Interconnection.

4.2.3 Class 3. Electric Line of Business Entities doing business in the Western Interconnection that do not own, control or operate transmission or distribution lines in the Western Interconnection, including power marketers, independent power producers, load serving entities, any other Entities whose primary business is the provision of energy services, and those Entities that are not eligible for membership in the other Member Classes and who have a substantial interest in the purposes of WECC.

4.2.4 Class 4. End users of significant amounts of electricity in the Western Interconnection, including industrial, agricultural, commercial and retail entities as well as organizations in the Western Interconnection that represent the interests of a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public or the environment.

4.2.5 Class 5. Representatives of states and provinces in the Western Interconnection, provided that such representatives will have policy or regulatory roles and do not represent state or provincial agencies and departments whose function involves significant direct participation in the market as end users or in Electric Line of Business activities.

4.2.6 Sub-Class Organization. A Member Class may subdivide in up to three subclasses based on a majority desire within that class for purposes of electing Member Advisory Committee representation.

4.3 Designation of Membership Class.

A Member of WECC may not belong to more than one Class. An applicant for membership will designate the Class for which it qualifies based upon the criteria for membership set forth in Section 4.2, –however any Member owning, controlling or operating Transmission Facilities or distribution facilities must belong to Class 1 or 2 unless the Board grants the Member's petition for a change in Member Class pursuant to the provisions of Section 4.4 of these Bylaws. Applications for membership will be submitted to WECC. WECC staff will review the application to verify eligibility for membership and Member Class designation. An applicant whose application has been rejected or any Member who disputes the WECC staff's determination regarding the appropriate Member Class designation may request review by the Governance Committee. If the applicant or any Member disagrees with the Governance Committee's decision, the applicant or such Member may appeal this decision to the Board.

4.4 Changes in Membership Class.

Notwithstanding any other provision of these Bylaws, upon a petition from a Member, the WECC staff (subject to review by the Governance Committee and appeal to the Board) may allow the Member to change Member Class if the interest of the Member is more closely aligned with the proposed Class than the Member's current Class.

4.5 Affiliates and Distinct Business Entities.

An Affiliate of a Member that satisfies the membership qualifications may also become a Member provided:

4.5.1 The Affiliate applying for membership and the Member disclose to the Chief Executive Officer all Affiliates that are WECC Members and the Classes to which the Affiliates belong. Every Member will promptly notify the Chief Executive Officer whenever it becomes, or ceases to be, an Affiliate of any other Member.

4.5.2 Affiliates may be members of the same Class; provided, however, a group of Affiliates within a single Class may only have one vote in any WECC forum. Except as set forth in Section 8.7.6, ~~A~~a group of Affiliates within a single Class may, by providing~~,~~ at least three (3) business days~~,~~ advance written notice to the Chief Executive Officer, split their single vote equally amongst all Affiliates or designate a single Affiliate as the group's voting Member.

4.5.3 For good cause shown and with the express approval of the Board, a company or organization containing functionally distinct entities within it may obtain separate memberships for such entities; provided that such entities will be considered Affiliates.

4.5.4 The Board may adopt a policy regarding whether Members may share the benefits of membership (including the right to receive information that is only available to Members) with a non-member Affiliate.

~~Upon receiving applications from non-WECC members to join the Ballot Body, WECC staff shall require such non-WECC members to identify their affiliations with other Ballot Body members in their applications to join the Ballot Body. WECC staff shall limit voting of affiliated non-WECC members in the same manner that would be used to limit voting by WECC member organizations.~~

4.6 Rights and Obligations of Membership.

Except as otherwise provided in these Bylaws or other applicable authority, Members of WECC have the following general rights and obligations:

4.6.1 The right to elect and remove Directors as described in Section 6.5;

4.6.2 The right to amend these Bylaws, and to review and rescind any Board amendment of these Bylaws, in accordance with Section 12;

4.6.3 The right to receive appropriate meeting notices, as well as reports and information produced by WECC;

4.6.4 The right to attend, participate and vote in all WECC Member meetings and the right to attend Board meetings (other than closed sessions of Board meetings) and to comment upon all matters considered in such meetings;

4.6.5 The right to be a member of, attend meetings of, and to introduce motions, debate and to vote in the deliberations of WECC committees, subject to the limitations of these Bylaws and such other reasonable limitations as the Board may adopt from time to time;

4.6.6 The right to invoke the dispute resolution provisions of these Bylaws;

4.6.7 The right to petition the Board to take any action consistent with applicable law (including Section 215 of the Federal Power Act and implementing orders and regulations), these Bylaws and the articles of incorporation and to have such petition voted upon in a reasonable and timely manner;

4.6.8 The obligation to abide by these Bylaws, decisions resulting from the dispute resolution process, and all standards or decisions of WECC, subject to the exceptions set forth in Section 4.7 and the enforcement provisions of Section 4.8.

4.6.9 The obligation to notify the Chief Executive Officer promptly of changes with respect to Affiliates as provided in Section 4.5.1 of these Bylaws; and

4.6.10 The obligation to pay in a timely manner the membership dues pursuant to Section 11.

4.6.11 The obligation to provide system data that the Board has determined is necessary for WECC functions and does not impose an undue burden on the Members; provided, however, that the Board shall adopt appropriate limitations on this obligation or procedures that protect and avoid unnecessary collection of confidential, privileged, trade secret, cybersecurity or critical energy infrastructure information or other information that the Board determines merits such protection consistent with applicable law.

4.6.12 The obligation to support surfacing minority and majority opinions or views within their Member Class, along with supporting rationale to enable the Board of Directors to make decisions based on informed judgment aligned with WECC's vision, mission and these Bylaws.

4.7 Limitations on Member Obligations.

4.7.1 The obligation of Members pursuant to Section 4.6.8 will not require any Member to take any action which the Member in good faith determines: 1) would exceed the physical capabilities of the Member's electric system (or any part of another's electric system that the Member has the legal right to cause to comply with a WECC action governed by Section 4.6.8); 2) would create serious and immediate risks to public health or safety (provided, however, that the shedding of load shall not in and of itself be deemed a serious and immediate risk to public health and safety for the purpose of this section); 3) would create an immediate risk of serious damage to facilities or equipment within its electric system or cause it to

operate any of its electric facilities or equipment in an unsafe manner; 4) would cause the Member to violate or improperly implement an applicable law, regulation, rule, order, FERC license provision or other legal obligation; or 5) would conflict with any non-power requirement applicable to the Member (including without limitation any obligation under environmental laws, regulations, court and administrative decisions or biological opinions).

4.7.2 Each Member shall retain sole control of its facilities and the use thereof, and a Member shall not be required to construct or dedicate facilities for the benefit of any other Member, or be required to take action, or refrain from action, as may be deemed necessary to maintain reliable service to its own customers and/or to fulfill its obligations to third parties; provided, that a Member shall comply with duly-adopted reliability standards applicable to its system and shall comply with any directives under existing security coordination agreements. Nothing in these Bylaws is intended to preclude application of Section 210 or 211 of the Federal Power Act. The above limitations shall not be construed as altering a Member's obligation to comply with applicable Reliability Standards or enforcement orders, or any other obligation arising under 18 C.F.R. Part 39.

4.8 Compliance and Enforcement.

The power of WECC to enforce Member obligations other than compliance with Reliability Standards and other obligations arising under 18 C.F.R. Part 39 and applicable Canadian and Mexican regulatory requirements is limited to suspension or termination of membership as set forth in this Section; provided, however, that: 1) nothing in this Section will limit the power of Members to agree to additional enforcement provisions in separate contracts (such as contracts pursuant to the Reliability Management System); 2) nothing in this Section will limit the power of WECC to propose solutions regarding Market Interface issues to any Applicable Regulatory Authority as described in Section 2.1.10; and 3) nothing in this Section will limit WECC's delegated authority under Section 215 of the Federal Power Act and 18 C.F.R. Part 39 and applicable Canadian and Mexican regulatory requirements to enforce reliability standards and perform other delegated or contractual functions within the Western Interconnection. The Board may suspend or, to the extent consistent with applicable law, terminate the membership of any Member for a material failure to meet any obligation of membership set forth in these Bylaws, including, but not limited to: 1) non-payment of dues sixty (60) days after the dues become delinquent; 2) intentionally or repeatedly violating any WECC Bylaw; 3) materially breaching or intentionally violating any FERC order or arbitration decision issued pursuant to these Bylaws; 4) willfully obstructing any lawful purpose or activity of WECC; or 5) remaining inactive as described in Section 5.9. The Board will give the affected Member not less than twenty-one (21) days prior written notice of any proposed suspension or termination, which will include the specific basis for the proposed action and, if applicable, instructions on curing the problem. Prior to terminating a membership, the Board will consider any information provided by the Member in response to the notice described herein.

4.8.1 Suspension. The suspension of a Member will not affect the Member's rights and obligations other than that the Member will not be entitled to vote at any meeting of the Members, Classes, –subclasses, or any committee until the suspension is removed except that a suspended Member may participate in the WECC proposed Reliability Standards Development Procedure.

4.8.2 Termination. The termination of membership will have the same effect, and be subject to the same continuing obligations, as such Member's withdrawal pursuant to Section 4.1, except that it will be effective as of the issuance date of the notice provided pursuant to Section 4.8.

4.9 WECC Structure and Governance Review.

At least each five years, the Board of Directors will conduct a thorough assessment of whether WECC is fulfilling its purposes in a manner that is consistent with: 1) the provisions of Section 2.2 of these Bylaws; and 2) the then-current state and the expected future evolution of the electric power industry within the Western Interconnection. Unless determined otherwise by a majority vote of both the Board of Directors and the Members Advisory Committee (MAC), the initial review required under this Section 4.9 will commence after the completion of the first full year of operation under these Bylaws as amended in June 2013 and will be done collaboratively with the MAC and to the extent practical, will be coordinated with any similar structure and governance reviews being conducted by Peak Reliability. In particular, the Board will focus on whether the standards, obligations, processes, and decisions WECC imposes on its Members are timely, fair, effective, and reasonable in view of the commercial, legal, regulatory, and economic needs and objectives of the affected Members. The Board will evaluate WECC's Board composition, Member Class structure, committee structure and activities, and staff responsibilities as they relate to the foregoing considerations. The assessment required by this Section 4.9 will be accompanied by Board recommendations for any changes the Board determines are warranted by the assessment. The assessment and recommendations prepared by the Board in accordance with this Section 4.9 will be submitted in writing to the Members at the first annual Member meeting held after they are completed.

5. Procedures for Member Decisions.

5.1 Quorum and Alternative Voting.

With the exception of voting on Regional Reliability Standards and Regional Criteria under the oversight of the WECC Standards Committee, members may conduct business and take votes only at duly noticed Member meetings. Members may not conduct any business of the membership as a whole at any meeting unless a quorum is first established.

5.1.1 Quorum. A majority of all Members, including a majority in at least three (3) Classes, will constitute a quorum for all meetings of the membership as a whole. A majority of the members of a Class or subclass will constitute a quorum for all Member Class or subclass meetings. Members participating through a designated alternative representative or through submission of an absentee ballot will be

counted in determination of a quorum. Inactive Members, as defined in Section 5.9 of these Bylaws, will not be counted in determining a quorum at Member, Member Class or subclass meetings. A quorum, once established, will be deemed to continue for the balance of any Member, Member Class, or subclass meeting, except that no election of Directors may occur without a quorum being present. Members may designate an alternate representative or submit an absentee ballot in a form consistent with Section 5.1.2 for any Member, Member Class, or subclass meeting.

5.1.2 Alternate or Absentee Voting: In the event that a Member's designated voting representative cannot attend a meeting of the Membership or a Member Class meeting where Directors are being elected or amendments to these Bylaws are considered, a Member may designate an alternate voting Member representative, with two (2) days written notice to the Corporate Secretary, or a Member may cast an absentee ballot pursuant to the procedures established by the Corporate Secretary.

5.2 General Membership Meetings.

All business of the Members acting as a whole will be conducted at meetings called by advance notice to all WECC Members provided in accordance with Section 5.5. Unless stated otherwise in these Bylaws, decisions at all meetings of the Members, Member Classes, or subclasses will be by simple majority vote of the Members present or otherwise represented in accordance with these Bylaws, with each Member having one vote, unless other Bylaw provisions provide for the allocation of the Member's vote. The Chair of the Board will preside over all Members acting-as-a-whole meetings.

5.3 Annual Member Meetings.

WECC will hold an Annual Meeting of all Members at a time and place determined by the Board. At the Annual Meeting, and at other times as provided for in these Bylaws, in addition to such other actions the Members may take, Member Classes will elect Directors for vacant director positions.

5.4 Special Member Meetings.

Members may hold special meetings whenever called by the Board. The Board will call special Member meetings whenever a majority of the Members of any Class request a special meeting or at such other times as it deems appropriate. The Chair of the Board will preside over all special Member meetings.

5.5 Member Class and Subclass Meetings

An individual WECC Member Class or subclass may hold a meeting for any purpose relevant to the interests of Class or subclass Members. Such meeting will be initiated by request by one or more Class or subclass Member(s), and agreement by at least fifty percent (50%) of Class or subclass Members.

5.6 Notice of Member Meetings.

5.6.1 Annual Meeting. The Chief Executive Officer will provide at least thirty (30) days' advance notice to all Members and the Board of the date, place and time of the Annual Meeting of the Members and an agenda of the business to be conducted at such meeting.

5.6.2 Other Member Meetings. The Chief Executive Officer will provide notice of regularly scheduled and special meetings of the Members to the Members not less than fifteen (15) days before the meeting if delivered by first-class mail, or not less than ten (10) days before the meeting if the notice is delivered personally, by telephone, by facsimile, electronic mail or express mail. If mailed, such notice will be deemed given when deposited in the United States mail, with first-class postage thereon prepaid, addressed to a Member. Such notice will state the date, time and place of the meeting and the meeting agenda.

5.6.3 Public and Website Notice. Public notice of each meeting of the Members will be placed on WECC's website at least ten (10) days before such meeting. In addition, the Chief Executive Officer will provide notice in the same manner and time as set forth in Section 5.6.2 of each meeting to each member of the public who so requests and who has provided appropriate information regarding delivery of notice.

5.7 Open Meetings.

All Membership meetings are open to observation by the public.

5.8 Policymaking Authority.

The Board of Directors may adopt policies for the interpretation and implementation of the meeting and voting procedures established in this Section 5.

5.9 Minimum Participation Requirement.

In order to be counted for quorum purposes at a meeting of the membership as a whole, Class, or subclass meeting, a WECC Member must actively participate (by attending in person, sending an alternate, or voting absentee) in at least one WECC meeting (including meetings of the Board, committees and subcommittees) each year. If the Member does not meet this minimum participation requirement, the Member will be considered an "inactive" Member until its active status is restored by participation in at least one WECC meeting (including meetings of the Board, committees and subcommittees) by attending in person, sending an alternate, or voting absentee. An inactive Member will not be counted toward establishing a quorum of the membership as a whole, of a Class, or of a subclass. An applicant for WECC membership or a WECC Member may at any time self-designate itself an inactive Member. Such designation will be effective until the Member is reinstated to "active" status. If a Member does not participate for twenty four (24) consecutive months, the Member's membership will be terminated. If a Member's membership is so terminated, reapplication for membership may be made at any subsequent time.

6. Governance.

6.1 Board of Directors.

Subject to those matters expressly requiring approval of the Membership, a Board of Directors elected by the Members will govern WECC. The Board of Directors will elect its own Chair and Vice-Chair from those individuals serving as Directors.

6.2 Composition of the Board and Board Member Qualifications.

6.2.1 The Board of Directors shall consist of nine (9) Directors. At all times, subject to temporary vacancies, the Board of Directors shall include at least three directors who have at least ten years of experience in the utility industry, preferably in the Western Interconnection, including at least one director who has transmission operations experience, at least one director who has transmission planning experience, and at least one director who has generation operations experience. At any time where the membership of the Member Advisory Committee (MAC) is modified, as may be provided in other provisions of these bylaws, to include representation for Entities of the two Canadian Provinces of British Columbia and Alberta and the Mexican State of Baja California, at least one Director, elected subsequent to such MAC representation, shall have international experience corresponding to such geographic area(s) and/or representation in the MAC.

6.2.2 The remaining members of the Board of Directors shall be selected in an effort to ensure diversity of background and experience. Desirable categories of experience may include: regulatory or legal; accounting, finance or economics; environmental; end-user advocacy; information technology; compliance or standards; public sector; and international.

6.2.2.1 Transmission operations experience shall preferably include experience in control center operations at the senior management or officer level.

6.2.2.2 Transmission planning experience shall preferably include experience in modeling and/or planning transmission facilities, including economic and reliability modeling at the senior management or officer level.

6.2.2.3 Generation operations experience shall preferably include experience in development or operation of generation facilities, including economic and reliability modeling at the senior management or officer level.

6.2.2.4 Regulatory or legal experience shall preferably include at least one of the following types of experience: state, provincial or federal industry regulation; significant litigation experience ideally at the appellate level; evaluation of complex legal arguments; and advising clients with respect to settlements.

6.2.2.5 Accounting, finance or economic experience shall preferably include experience as a Chief Financial Officer, a Chief Account Officer, a

Corporate Risk Officer, a Certified Public Accountant, or the equivalent thereof.

6.2.2.6 Environmental experience shall preferably include experience advocating environmental interests before local, state or federal agencies or boards, and/or leadership experience in representing environmental interests in relation to energy issues.

6.2.2.7 End-user advocacy experience shall preferably include experience advocating end-user economic interests before local, state or federal ratemaking agencies or boards.

6.2.2.8 Information technology experience shall preferably include experience as a senior level manager responsible for integrating information technology services with organizational needs in areas such as capacity planning, budget and finance, acquisition and deployment, operations, change management, application development, trade ally relationships, user support, data quality, security and similar areas.

6.2.2.9 Compliance or standards experience shall preferably include experience as a senior level officer or manager for corporate compliance with internally and/or externally imposed requirements, rules or standards.

6.2.2.10 Public sector experience shall preferably include experience representing the public interests with respect to energy issues.

6.2.2.11 International experience shall preferably include experience as described in the previously listed experience categories, but in the Canadian provinces of British Columbia or Alberta, or the Mexican state of Baja California.

6.2.3 Director Affiliation Restrictions. A Director may not be a full time employee of a Registered Entity. Nor may a Director be affiliated with any Member or Registered Entity operating in the Western Interconnection, nor a Director of an entity performing the function of Reliability Coordinator in the Western Interconnection.

6.2.3.1 For the purposes of this section, "affiliated" shall mean (1) an employee of, (2) a contractor for, (3) an employee of a contractor for, or (4) an equity owner of Registered Entity or Member. For purposes of determining whether a Director is "affiliated" the term "Director" shall include a spouse and/or minor child of the Director.

6.2.3.2 A Director with an equity interest in private or publicly traded companies that are end-users of electricity in the Western Interconnection but are not

otherwise "affiliated" pursuant to the restrictions set forth in Section 6.2.2 shall not be considered to be "affiliated".

6.2.3.3 A Director with an equity ownership in a broadly diversified mutual fund which may from time to time include interests in one of the types of organizations described in Section 6.2.2, shall "not be considered to be "affiliated, provided that such equity interest cannot confer a controlling interest in a Member or Registered Entity within the Western Interconnection.

6.2.3.4 A Director receiving post-employment compensation, which compensation is not indexed to the success of the disbursing entity shall not be considered "affiliated".

6.2.3.5 A Director shall not be considered "affiliated" solely by having a contractual relationship with a state government that has one or more agencies that are Members, provided that the Director cannot be affiliated with the Member agency or agencies.

6.2.3.6 A Director shall not be considered "affiliated" for being a residential or small business end-user of electricity or for being affiliated with, a member of, or a contributor to an organization that represents a substantial number of end users or a substantial number of persons interested in the impacts of electric systems on the public interests or the environment, but a Director shall be considered "affiliated" if the Director is an employee of, or serves as a director, trustee, or officer or in any other policy-setting capacity with respect to any such organization.

6.2.3.7 The affiliation restrictions set forth in this Section are not all encompassing. Candidates and Board members are expected to disclose all known potential financial or relationship conflicts, including any known relationships between companies they have affiliation with and/or entities described in Section 6.2.2. Furthermore, any Nominating Committee will be expected to investigate and evaluate all potential conflicts, whether financial or otherwise.

6.2.4 In addition, the Board may provide for the Chief Executive Officer ("CEO") of WECC to be a voting, additional tenth, member of the Board through the inclusion of such a provision in the resolution the Board adopts appointing WECC's CEO. Such provision shall not permit the CEO to be a member of a Board committee or to cast either a tie-breaking vote or a vote that creates a tie. The CEO may not serve as the Chair or Vice-Chair of the Board.

6.3 Term of Office.

Directors will hold office for staggered terms of three (3) years, three Directors' terms ending each year. Each three (3) year term shall commence upon the adjournment of the portion of the Annual Member Meeting provided for in Section 5.3, in which all Members are counted for purposes of determining a quorum. Similarly, the three year terms of outgoing Directors shall end upon the adjournment of that portion of the Annual Member Meeting in which all Members are counted for purposes of determining a quorum, whether that results in a longer or shorter term than exactly three years.

6.4 Nomination, Selection and Compensation of Directors.

6.4.1 Nominating Committee. Candidates for a Director position shall be nominated by a Nominating Committee. The Nominating Committee shall consist of seven members. Three members shall be Directors, not standing for re-election, designated by the Board Chair. The remaining four Nominating Committee members shall be designated by the Member Advisory Committee and come from individuals serving on the Member Advisory Committee, with two (2) members being from Classes 1, 2, and/or 3, and two (2) members being from Classes 4 and/or 5.

6.4.1.1 If the Member Advisory Committee does not designate MAC members to serve on the Nominating Committee within 30 days of being notified of the Board Chair's designation of the three Directors to serve on the Nominating Committee, the Board Chair may designate MAC members to serve.

6.4.1.2 A Nominating Committee shall be formed each year not less than 180 days prior to the Annual Meeting. A Nominating Committee will continue to function until a replacement Nominating Committee is formed, but may not continue for a period longer than twelve (12) months from its creation, provided however, that the Board, by resolution, may authorize a Nominating Committee to function beyond twelve (12) months as the Board may determine is necessary.

6.4.2 Director Candidate Nominations.

6.4.2.1 The Nominating Committee shall develop candidate pools and make candidate nominations to the Members. The Nominating Committee may consider any qualified applicant in developing the candidate pool, and may identify applicants through the following process: (1) selecting and utilizing an independent search firm to provide the Nominating Committee with a list of qualified applicants for each Director position subject to election; (2) consider an incumbent Director who is willing to stand for reelection, including a review of such Director's tenure on the Board of Directors; (3) consider external nominations.

6.4.2.2 External parties, including but not limited to Members and Western Interconnection stakeholders, may recommend candidates (self-recommendations and third party recommendations) to the Nominating Committee for consideration, by submitting the following: the candidate's resume, a summary of the candidate's relevant experience, a disclosure statement from the candidate, and a letter of interest from the candidate. All recommendations from external parties must be submitted to the Nominating Committee within sufficient time for the Nominating Committee to evaluate the candidate prior to the notification required in Section 6.4.2.5.

6.4.2.3 The Nominating Committee shall review the qualifications of the potential candidates and put forth one nominee for each Director position up for election.

6.4.2.4 Five (5) affirmative votes of the Nominating Committee shall be necessary to put forth a nominee to the Members.

6.4.2.5 At least sixty (60) days in advance of the Annual Meeting, the Nominating Committee shall notify the Board Chair whether or not it has finalized all Director nominations. If the Committee fails to put forth a nomination for an open position, then the Board Chair may form a new Nominating Committee with different Board and Member Advisory Committee members, who shall be tasked with developing any remaining nominations for open Director positions.

6.4.2.6 Each nominee, put forth by the Nominating Committee, shall be presented for separate election by the Members.

6.4.3 Director Elections. Members will vote for each vacant Director position separately. A candidate will be elected to the Board upon majority vote of the Members as a whole in addition to a majority of the Classes (three of the five) having a majority vote from the Members of the individual Class.

6.4.4 Should a candidate fail to receive the required vote of the Members or Member Classes, the Board may:

6.4.4.1 conduct a new election of an alternate candidate put forward by the Nominating Committee, if any, or the Board may ask the Chair to establish a new Nominating Committee to recommence the nomination and election process. Where a candidate has not received the required vote of the Members and Member Classes, the director position shall remain vacant until a candidate is elected, except as provided in Section 6.7.2.

6.4.5 Annual Compensation of Directors. Every two years, or sooner if, in the discretion of the CEO, a new survey is required, the CEO shall contract with an appropriate firm to conduct a national compensation survey, which shall provide an independent review of the compensation paid independent directors. The latest survey so procured shall be used by the Nominating Committee to make an annual recommendation for the compensation of Directors for the following year. Any such recommendation shall require five (5) affirmative votes of Nominating Committee members. This recommendation shall be presented to the MAC no later than one hundred fifty (150) days prior to the Annual Meeting. The MAC shall set the compensation for the Directors at least one hundred and twenty (120) days prior to the Annual Meeting. When making this decision, the MAC shall consider the recommendation of the Nominating Committee and any other material relevant to setting Director compensation. If the Nominating Committee is unable to reach the five (5) vote majority necessary to make a compensation recommendation, the MAC shall make no changes to the compensation paid Directors for the following year.

6.5 Removal of Directors.

The Members or the Board may remove a Director before completion of the Director's term of office pursuant to the following provisions.

6.5.1 Removal by the Members. Directors may be removed only for gross negligence, violation of local, state, provincial, or federal laws, gross misconduct, or failure to meet the fiduciary obligations of Directors.

6.5.1.1 Removal of a Director will be by a vote of a majority of all the WECC Members, not just those Members voting, in addition to a majority of the Classes (three of the five) having a majority vote from the Members of the individual Class. Removal may only take place at a meeting called for that purpose by notice provided in accordance with the notice requirements for member meetings. A vote, by all Members, to consider removal of a Director will occur based upon a petition, for such an all-Member vote, supported by twenty percent (20%), each, of the Members of three of the five Member Classes.

6.5.2 Removal by the Board. The Board may remove any Director for gross negligence, violation of local, state, provincial, or federal laws, gross misconduct, or failure to meet the fiduciary obligations of Directors. Such removal will only occur upon the affirmative vote of not less than six (6) Directors.

6.6 Resignation.

Any Director may resign from their position at any time by written notice to the Board by delivery to the Chair. The acceptance of a resignation will not be required to make it effective.

6.7 Procedures for Filling Vacant Director Positions.

6.7.1 Director Vacancies. If the position of any Director becomes vacant prior to its normal term expiration, the remaining Directors may charge the Nominating Committee with selecting a successor immediately. The Nominating Committee will follow the requirements set out in Sections 6.2.1 and 6.2.2 in its selection of any successor Director. Alternatively, if less than one (1) year remains in the term of that Director, the remaining Directors may choose to leave the position vacant for the remainder of the term.

6.7.2 Holdover to Cure Procedural Vacancies. Whenever an incumbent Director is a candidate for a Director position and a vacancy would be created due to expiration of the Director's term-, the Director may continue to serve, for up to an additional 12 months, until such time as an election of the Director's position can be conducted, provided the vacancy arises from a lack of quorum or other procedural inability to elect a candidate for the Director position.

6.7.3 Should the number of serving Directors fall below seven (7), the Board may appoint one or more individuals to serve as temporary Directors until such time as replacement Directors can be elected by the Members.

6.7.3.1 In appointing temporary Directors, the Board shall select individuals who meet the requirements of Section 6.2.

6.8 Duties of Directors.

The Directors will have the following duties:

6.8.1 Fiduciary Obligation to WECC: All Directors, will have a fiduciary obligation to WECC consistent with the requirements for Directors of Utah non-profit corporations. Members of the Board will at all times act in conformance with such requirements, these Bylaws and the Standards of Conduct set forth in Appendix A.

6.8.2 Preserve Non-Affiliated Status: Throughout their terms, Directors will have a duty to avoid any affiliation that is inconsistent with the qualifications for Directors in Section 6.2.2 of these Bylaws. If a Director becomes aware of any intervening disqualification, he/she must either resign or eliminate the disqualification (e.g., dispose of securities) within sixty (60) days.

6.9 Powers of Directors.

The management of all the property and affairs of WECC will be vested in the Board of Directors. The Board will hold annual elections to select a Board Chair and to fill any other Board officer positions that may be created by the Board or required by applicable law. The Board may exercise all the powers of WECC and do all lawful acts and things (including the adoption of such rules and regulations for the conduct of its meetings, the exercise of its powers and the management of WECC) as are consistent with these Bylaws and the Articles of Incorporation. The Board will give serious consideration to the Member Advisory Committee's and the Western Interconnection Regional Advisory Board's (or any successor) recommendations. The Board will respond to Member

Advisory Committee and Western Interconnection Regional Advisory Board recommendations through a means which the Board determines appropriate.

6.10 Delegation of Board Authority.

The Board may delegate to the Chief Executive Officer or to any Board Committee formed pursuant to Section 7.7.3 any or all of its powers and authority except: 1) any power which it may not delegate pursuant to applicable Utah law; 2) the power to adopt any reliability standard; 3) the power to determine when to exercise the Backstop Authority of WECC; 4) the power to approve budgets; 5) the power to form committees; 6) the power to amend the Bylaws; 7) the power to elect the Chair and other officers of the Board; and 8) the power to hire, fire or set the terms of employment of the Chief Executive Officer. The Board may also delegate to any Member committee the power to make specific decisions, subject to the right of any Member to appeal any of such decisions to the Board within 30 days of the committee vote on the decision by writing a letter to the Chief Executive Officer that describes in reasonable detail the grounds for appeal, and requests that the appeal be considered by the Board at its next regularly scheduled meeting, subject to applicable notice requirements. Delegation will be by express decision and will require the affirmative vote of not less than a majority of the Directors. Any Director may call for a vote to rescind such delegation at any time and such delegation will be rescinded if a majority of the Directors vote to do so.

6.10.1 Notice to Members. Within seven (7) days of any decision delegated pursuant to Section 6.10, except for routine decisions of the Chief Executive Officer, Members will be notified of the decision by electronic mail, posting on the WECC website and any other means determined appropriate by the Board. Routine decisions of the Chief Executive Officer will be noticed in periodic reports to the Board and Members as determined by the Board, which will be sent to Members by electronic mail and posted on the WECC website.

6.10.2 Board Review of Delegated Decisions. Decisions delegated pursuant to Section 6.10 will be reviewed by the Board at the request of any Director, provided such request is lodged with the Secretary within thirty (30) days of the notice. Whenever it determines that a matter requires an urgent decision, the Board may shorten the deadline for requests for review, provided that: 1) the notice and opportunity for review will be reasonable under the circumstances; and 2) notices to Members will always contain clear notification of the procedures and deadlines for Board review. A request for review of a decision will stay the effect of the decision pending review unless the Board in making the delegation expressly determines otherwise.

7. Procedures for Board Decisions.

7.1 Quorum.

No business will be conducted by the Board unless at least five (5) Directors are present, or six (6) Directors if the CEO is counted to determine a Board quorum.

7.2 Majority Vote.

A decision of the Board will require an affirmative vote of a majority of Directors present and not abstaining; provided that no decision of the Board shall be made with fewer than three (3) affirmative votes, or four (4) affirmative votes if the CEO is counted to determine a Board quorum. Directors may not vote by proxy or by absentee ballot, but Directors may participate in Board meetings by telephone as provided in Section 7.3 of these Bylaws.

7.3 Attendance at Board Meetings by Teleconference.

Any or all of WECC's Directors may participate in any meeting of the Board by telephone conference or any other means of communication that enable all Directors participating in the meeting to simultaneously hear one another. Every Director participating in a meeting in the manner described in the preceding sentence will be deemed to be present in person at that meeting.

7.4 Board Action by Unanimous Consent.

7.4.1 Action Without a Meeting. Unless WECC's Articles of Incorporation or applicable law provides otherwise, action required or permitted to be taken at a meeting of the Board may be taken without a meeting through one or more written consents describing the action taken. Any Board action taken by written consent must be signed by all Directors in office at the time the action is taken. Such actions must be noticed to Members in accordance with Section 7.5 and Members must be given an opportunity to comment prior to the Board taking such actions through electronic mail, comments on the website or other appropriate means. The required notice of such meeting may generally describe the arrangements (rather than the place) for the holding of the meeting. All other provisions herein contained or referred to will apply to such meeting as though it were physically held at a single place. All Board actions by written consent must be filed with WECC's Board meeting minutes. Action taken under this Section is effective when the last Director signs the consent, unless the consent specifies an earlier or later effective date. Any action by written consent has the same effect as a meeting vote and may be described as such in any document.

7.4.2 Waiver of Procedures. For any specific action at any noticed meeting of the Board, and under exigent or unusual circumstances, the Board by unanimous vote of those present may waive any procedural requirement applicable to Board decision-making, including any requirement for notice of a specific potential action, except for the following: 1) the requirement for notice of the time and place of the meeting pursuant to Section 7.5; 2) the quorum and voting requirements of Sections 7.1 and 7.2; and 3) any non-procedural limitation on the power of the Board to make a decision, including, but not limited to, those restrictions in Sections 6.10 (limiting the power to delegate) and 12.1 (limiting the power to amend the Bylaws). Whenever such action is taken, a statement describing the action, the exigent or unusual circumstances, the specific procedure waived, the basis for the waiver and the votes of all Directors present shall be

posted on the website and communicated in writing or by e-mail to all Members within five (5) days.

7.5 Notice of Board Meetings.

7.5.1 Regular Meetings. Except as set forth in Section 7.5.2 regarding urgent business, all regular business of the Board will occur at the Board meetings, at least twenty-one (21) days' advance notice of which has been provided by the Chief Executive Officer to all Directors and all Members. Notice will include an agenda that will identify those matters on which a vote will be taken at the meeting. The foregoing requirement shall not preclude the Board from taking an action that is different from the specific proposed action identified in the agenda, as long as the relevant subject matter has been reasonably identified in the agenda. The Directors will establish a regular meeting schedule that will be made available to the Members. The schedule will include not less than two meetings of the Board annually.

7.5.2 Special Meetings. Whenever the Chair of the Board or any three (3) Directors find that there is urgent business requiring Board action before the next regular Board meeting, a special meeting of the Board may be called. Such special meetings will be held upon as much written notice to each Board Member and all Members as is possible under the circumstances, which will not be less than three (3) days. However, this notice of special meetings may be waived if: 1) the waiver is by a writing signed by a quorum of Board members; and 2) as much notice of the meeting as practicable has been given to WECC Members via e-mail and posting on the WECC website.

7.5.3 Public and Website Notice. Public notice of each meeting of the Board will be placed on WECC's website at least ten (10) days before such meeting (or such lesser time as provided pursuant to Section 7.5.2). In addition, the Chief Executive Officer will provide notice of each meeting by first-class mail, facsimile or electronic mail to each member of the public who so requests and who has provided appropriate information regarding delivery of notice.

7.6 Open Meetings.

Except as provided in Section 7.6.1, all regular and special meetings of the Board will be open to observation by any Member and any member of the public.

7.6.1 Closed Session. Notwithstanding the provisions of Section 7.6, upon an affirmative vote of two-thirds (2/3) of the Directors present, the Board may meet in closed session: 1) to consider the employment, evaluation of performance, or dismissal of an employee of WECC and to deliberate regarding decisions the Board may be called upon to make regarding the nomination, qualification, appointment, or removal of a member of the Board of Directors; 2) to discuss pending or proposed litigation and to receive confidential attorney-client communications from legal counsel; and 3) to receive and discuss any

information that is privileged, trade secret, cybersecurity, critical energy infrastructure information (as defined by the FERC), protected from public disclosure by law or that the Board determines should be confidential in order to protect a legitimate public interest.

7.6.1.1 Attendance by an Affected Director. Closed sessions of the Board may not be attended by a Director under the following circumstances: 1) where the qualifications or performance of the Director or the Director's spouse or children are being discussed; 2) where the Director is employed by an entity that is or is likely to become a party to the litigation being discussed; and 3) where the Director or the Board determines that the Director would have a serious and substantial conflict of interest by becoming privy to confidential attorney-client or trade secret information that is to be presented to the Board in closed session.

7.6.1.2 Announcement of Closed Session. Before adjourning into closed session, the Chair of the Board will announce the purpose of the closed session in a manner that provides the public an understanding of the general subject matter to be discussed but which does not reveal sensitive or personal information. The Board will not discuss additional items outside the scope of this description.

7.6.1.3 Confidentiality of Closed Session. All Directors and others present will maintain the confidentiality of discussions and decisions made in closed session. The Board will appoint a secretary for closed session to keep a minute book for the purpose of recording the subject matter discussed in closed session and any actions taken in closed session. After a closed session has ended, the Board Chair shall provide the public a general description of the business conducted during the closed session, without breaching the confidentiality of the information used in the session.

7.7 Board Committees.

7.7.1 Governance Committee. The Chair will appoint a Governance Committee that shall: oversee implementation and amendment of these Bylaws and address such other issues pertinent to Governance as the Board may choose to delegate to it. The Chair will designate one of the appointed Directors to be the Chair of the Governance Committee.

7.7.2 Nominating Committee. Constituted as described in Section 6.4.1 of these Bylaws.

7.7.3 Other Board Committees. The Board may appoint such Board committees as it deems necessary from time to time to carry out its business affairs. In appointing such committees, the Board will specify their purpose, membership, voting, notice and meeting procedures and such other direction as the Board may deem

appropriate. The Board may appoint one or more Members or other persons to participate in Board committees as full voting members or as non-voting advisory members.

7.7.4 Standards of Conduct for Board Committee Members. Members of Board committees shall comply with the Board Member Standards of Conduct set forth in Appendix A.

8. Member Committees.

8.1 Purpose.

WECC will have committees composed of its Members to advise and make recommendations to the Board. Such committees will include both standing committees required by these Bylaws and such other committees as the Board may choose to create.

8.2 Standing Committees.

WECC will have the following standing committees:

8.2.1 Member Advisory Committee. This committee is comprised of Member representatives elected by the Member Classes, or subclasses, as set forth herein.

8.2.1.1 The committee shall advise the Board on any matters the Board requests the committee to evaluate or consider; and advise the Board on matters as the committee deems appropriate.

8.2.1.2 The committee's Chair or designee will attend the Board's meetings to provide advice, clarifications or respond to Directors' questions. The Board Chair and committee Chair shall develop guiding principles and procedures as necessary, to ensure open, effective, and efficient dialog between the MAC and Board. Such guiding principles and procedures may be amended by the Board and committee's Chairs.

8.2.2 WECC Standards Committee. This committee will oversee the process for responding to requests for Regional Reliability Standards and Regional Criteria in accordance with the Reliability Standards Development Procedures. The WECC Standards Committee is responsible for determining if a request for a Regional Reliability Standard or a Regional Criteria is within the scope of WECC's activities, and for overseeing the drafting, comment and voting process for a Regional Reliability Standard or Regional Criteria. The WECC Standards Committee shall also oversee the process for responding to requests for interpretations of Regional Reliability Standards and Regional Criteria. The WECC Standards Committee shall consist of one member from each of the WECC Standards Voting Sectors set forth in ~~Section 8.6.5.2~~the Reliability Standard Development Procedures, and a member of the WECC Board who shall act as chair of this committee. The WECC Board shall approve a Charter for the

WECC Standards Committee that describes the WECC Standards Committee membership selection process.

8.2.3 Planning Coordination Committee. This committee will advise and make recommendations to the Board on all matters within the jurisdiction of WECC pertaining to maintaining reliability through evaluating generation and load balance and the adequacy of the physical infrastructure of the interconnected Bulk Electric System within the Western Interconnection.

8.2.4 Operating Committee. This committee will advise and make recommendations to the Board on all matters within the jurisdiction of WECC pertaining to maintaining reliability through the operation and security of the interconnected Bulk Electric System in the Western Interconnection.

8.2.5 Market Interface Committee. This committee will advise and make recommendations to the Board on the development of consistent Market Interface practices and compatible commercial practices within the Western Interconnection. It will consider matters pertaining to the impact of WECC's reliability standards, practices, and procedures on the commercial electricity market in the Western Interconnection, and facilitate analysis of the impact of electricity market practices on electric system reliability.

8.3 Other Committees.

8.3.1 The Board may create such other committees as it may desire from time to time. The Board will specify the functions, duties and responsibilities of any such committee at the time of its creation. The Board will also specify the membership rules, quorum requirements, voting levels and meeting and notice requirements at the time of creation. Any changes in the membership rules, quorum requirements, or voting levels of a committee, once established by the Board, will require a seventy-five percent (75%) vote of the Board to alter. The specific function or sunset date for a committee will be designated by the Board at the time of the committee's creation. The committee will terminate its activities upon the completion of its function or the expiration of the date set by the Board.

8.4 ~~Assessment of Standing Committee Activities.~~ [Repealed]

~~Within eighteen months of the Federal Energy Regulatory Commission (FERC) approval of Section 6 establishing an independent Board, and, thereafter, within no longer than a five year period after the previous review, the Board of Directors will conduct a thorough review of the activities of each of WECC's standing committees to assess whether they are effectively furthering WECC's purposes in a manner that is consistent with: 1) the provisions of Section 2.2 of these Bylaws; and 2) the then current state and the expected future evolution of the electric power industry within the Western Interconnection. The Board's review will assess whether there are any aspects of the standing committees' functions or~~

~~procedures that impede development of WECC standards, obligations, processes, and decisions that are timely, fair, effective, and reasonable in view of the commercial, legal, regulatory, and economic needs and objectives of the affected Members. The Board will propose to the membership, at the Members' annual meeting held after completion of a review required by this Section 8.4, any changes to standing committee structures, functions, or procedures that the Board determines are warranted by its review.~~

8.5 Procedures for Member Advisory Committee Decision-Making.

8.5.1 Member Advisory Committee (MAC). The committee shall be comprised of three representatives from each of the five (5) Member Classes, for a total of fifteen (15) members.

8.5.1.1 The Board, by resolution, may create up to three additional representative positions on the MAC, to include representation for Entities of the Canadian Provinces of British Columbia, and/or Alberta, and/or the Mexican State of Baja California. The Board resolution shall set forth the terms through which Canadian or Mexican representatives shall be selected and serve.

8.5.2 MAC Member Elections. At the Annual Members Meeting, each Member Class shall conduct elections to elect Class member representatives for the committee. As set forth herein, each Class may subdivide into up to three subclasses for purposes of electing a Class' MAC members.

8.5.2.1 Committee member terms. Each committee member will serve a three year term. Terms shall be staggered such that one of each Class' representative committee member's terms ends each year. Class committee members may have term limits as determined appropriate by the Class or subclass electing such committee member.

8.5.2.2 Subclasses. Each Class will determine the need for diversity within the Class (e.g., geographic, stakeholder issues, etc.) which may lead to the establishment of subclasses. A Class may subdivide into up to three subclasses. Each Class shall determine to establish or discontinue its subclasses, if any, by majority vote of the members in the Class.

8.5.2.3 Committee member nominations and elections. Only members of each Class, or subclass, if applicable, may nominate and vote on candidates for election as a MAC member representative for their respective Class or subclass.

8.5.2.3.1 A Class or subclass candidate need not be a member of the Class or subclass, neither an employee of a Class or subclass member.

8.5.2.3.2 A quorum of a majority of the members of a Class or subclass must be present in order to elect a MAC member for the Class or subclass; election shall be by simple majority of votes cast.

8.5.2.3.3 Where there are more candidates for election than positions to fill, absentee ballots shall allow voters to order the candidates by order of preference so that their wishes may be honored in case a runoff is required. Absentee ballots shall be counted in the first ballot based on the top choice, or the top two or three choices if more than one seat is being filled. In any runoff election, absentee ballots shall be counted based on the highest preferences indicated for the candidates who remain in the runoff election.

8.5.2.3.4 Other nomination and election procedures, beyond those contained in these bylaws, may be proposed for a Class or subclass. Contingent upon their approval, by the General Counsel, for their submission to Members, they may be adopted for implementation by majority vote of the Member Class or subclass.

8.5.3 MAC Member Vacancy by Resignation or Removal

8.5.3.1 Resignation. At any time, any MAC member may resign from their position by providing written notice of resignation to the MAC Chair. Such notice shall be effective as of the date the notice is submitted to the MAC chair.

8.5.3.2 Removal. The MAC or the Member Class or subclass which elected a MAC member may remove the MAC member prior to completion of the Mac member's term of office as set forth herein:

8.5.3.2.1 Removal by the MAC. The MAC may remove any MAC member for gross negligence, gross misconduct, violation of local, state, provincial, or federal law, or gross failure to carry out the duties of a MAC member. Such removal will only occur after the affirmative vote of at least two-thirds (2/3) of the MAC members.

8.5.3.2.2 Removal by the Electing Class or Subclass. The electing Member Class or subclass may remove any MAC member representing that respective Class or subclass. Such removal will occur after the affirmative vote of a majority of the Members of the electing Class or subclass.

8.5.3.3 Vacancy. Whenever a MAC vacancy occurs, the MAC Chair shall conduct a proper and effective election, allowing for a reasonable period to select candidates and to organize such an election.

8.5.3.3.1 Whenever a MAC vacancy occurs, the MAC Chair shall, as promptly as feasible, conduct an election consistent with these Bylaws for the Member Class or subclass from which the vacancy arose, allowing for a reasonable period to select candidates and to organize such an election.

8.5.3.3.2 Until an election can be held, the MAC Chair may appoint an interim MAC member to fill the vacancy as may be required to meet the MAC quorum requirements of 8.5.8. The appointee shall serve until an effective election can be held. Any interim appointment must come from Members of the same Class or subclass from which the vacancy arose.

8.5.4 MAC officers. At the Annual Meeting, after incoming MAC members have been duly elected by the Member Classes or subclasses, if applicable, the MAC will elect the MAC Chair and MAC Vice-Chair from the MAC members. The Chair and Vice-Chair must represent different Classes, and shall serve one year terms, measured from the Annual Meeting to the next Annual Meeting. In the event of the resignation or removal of the Chair or Vice-Chair, the MAC members shall, at their next regular or special meeting, whichever is sooner, elect a new MAC Chair or MAC Vice-Chair, respectively.

8.5.5 MAC Member Duties. All MAC members shall have a duty to represent the interests of their Member Class or subclass. All MAC members shall maintain regular contact with the members of their Member Class as issues are considered by the MAC, and shall make reasonable good faith efforts to present and discuss both majority and minority opinions from their Member Class on matters before the MAC.

8.5.6 Regular and Special Meetings.

8.5.6.1 Regular meetings. All regular business of the MAC shall occur at MAC meetings which are noticed pursuant to Section 8.5.7. The MAC shall meet in person not less than two times per year, including once in conjunction with the Annual Meeting. The MAC shall establish a regular meeting schedule, which will be made available to the Members and Directors electronically, and available to the public through posting on the WECC website.

8.5.6.2 Special Meetings. Whenever the MAC Chair finds, or upon request to the MAC Chair from any five (5) MAC Members, that there is urgent business requiring MAC consideration or action prior to the next regularly

scheduled meeting, then a special meeting shall be called with notice given in accordance with Section 8.5.7.

8.5.7 Notice.

8.5.7.1 Regular Meetings. All regular meetings of the MAC shall require at least twenty-one (21) days written notice to the MAC members, the Directors, and the Members. Such notice shall specify the time and place of the meeting, and an agenda of the business to be conducted including those matters upon which a vote will be taken. Notice of regular MAC meetings shall be effective upon electronic distribution, and shall be posted to the WECC website within one (1) business day of electronic distribution.

8.5.7.2 Special Meetings. Any special meetings of the MAC shall require at least ten (10) days written notice to the MAC members, the Directors, and the Members. Such notice shall specify the time and place of the meeting, and an agenda of the business to be conducted, including those matters upon which a vote will be taken. Notice of special MAC meetings shall be effective upon electronic distribution, and shall be posted to the WECC website within one (1) business day of electronic distribution.

8.5.8 Quorum. No business shall be conducted by the MAC unless a majority of the MAC members is present, including at least one MAC member from each Member Class which elects MAC members (not including subclass designations).

8.5.9 Majority Vote. A decision of the MAC shall be upon a simple majority vote of committee members voting unless otherwise required in other bylaw provisions.

8.5.10 Remote Participation at MAC Meetings. Any or all of the MAC members may participate in any meeting of the MAC electronically or by telephone, or by any other means of communications which enables the MAC members to simultaneously hear one another. Every MAC member participating in a meeting in this manner will be deemed to be present in person at the meeting.

8.5.11 Reporting to the Board. The MAC Chair, or designee, shall provide a report to the Board at each Board meeting detailing the business carried out by the MAC, and advising the Board of MAC recommendations on matters as set forth in Section 8.2.1 herein. In the event that there are dissenting MAC member opinions regarding a matter on which the MAC is advising or providing recommendations to the Board, the MAC Chair, or designee, shall present dissenting opinions and rationales in conjunction with the respective MAC advice or recommendations.

8.5.12 Open Meetings. Except as provided in Section 8.5.13, all regular and special meetings of the MAC will be open to observation by any Member, Director, and/or any member of the public.

8.5.13 Closed Session. Notwithstanding the provisions of Section 8.5.12, after a quorum has been established at any MAC meeting and upon an affirmative vote of two-thirds (2/3) of the MAC members present, the MAC may close an open meeting and reconvene in closed session in the following instances: (1) to receive and/or discuss confidential attorney-client privileged information from WECC's counsel; or (2) to receive and discuss any other information which is privileged, confidential, proprietary, trade secret, or otherwise protected from public disclosure by law.

8.5.13.1 Attendance by an Affected MAC Member. Closed sessions of the MAC may not be attended by a MAC member under the following circumstances: (1) when the qualification or performance of the MAC member is being discussed; (2) when the MAC member is employed by an entity that is or is likely to become a party to the litigation or legal issue being discussed; or (3) when the MAC Chair determines that the MAC member would have a conflict of interest by becoming privy to the privileged or confidential information that is to be presented to or discussed by the MAC in closed session.

8.5.13.2 Attendance by Directors. Any member of the Board may attend a closed session of the MAC unless the topic considered by the MAC concerns the Director.

8.5.13.3 Announcement and Adjournment of Closed Session. Prior to adjourning to a closed session, the MAC Chair will announce the purpose of the closed session in a manner that provides the public an understanding of the general subject matter to be discussed, but which does not reveal privileged, confidential or otherwise sensitive personal information. The closed session then shall be limited in scope to the publicly stated purpose of the closed session. After the closed session has ended, the MAC Chair shall provide the public a general description of the business conducted during the closed session, without breaching the confidentiality of the information used in the session.

8.5.13.4 Confidentiality of Closed Session. All MAC members and any others present at a closed session shall maintain the confidentiality of the information, discussions, and decisions made in closed session. Unless otherwise required, all MAC members and closed session attendees shall execute an appropriate confidentiality agreement provided by WECC's General Counsel. The MAC Chair will appoint a secretary for the closed session to take minutes of the closed session, which shall be delivered to the WECC Corporate Secretary. Minutes of the closed session will be maintained confidential by the Corporate Secretary.

8.5.14 MAC Committees. The MAC may appoint such subcommittees and work~~ing~~ groups as it deems necessary from time to time to carry out its business affairs. In

appointing such subcommittees or work~~ing~~ groups, the MAC will specify, in a charter, their purpose, membership, voting, notice and meeting procedures, and other such direction as the MAC deems appropriate. The MAC may appoint one or more MAC members or other persons to participate in MAC subcommittees or work~~ing~~ groups as full voting members or as non-voting advisory members.

8.5.15 MAC meetings and activities will be self-~~-~~funded by Members with respect to labor and travel expenses. However, WECC and WECC staff will provide facilitation and coordination support, including payment for the expenses of meeting facilities. A MAC member may seek reimbursement, from WECC, for reasonable and actual travel expenses arising from attendance at MAC meetings, consistent with WECC employee travel expense reimbursements, where such MAC member's travel expenses are not reimbursed by any Member or other source.

8.6 Procedures for Committees other than the Member Advisory Committee.

8.6.1 Reports to Board of Directors. Action by a committee will be in the form of a recommendation for Board action except in those instances in which the Board has, by resolution, specifically delegated to a committee the power to take action subject to an appeal to the Board by any Member. The recommendation of a committee must be forwarded to the Board for its action along with any minority or dissenting reports filed with the committee Chair or Vice-Chair.

8.6.2 Subcommittees, Task Forces and Ad Hoc Groups. Any Board or member committee may create such subcommittees, task forces or other ad hoc groups ("subcommittee") as it deems appropriate to carry out the committee's responsibilities consistent with these Bylaws and the direction of the Board. The composition, responsibilities and procedures of such groups shall be specified by the committee as appropriate; provided, however that: 1) the committee may only delegate to such subcommittee responsibilities that are within the scope of the committee's responsibilities pursuant to these Bylaws and direction of the Board; and 2) the subcommittee may only make recommendations to the committee. A committee may create a subcommittee without prior approval of the Board; provided, however, that the committee shall promptly inform the Board in writing and at the next Board meeting regarding the creation of the subcommittee. The notification to the Board shall include a charter for the subcommittee that describes how members of the subcommittee will be selected, the duties of the subcommittee, and whether the committee has established a sunset date for review of (1) the need for the subcommittee and (2) the charter of the subcommittee.

8.6.3 Committee Officers. The Board will appoint the Chair and Vice-Chair of each committee. The Committee Chair or Vice-Chair will preside over all meetings of the committee and will report recommendations of the committee to the Board of Directors. The Chair and Vice-Chair will be responsible for informing the Board regarding minority opinions and other information required by the Board along

with overall committee recommendations. Whenever the committee elects to form a subcommittee to represent regions or address specific tasks, the Chair (or in the absence of the Chair, the Vice-Chair) will have the power to appoint the members of such subcommittee from both members of the committees and non-members. Upon resignation of the Committee Chair, the Vice Chair shall serve as Chair until the Board appoints a replacement. Upon resignation of the Vice Chair, the Chair may appoint a temporary Vice Chair to serve until the Board appoints a replacement. Upon resignation of both the Chair and Vice Chair, the Chair of the Board may appoint one or more temporary replacements to serve until the Board appoints permanent replacements.

8.6.4 Committee Membership. Except as provided in Sections 8.2.2 and 8.6.4.1, any Member of WECC may designate one representative as its committee member to any standing committee or other committee. The WECC Member will have one vote at any committee meeting through that committee member. Any number of other persons may attend a committee meeting, but such persons will have no right to vote without a prior designation of representation by a WECC Member.~~, except that interested stakeholders may, under Section 8.6, vote on proposed Reliability Standards or revisions to Reliability Standards~~.

8.6.4.1 Dual Representation for Functionally-Separated Members. A Member which has distinct and functionally-separated interests as both a transmission provider and a transmission customer may designate two representatives as committee members to any standing committee, one to represent each functionally separate interest. Each such committee member will have one vote. The privilege granted by this Section is subject to revocation by the Board on a case-by-case basis or generally whenever the Board finds, upon petition from any Member or its own motion, that such dual representation creates unfairness or imbalance within a committee.

8.6.5 Committee Voting and Classes.

8.6.5.1 Classes. For purposes of voting, committees, excluding the WECC Standards Committee and the Member Advisory Committee, will have three classes of membership:

8.6.5.1.1 Transmission Provider Members;

8.6.5.1.2 Transmission Customer Members; and

8.6.5.1.3 States and Provincial Members (Member Class 5).

~~8.6.5.2 WECC Standards Voting Sectors. For purposes of voting on Regional Reliability Standards and Regional Criteria, a Ballot Body consisting of five registered sectors (8.6.5.2.1 through 8.6.5.2.5) and three non-~~

registered sectors (8.5.5.2.6 through 8.6.5.2.8) shall be established. If an Entity is eligible for a registered sector, then that Entity may be eligible for more than one registered sector. An Entity can only be in one non-registered sector. An Entity cannot be in both a registered and a non-registered sector. The first five sectors (8.6.5.2.1 through 8.6.5.2.5) shall be limited to Entities which are listed in the North American Electric Reliability Corporation ("NERC") compliance registry and to those Canadian and Mexican Entities that perform functions that, if performed in the United States, would allow these Entities to be registered for compliance in the NERC compliance registry. A WECC member or Participating Stakeholder who wishes to participate in voting on Reliability Standards and Regional Criteria shall apply for membership in the Ballot Body in any or all of the registered WECC Standards Voting Sector(s) for which it believes it is eligible, or one of the three non-registered sectors. WECC staff shall confirm Participating Stakeholder's eligibility for such Sector(s). Decisions of the staff to approve, deny, or restrict the admission of an entity to a voting sector may be appealed to the Governance and Nominating Committee. Decisions of the Governance and Nominating Committee to affirm or reverse such decisions of staff may be appealed to the Board. The following sectors are established:

8.6.5.4.0 Transmission Sector. This sector consists of Western Interconnection Entities registered in the NERC compliance registry as transmission owners, transmission operators, transmission service providers, or transmission planners;

8.6.5.6.0 Generation Sector. This sector consists of Western Interconnection Entities registered in the NERC compliance registry as generation owners or generation operators;

8.6.5.8.0 Marketers and Brokers Sector. This sector consists of Western Interconnection Entities registered in the NERC compliance registry as purchasing-selling Entities;

8.6.5.10.0 Distribution Sector. This sector consists of Western Interconnection Entities registered in the NERC compliance registry as distribution providers or load-serving Entities;

8.6.5.12.0 System Coordination Sector. This sector consists of Western Interconnection Entities registered in the NERC compliance registry as balancing authorities, reserve sharing groups, planning authorities, resource planners, interchange authorities, or reliability coordinators. WECC may cast a vote in this sector;

8.6.5.14.0 End Use Representative Sector. This sector consists of non-registered members of WECC Member Class Four;

~~8.6.5.16.0 State and Provincial Representatives Sector. This sector consists of non-registered WECC members of WECC Member Class Five;~~

~~8.6.5.18.0 Other non-registered WECC Members and Participating Stakeholders Sector. This sector consists of consultants and other members of WECC Member Class Three, or interested stakeholders who qualify for Participating Stakeholder status but are not registered in the NERC compliance registry.~~

~~8.6.5.20~~8.6.5.2 Voting. Except as provided in Section 4.5.2 ~~and 8.6.5.4~~, each committee member will have one vote. In order for a recommendation to be made to the Board, such recommendation must receive a simple majority vote of both: 1) committee members present and voting from the Transmission Provider Class; and 2) committee members present and voting from Transmission Customer Class. The Board will adopt voting and record-keeping procedures to ensure that committee voting is conducted consistent with these Bylaws. This requirement will also apply where decision making power has been delegated to a committee pursuant to Section 6.9.1.

~~8.6.5.20.1~~8.6.5.2.1 State and Provincial Votes. The position of the state and provincial Class committee members must be recorded, but the failure of a proposed recommendation or decision to obtain a simple majority vote of the state and provincial committee members will not prevent the recommendation or decision from being posted for due process comment or sent to the Board of Directors.

~~Voting on Regional Reliability Standards and Regional Criteria. Whenever the WECC Standards Committee determines that a draft Regional Reliability Standard or Regional Criteria is ready for consideration by the Ballot Body, it shall be presented for a vote. Members of the Ballot Body shall be provided an opportunity to opt into a Ballot Pool formed for purposes of voting on each of the proposed Regional Reliability Standards or Regional Criteria as described in the Reliability Standards Development Procedures. A two-thirds quorum of the specially formed Ballot Pool is required for a valid vote. Members of the Ballot Pool shall cast their vote in the WECC Standard Voting Sectors listed in 8.6.5.2. When members of the Ballot Body who are eligible to vote in more than one of the sectors defined in 8.6.5.2 join the Ballot Pool, they may cast one vote in each voting sector in which they are eligible. Calculation of the vote by the WECC Standard Voting Sectors will be pursuant to a weighted sector voting formula as described in the Reliability Standards Development Procedures. If the Ballot Pool~~

~~approves a proposed Regional Reliability Standard or Regional Criteria, then that proposed Regional Reliability Standard or Regional Criteria will be recommended to the WECC Board. The process of approving proposed Regional Reliability Standards and Regional Criteria is further guided by the Reliability Standards Development Procedures.~~

8.6.6 Notice and Review of Committee Recommendations and Decisions (Due Process). Committee recommendations or decisions delegated to a committee pursuant to Section 6.9.1 will be subject to the due process provisions of this Section. Following a committee's development of a proposed recommendation or decision, the committee will post the proposed recommendation or decision on the WECC website for review and comment by other WECC Members, and other interested parties. The committee will provide all Members e-mail notification of the posting and will allow at least thirty (30) days for comment on the proposal. The committee will consider all such additional input before reaching its final recommendation or decision. If the committee's recommendation or decision changes significantly as a result of comment received, the committee will post the revised recommendation or decision on the website, provide e-mail notification to Members and provide no less than ten (10) days for additional comment before reaching its final recommendation or decision. Upon reaching its final recommendation or decision, the committee will forward it to the Board. Whenever it determines that a matter requires an urgent decision, the Board may shorten any time period set forth in this Section, provided that: 1) notice and opportunity for comment on recommendations or decisions will be reasonable under the circumstances; and 2) notices to Members will always contain clear notification of the procedures and deadlines for comment.

8.7 Procedures for Developing and Voting on Reliability Standards.

8.7.1 Rights and Obligations of WECC Members and Participating Stakeholders. All WECC Members and Participating stakeholders are entitled to participate in the development of and to vote on Reliability Standards, Regional Criteria or revisions, subject to any applicable obligations, limitations and conditions set forth in these Bylaws, and in accordance with the WECC Reliability Standards Development Procedures.

8.7.1.1 Participation. The right to participate in Reliability Standards and Regional Criteria development and voting includes the right to request the development or revision of a Reliability Standard, the right to receive notice of, attend and participate in related WECC discussions, the right to review information relevant to a Reliability Standard or revision, the right to provide written comments on a proposed Reliability Standard, Regional Criteria, or revision, the right to participate in voting on a Reliability Standard, Regional Criteria, or revision and the right to file an appeal requesting review of any decision on a Reliability Standard, Regional Criteria, or revision.

8.7.2 Voting. The procedures and conditions for voting by WECC Members and Participating Stakeholders are set forth in the Reliability Standards Development Procedures. ~~and in Sections 8.6.5.2 and 8.6.5.4 of these Bylaws. A Participating Stakeholder may only vote on a proposed Reliability Standard or revision if they have applied for and been granted Participating Stakeholder status in accordance with Section 8.7.2 below. A Participating Stakeholder is only entitled to vote on Reliability Standards and revisions, and may only vote on Regional Criteria if the proposed Regional Criteria could result in sanctions to a non-WECC member. A Participating Stakeholder is not entitled to vote in any other WECC committee balloting process or in elections for WECC Directors.~~

8.7.3 ~~Special Procedures~~Board Authority to Address Regulatory Directives. The Board shall have backstop authority to address regulatory directives as described in the Reliability Standards Development Procedures. ~~If the Board determines that the procedures for drafting and voting on Reliability Standards did not result in a proposed Reliability Standard that addresses a directive issued by an Applicable Regulatory Authority, the Board shall have authority to take certain actions as described in the Reliability Standards Development Procedures to ensure that a Reliability Standard responsive to an Applicable Regulatory Authority's directive is drafted, approved and/or submitted to the Applicable Regulatory Authority. In the event that a Reliability Standard or revision that is proposed in response to an Applicable Regulatory Authority's directive fails to achieve a majority vote of the Ballot Pool, or if a quorum of the Ballot Pool was not established upon re-ballot of a proposed Reliability Standard, then the Board has the authority to take appropriate actions, as described in the Reliability Standards Development Procedures, to ensure that a Reliability Standard responsive to a regulatory directive can be submitted to NERC and FERC with a request that it be made effective. To exercise such authority, the Board must find that the proposed Reliability Standard or revision 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. If the Board is unable to make this finding, then the Board may direct that the proposed Reliability Standard be filed with the Applicable Regulatory Authority as a compliance filing in response to the regulatory directive, along with a recommendation that the standard not be made effective and an explanation of the basis for the recommendation.~~

8.7.4 Participating Stakeholder Application Process. Any person or entity that is an interested stakeholder may apply to WECC for Participating Stakeholder status and, upon WECC's acceptance of such application, acquire the participation and voting rights set forth above in Section 8.7.1. WECC staff, under the direction of the CEO, will process applications and make the initial determination of eligibility for Participating Stakeholder status. Denial of Participating Stakeholder status may be appealed to the WECC Governance ~~and Nominating~~ Committee and, if denied by the Governance ~~and Nominating~~ Committee, to the

WECC Board. A person or entity's Participating Stakeholder status will be maintained so long as the Participating Stakeholder continues to meet the requirements set forth in Section 3.24 and participates in at least one WECC meeting per year at which a Reliability Standard or revision is discussed. In the event a person or entity's Participating Stakeholder status lapses due to failure to meet the above minimum participation requirement, the person or entity may restore Participating Stakeholder status by re-applying for Participating Stakeholder status and attending a WECC meeting at which a Reliability Standard is discussed.

8.7.5 WECC Standards Voting Sectors. WECC staff shall confirm eligibility for the WECC Standards Voting Sectors set forth in the Reliability Standards Development Procedures. Decisions of the staff to approve, deny, or restrict the admission of an entity to a voting sector may be appealed to the Governance Committee. Decisions of the Governance Committee to affirm or reverse such decisions of staff may be appealed to the Board.

8.7.6 WECC staff shall require Ballot Body members to identify their affiliations with other Ballot Body members. Affiliates within a single Standards Voting Sector may only have one vote in that Standards Voting Sector. Affiliates within a single Standards Voting Sector must designate a single Affiliate as the group's Ballot Pool member to vote in that Standards Voting Sector.

8.8 Notice of Committee Meetings.

8.8.1 Standing Committees. The committee Chair, with the assistance of the Chief Executive Officer, will ensure that not less than ten (10) days' notice of all standing committee meetings is posted on the WECC website and is also provided to: 1) members of the committee; 2) Participating Stakeholders (if the meeting concerns development or approval of a Reliability Standard or revision); and 3) any WECC Member or member of the public requesting notice. A committee may take up any matter at a duly noticed meeting including matters not expressly identified in the notice; provided, however, that a final recommendation to the Board must be made in accordance with Section 8.6.1.

8.8.2 Other Committees. Notice of other committee meetings will be provided in the manner adopted for such notice by the affected Members and in accordance with the requirements of Section 8.8.1.

8.9 Open Meetings.

All committee meetings of WECC will be open to any WECC Member, Director and for observation by any member of the public, except as set forth in these bylaws or in policies on closed sessions that the Board may adopt for the purpose of preventing public disclosure of information that the Board might more appropriately discussed in closed session.

9. The Chief Executive Officer, Officers, and Employees.

9.1 Designation of Officers and Terms of Office.

WECC will have a Chief Executive Officer, a Secretary, and any other officers specified by the Board from time to time. The Chief Executive Officer will also hold the title of President of WECC if applicable law requires WECC to have a President. Each officer will be appointed by the Board and will serve for the term of office specified in the Board action appointing the officer and until his or her successor is appointed. Any two or more offices may be held by the same person except the offices of Chief Executive Officer and Secretary.

9.2 Chief Executive Officer Qualifications.

The Chief Executive Officer will be a person with senior management level experience and knowledge of bulk power electric transmission systems reliability, planning and operations.

9.3 Standards Applicable to All Employees.

A person may not be an officer or employee of WECC if: 1) the person is also the employee of or has a contractual relationship with any Entity, or any Affiliate of any Entity, that is eligible for membership in WECC; or 2) the person has a financial interest that, in the judgment of the Board or the Chief Executive Officer, creates the fact or appearance of bias, undue influence or lack of objectivity regarding any action or decision of WECC. The Board will adopt Standards of Conduct for officers and employees setting forth their duty of care, duty of loyalty, duty to avoid conflicts of interest and related matters intended to promote their neutrality, objectivity and professionalism. Upon adoption, such standards shall be attached hereto as Appendix B.

9.3.1 Exemptions from the disqualification criteria found in Section 9.3 are as follows:

9.3.1.1 Status as a residential electricity customer will not disqualify a person from employment with WECC.

9.3.1.2 A candidate for Chief Executive Officer or employee of WECC will not be disqualified for owning shares in a mutual fund because the mutual fund owns an interest in a Member or an Affiliate of a Member.

9.3.1.3 The disqualification standards described in Section 9.3 will not apply to disqualify a candidate who is receiving payments from a pension plan of a Member or an Affiliate of a Member in a form other than securities of such Member or Affiliate if the pension plan payments bear no relationship to the economic performance of the Member or Affiliate.

9.3.2 If an officer or employee receives a gift or inheritance of securities in any Member or Affiliate, he/she must resign or dispose of such securities within six (6) months of the date of receipt. Within six (6) months of the time a new

Member is added in which an officer or employee owns securities, the officer or employee will resign or dispose of those securities.

9.4 Employment.

The Chief Executive Officer will be employed by the Board of Directors and will serve at the Board's pleasure. Any contract of employment with a Chief Executive Officer will permit the Board to dismiss the officer with or without cause.

9.5 Chief Executive Officer's Duties.

Subject to the Board's direction, the Chief Executive Officer or his/her designees will have the following duties, among others:

9.5.1 Execute policies at the direction of the Board and be responsible to the Board for the performance of the WECC functions described in Section 2;

9.5.2 Hire and fire staff within the constraints of the annual budget;

9.5.3 Perform administrative duties, such as preparing annual budgets for the approval of the Board, making employment decisions and ensuring conformance with regulatory requirements;

9.5.4 Develop and implement employment policies and standards of conduct; and

9.5.5 Accept or reject membership applications in accordance with the criteria of these Bylaws.

9.6 Secretary's Duties.

9.6.1 Maintain Member and Affiliates Lists. The Secretary will maintain continuously updated lists of all Members and Affiliates.

9.6.2 Maintain Official Records. The Secretary will keep minutes of all WECC Board and Member meetings and will receive and maintain minutes of committee meetings and all other official records of WECC. Within five (5) business days after any vote taken by Members, the Board, a Class or any committee, the Secretary will provide notice to all Members and Participating Stakeholders (if applicable) of the results of such a vote through postings on the website, email and/or other means of communication.

9.6.3 Maintain Website. The Secretary will oversee the creation, maintenance, and updating of the WECC's website and the information published through it.

10. Dispute Resolution.

Except as may be otherwise provided herein, and subject to the conditions set forth in Appendix C, Section A.1, disputes between Members and/or WECC will be resolved pursuant to the WECC Dispute Resolution Procedures set forth in Appendix C. Matters subject to the

jurisdiction of the WECC Compliance Hearing Body are not subject to the procedures in Appendix C.

11. Costs and Finances.

11.1 Funding of Reliability Activities.

11.1.1 U.S. Statutory Funding. WECC shall fund all activities undertaken pursuant to Section 215 of the Federal Power Act in accordance with the funding provisions and procedures of that law and related FERC regulations and orders. The Board shall approve a budget for such activities in time for submission to the ERO and to the FERC for approval of such funding in accordance with applicable requirements.

11.1.2 International Funding. WECC shall fund reliability activities undertaken in accordance with any agreements it enters into with Canadian or Mexican Entities. Specifically:

(a) Subject to (b), in the event that a Canadian or Mexican Entity seeks membership in the WECC, that Entity may elect to negotiate an agreement with WECC that provides the terms upon which that Entity will become a Member and, among other things, participate in and/or fund WECC. In such a case and unless agreed otherwise, the Canadian or Mexican Entity shall not be a Member of WECC and shall not have an obligation to fund activities undertaken by the WECC until the terms of such agreement are executed.

(b) Section 11.1.2(a) shall not apply to any Canadian or Mexican Entity that is a Member as of the date of the approval of these WECC Bylaws. Existing Canadian or Mexican Members shall continue as Members in accordance with the terms and conditions of their membership as of the date of the approval of the WECC Bylaws, including the terms and conditions of any agreements in place as of the date of the approval of these WECC Bylaws. Nothing in the Section precludes existing Canadian or Mexican Members from negotiating an agreement with WECC that modifies the terms of its participation in and funding of WECC at any time.

11.1.3 Equitable Allocation of Funding. In adopting budgets for the costs of reliability activities, the Board shall endeavor to achieve an equitable allocation as between funding through Sections 11.1.1 and 11.1.2 based upon the net energy to load and other relevant factors consistent with applicable law, the Delegation Agreement and any International Reliability Agreements.

11.2 Dues.

The Board may require Members and Participating Stakeholders to pay nominal annual dues consistent with applicable FERC requirements (or those of International Reliability Agreements as applicable) to cover reasonable costs of membership and/or participation

in standards development that are not funded through Sections 11.1.1 or 11.1.2. Initial dues of a Member or Participating Stakeholder will be submitted with a completed application for membership or Participating Stakeholder status and will be for the prorated share of the full annual amount based on the Member's or Participating Stakeholder's actual months of membership or participation in the calendar year. In determining nominal dues, the Board may consider all relevant factors including, but not limited to, the ability of different classes of membership or Participating Stakeholders to pay such dues. The Board may also reduce, defer or eliminate the dues obligation of an individual Member or Participating Stakeholder for good cause shown.

11.3 Funding of Non-Statutory Activities.

To the extent that WECC elects to fund any activities not eligible for funding pursuant to Sections 11.1.1 and 11.1.2, it shall do so through the use of service fees, charges or dues applicable to the persons or entities that voluntarily participate in such activities. Participation in or funding of such activities shall not be a condition of membership in WECC.

12. Amendments to these Bylaws.

These Bylaws may be amended by either the Board or by the Members in accordance with the following procedures.

12.1 Amendment by the Board.

Except for those provisions described below, the Board may approve an amendment of the Bylaws after providing not less than thirty (30) days' notice of the proposed amendment to all Members. Approval of such an amendment requires the affirmative votes of not less than two-thirds (2/3) of the Directors in office. Such amendment will become effective sixty (60) days after its approval by the Board (1) unless the vote is appealed to the Members prior to the sixtieth day, or (2) subsequent regulatory approval is required. A Member appeal shall be sufficient to hold implementation of an amendment if a majority of any Class files a petition with the Secretary seeking appeal of such amendment. If such an appeal is received, the membership will vote on whether to rescind the Board approved amendment at the next Annual Meeting unless the Board calls a special meeting of the Members beforehand. An appeal will only be successful if a majority of all Members and a majority (three of five) of Member Classes vote to rescind the amendment. If the appeal vote is not successful, then the amendment will be deemed approved as of the day of the failed Membership vote. If subsequent regulatory approval is required for the amendment, then the amendment shall be effective upon the effective date of such approval.

12.1.1 Notwithstanding the foregoing, both Board and Member approval is required to amend provisions of these Bylaws concerning Sections 1.1 and 1.2; Section 4.2; Sections 6.2 through 6.8, inclusive; Section 7.2; Section 10; Sections 12.1 through 12.4, inclusive; Appendix C, and any other sections as may be required by Utah law. In such case, the Board shall first vote on the proposed amendment. If approved by the Board by the majority specified in Section 12.1 necessary to attain Board approval, the amendment must then be noticed to Members at least sixty (60) days prior to the Annual Meeting or a Special Member Meeting at

which the Member vote will occur. The amendment will then be approved if approved by two thirds (2/3) or more of the Members who vote upon such amendment.

12.2 Amendment by the Members.

Upon petition filed with the Secretary by any Member or Director, at any Annual Meeting the Members may amend any provision of these Bylaws; provided: 1) the proposed amendment has first been presented to the Board and not adopted (this provision will not apply to amendments which the Board is prohibited from adopting); 2) Members have received not less than sixty (60) days' notice of the proposed amendment, the reasons there for and a statement of the Board's position regarding it; and 3) the amendment receives the affirmative votes of not less than two-thirds (2/3) of all Members and a majority of Member Classes.

12.3 Amendments in Response to Mandatory Membership.

If at any time, pursuant to legislation or otherwise, membership becomes mandatory for some or all Members, upon the request of the affected Member(s) the Board will consider amendments to these Bylaws appropriate to such mandatory membership.

12.4 Amendments proposed by FERC.

FERC, upon its own motion or upon complaint, may propose an amendment to these Bylaws pursuant to 18 C.F.R. § 39.10(b).

13. Termination of Organization.

WECC may be terminated upon a vote of a majority of the Members in accordance with the provisions of Utah law, the Federal Power Act and the requirements of the Delegation Agreement and applicable International Reliability Agreements. Immediately upon such a vote, the Board will, after paying all debts of WECC, distribute any remaining assets in accordance with the requirements of Utah law, the Internal Revenue Code and these Bylaws.

14. Miscellaneous Provisions.

14.1 Limitation on Liability.

It is the express intent, understanding and agreement of the Members that the remedies for nonperformance expressly included in Section 4.8 hereof shall be the sole and exclusive remedies available hereunder for any nonperformance of obligations under these Bylaws. Subject to any applicable state or federal law which may specifically limit a Member's ability to limit its liability, no Member, its directors, members of its governing bodies, officers or employees shall be liable to any other Member or Members or to third parties for any loss or damage to property, loss of earnings or revenues, personal injury, or any other direct, indirect, or consequential damages or injury which may occur or result from the performance or nonperformance of these Bylaws, including any negligence, gross negligence, or willful misconduct arising hereunder. This Section 14.1 of these Bylaws applies to such liability as might arise between Members under these Bylaws. This Section 14.1 does not apply to parties to the Agreement Limiting Liability Among Western Interconnected Systems ("WIS Agreement") with respect to matters covered by the WIS Agreement and does not apply to any liability provision in any other agreement.

14.2 Indemnification.

WECC shall indemnify and hold harmless its Directors, officers, employees, agents and advisors against any and all damages, losses, fines, costs and expenses (including attorneys' fees and disbursements), resulting from or relating to, in any way, any claim, action, proceeding or investigation, instituted or threatened, arising out of or in any way relating to any action taken or omitted to have been taken (or alleged to have been taken or omitted to have been taken) by such person in connection with actions on behalf of WECC, and against any and all damages, losses, fines, costs and expenses (including attorneys' fees and disbursements) incurred in connection with any settlement of any such claim, action, proceeding or investigation unless such action of such person is determined to constitute fraud, gross negligence, bad faith or willful misconduct with respect to the matter or matters as to which indemnity is sought.

14.3 No Third Party Beneficiaries.

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

14.4 Informal Inquiries for Information.

Nothing in these Bylaws shall preclude: 1) a Member from making an informal inquiry for information outside of the procedures outlined in Section 4.6.11 hereof to another Member and 2) that other Member from responding voluntarily to that informal inquiry, provided, however, that any such response to an informal inquiry for information shall not be binding upon that other Member and shall be used by the Member making the informal inquiry for informational purposes only.

15. Incorporation.

WECC shall organize itself as a non-profit corporation pursuant to the laws of the state of Utah regarding non-profit corporations under the name "Western Electricity Coordinating Council." All Members agree to take no actions that would contravene the ability of WECC to maintain its status as a non-profit corporation existing pursuant to the Utah Act. The Board shall adopt these Bylaws as the Bylaws of WECC as a non-profit corporation.

WECC is intended to qualify as an organization described in Section 501(c)(4) of the Internal Revenue Code. No part of any net earnings of WECC shall inure to the benefit of any Member or individual. Upon liquidation, to the extent consistent with the Internal Revenue Code and Utah law, any monies remaining from assessments paid by Members for the costs of WECC shall be rebated to Members in proportion to their payments. Any remaining assets of WECC shall be transferred to another organization exempt from tax under Section 501(a) of the Internal Revenue Code, or government agency, promoting the same purposes as WECC, as designated by the Board.

16. Governing Law.

Unless otherwise agreed, if any conflict of law arises under these Bylaws among the Members, the laws of the United States of America shall govern, as applicable. The venue for any legal

action initiated under these Bylaws shall be the city and state (or province) in which the headquarters of WECC is located.

17. WECC Transition

The provisions of this Section shall apply to that period of time and activities associated with the transition of WECC from a hybrid Board of Directors to an independent Board of Directors with a Member Advisory Committee.

17.1 Board of Directors transition.

17.1.1 The transition of WECC governance from a hybrid Board to an independent Board of Directors will be effective upon the effective date of Federal Energy Regulatory Commission approval of Section 6.1 establishing an independent Board ("Effective Date"). The non-affiliated directors of WECC, whose terms extend past the Effective Date, so willing to continue to serve, shall form part of the initial cadre of independent Directors. These continuing Directors shall be entitled to serve the remainder of their respective three-year terms of office.

17.2 Transition Exceptions

The nomination, election and term of additional independent Directors shall be in conformance with the requirements of these bylaws, as amended, except:

17.2.1 The requirement that the Nominating Committee notify the Board Chair of the committee's nominations sixty (60) days prior to an Annual Meeting shall not apply.

17.2.2 Appointments of Member Advisory Committee members to the Nominating Committee shall be made such that no one class can occupy more than one seat at a time and cannot have a representative on the committee more than two years in a row.

17.2.3 Director positions of non-affiliated directors of WECC, whose terms extend beyond the Effective Date, but whose directors resign or indicate they will resign prior to the Effective Date, will be filled through the same nomination and election process used to select additional independent directors as provided above.

17.2.4 Those Directors first elected as a result of this transition from a hybrid to an independent Board will draw lots to determine their term length determined to achieve the staggered terms required by Section 6.3.

17.2.5 The nomination and election of a number of additional Directors needed to seat the entire Independent Board as described in section 6.4 as of the Effective Date may occur prior to the Effective Date. While the nomination and election of an individual to a director position may occur prior to the Effective Date, such nomination and election shall have the full force and effect of these bylaws after the Effective Date.

17.3 Member Advisory Committee transition

17.3.1 Initial Formation. When there is a meeting where Members vote to amend the WECC bylaws to provide for a Member Advisory Committee (MAC), the MAC will initially be constituted through elections conducted in conjunction with the same meeting.

17.3.2 Election of the initial MAC member representatives shall be as provided in these bylaws, as amended, except:

17.3.3 Where what had been the Class Seven membership category is combined with the Class Three membership category, Class Seven Members will indicate, prior to the meeting, whether they intend to continue participation in WECC as a member of the newly combined Class Three category. Entities so indicating will be considered members of Class Three for purposes of the initial formation of the MAC and shall be entitled to participate in elections for Class Three member representatives of the MAC.

17.3.4 Member Classes will not be allowed to subdivide into subclasses for purposes of electing class representative MAC members at the meeting where the MAC is initially formed and where initial MAC member elections are conducted.

17.3.5 The terms of each Class' three (3) initial Class representative members on the MAC shall be allocated, by the drawing of lots, such that the intended staggered terms for MAC members will be obtained, with one of a Class' initial MAC member representatives serving an initial term of one year, another two years, and another three years.

APPENDICES

A. Board Member Standards of Conduct

B. Officers and Employees Standards of Conduct

C. WECC Dispute Resolution Procedures

Appendix A
Standards of Conduct for
Members of the WECC Board of Directors

By accepting appointment to the Board of Directors (the "Board") of the Western Electricity Coordinating Council ("WECC"), a Director agrees to abide by the duties required of corporate directors and trustees. Utah law (and similar law in other states) imposes quasi-fiduciary duties of care and loyalty on all corporate directors or trustees, including directors and trustees of nonprofit corporations. For as long as he or she remains a member of the Board of Directors of WECC, a Director will abide by the following standards of conduct.

I. Duty of care. The Directors of a corporation are bound to use due care and to be diligent in respect to the management and administration of the affairs of the corporation. This duty of care is generally thought to have two components: the time and attention devoted to corporate affairs and the skill and judgment reflected in business decisions.

A. Each Director will regularly attend Board of Directors meetings, digest the materials sent to him or her, participate in Board discussions and make independent inquiries as needed.

B. In voting on any matter before the Board or otherwise acting in his or her capacity as a Director, each Director will:

1. make reasonable inquiry to inform himself or herself of the nature and consequences of the matter or action at issue;

2. exercise, at a minimum, the degree of care, skill, and diligence that an ordinarily prudent business person would exercise under similar circumstances; and

3. act in a manner the Director, in the exercise of his or her independent judgment, believes to be in the best interests of WECC and the membership of WECC, taken as a whole.

C. In exercising the duty of care described in paragraphs IA and B above, a Director has the right to rely on statements by the persons immediately in charge of business areas of WECC, to rely on professionals and experts (such as engineers, accountants and lawyers) and to rely on committees of WECC, unless facts or circumstances appear which would prompt further concerns of the ordinarily prudent person.

II. Duty of loyalty. The duty of loyalty imposes on a Director the obligation to remain loyal to WECC, acting at all times in the best interests of WECC and its Members as a whole and unhampered by any personal pecuniary gain. This duty does not preclude a Director from being employed in a competing or related business so long as the Director acts in good faith and does not interfere with the business of WECC.

A. Each Director will carry out his or her duties as a Director in good faith.

B. Each Director will refrain from using any influence, access, or information gained through his or her service as a Director to confer any improper personal benefit (financial or otherwise) upon himself or herself, any family member, or any person living in the Director's household.

C. Each Director will refrain from using any influence, access, or information gained through his or her service as a Director to confer an improper benefit (financial or otherwise) on any organization:

1. for which the Director serves as an officer, director, employee, consultant, or in any other compensated or management position; or

2. in which the Director or any family member or person living in the Director's household has a material financial interest (whether as a shareholder, partner, or otherwise).

D. To the extent permitted by law, each Director will maintain the confidentiality of:

1. any confidential or proprietary information of WECC disclosed or available to the Director;

2. any confidential or proprietary information of WECC Member(s) to which the Director has access by virtue of his or her status as Director; and

3. any confidential or proprietary information of third parties that has been provided to WECC or the Board on condition of confidentiality.

E. Conflicts of Interest. Because conflicts of interest may arise from time to time, specific guidelines are provided. In general, conflicts of interest involving a Director are not inherently illegal nor are they to be regarded as a reflection on the integrity of the Board or of the Director. It is the manner in which the Director and the Board deal with a disclosed conflict that determines the propriety of the transaction.

Directors of nonprofit corporations may have interests in conflict with those of the corporation. The duty of loyalty requires that a Director be conscious of the potential for such conflicts and act with candor and care in dealing with these situations.

The following are guidelines for Directors with actual or potential conflicts of interest:

1. Each Director has a responsibility to recognize potential conflicts of interest and to be guided when acting as a Director by his or her independent judgment of what is in the best interests of WECC and the membership of WECC, taken as a whole. If any Director has questions about whether a conflict of interest exists, he or she may make inquiry to the Chief Executive Officer of WECC for advice.

2. Potential conflicts of interest may arise because of a Director's private, individual interests (personal conflicts of interest) or because of relationships the Director may have with other organizations or interest groups (organizational conflicts of interest). Current or past employment or other compensation-based relationships with one or more WECC Members are examples of potential organizational conflicts of interest. Whether a potential conflict of interest is personal or organizational, in all cases involving WECC affairs a Director's conflicting interests are subordinate to those of WECC and the membership of WECC, taken as a whole.

3. Personal conflicts of interest.

   a. Personal conflicts of interest exist if a Director, a member of the Director's family, or a person sharing the Director's household: 1) has a material financial interest in a matter or transaction that comes before the Board for action; or 2) stands to receive a benefit (in money, property, or services) from a transaction involving WECC to which the person is not legally entitled.

   b. In cases of personal conflicts of interest, the affected Director's obligations are to:

      (1) disclose to the Board, before the Board acts with respect to that matter, the material facts concerning the Director's personal conflict of interest; and

      (2) refrain from voting, and from attempting to influence the vote of any other Director(s), in those matters in which the Director has a personal conflict of interest.

4. Organizational conflicts of interest.

   a. An organization has a "direct" conflict of interest if a decision by the Board would confer material benefits on that organization that other WECC Members would not share, or impose material detriments or costs on that organization that other WECC Members would not share. The fact that many if not all Members are affected to some extent by Board decisions on core issues such as standards, new transmission lines and their ratings, does not create or constitute a "direct" conflict of interest.

   b. It is not a "direct" conflict of interest for a Director to be associated with an organization or an interest group that may stand to benefit from decisions made or actions taken by the Board, so long as the Director does not attempt to use his or her position as a Director to confer special

benefits on associated organizations or interest groups when other WECC Members would not share in those benefits.

c. In cases of potential "direct" organizational conflicts of interest, the affected Director's obligations are to:

(1) disclose to the Board, before the Board acts with respect to the matter, the material facts concerning the organizational conflict of interest; and

(2) refrain from voting and from attempting to influence the vote of any other Director(s) with respect to the proposed action or decision.

Appendix B
Officers and Employee
Standards of Conduct

By accepting employment with the Western Electricity Coordinating Council ("WECC"), an Employee agrees to abide by these Standards of Conduct. For the purpose of these Standards, an Employee includes each and all officers, employees and substantially full-time consultants and contractors of WECC.

I. Duty of care. The Employees of WECC are bound to use due care and to be diligent in respect to the management and administration of the affairs of the corporation. This duty of care is generally thought to have two components: the time and attention devoted to corporate affairs and the skill and judgment reflected in business decisions.

Employees shall not have any outside employment that limits in any way their ability to fulfill their employment responsibilities to WECC. If an Employee has any question about whether outside employment is consistent with this standard, they should consult with their supervisor.

II. Duty of loyalty. The duty of loyalty imposes on an Employee the obligation to remain loyal to the WECC, acting at all times in the best interests of WECC and its Members as a whole and unhampered by any personal pecuniary gain. WECC expects all Employees to avoid adversely affecting the public's confidence in the integrity and reputation of WECC. Any conduct or activities of any Employee should be capable of being justified and withstanding public scrutiny.

A. Each Employee will carry out his or her duties as an Employee in good faith, with integrity and in a manner consistent with these Standards and all applicable laws governing WECC.

B. Each Employee will refrain from using, or creating the appearance of using, any influence, access, or information gained through his or her service as an Employee to confer any improper personal benefit (financial or otherwise) upon himself or herself, or Family Member.[1] Employees shall not accept gifts or entertainment that would tend to affect, or give the appearance of affecting, the performance of their duties; provided, however, that Employees may accept de minimus food or entertainment or non-cash gifts received as part of a social or special occasion in amounts not to exceed $1000 per source per year.

C. Each Employee will refrain from using, or creating the appearance of using, any influence, access, funds or information gained through his or her service as an Employee to confer an improper benefit (financial or otherwise) on any organization. The obligation to avoid the appearance of impropriety shall apply in particular to any organization:

1 For purposes of these Standards, a Family Member includes a spouse, domestic partner, child of the Employee, or a relative living in the same home as the Employee.

1. for which the Employee is serving or has in the past served as an officer, director, employee, consultant, or in any other compensated or management position; or

2. in which the Employee, or Family Member has a material financial interest known to the Employee (whether as a shareholder, partner, or otherwise).

D. Employees shall not use their WECC position, WECC funds or WECC resources to support any political party, candidate or proposition except as expressly authorized by the Board.

E. To the extent permitted by law, each Employee shall maintain the confidentiality of:

1. any confidential or proprietary information of WECC disclosed or available to the Employee;

2. any confidential or proprietary information of WECC Member(s) to which the Employee has access by virtue of his or her status as Employee; and

3. any confidential or proprietary information of third parties that has been provided to WECC or the Board on condition of confidentiality.

F. Conflicts of Interest. The following conflicts of interest policy shall apply to all WECC Employees. Conflicts of interest may arise from time to time. In general, conflicts of interest involving an Employee are not inherently illegal, nor are they to be regarded as a reflection on the integrity of WECC or of the Employee. It is the manner in which the Employee and WECC deal with a disclosed conflict that determines the propriety of the transaction. The following are guidelines for Employees with actual or potential conflicts of interest:

1. In general, personal conflicts of interest exist if an Employee, or a Family Member, has a material financial interest in a matter or transaction that comes before WECC for action, or stands to receive a benefit (in money, property, or services) from a transaction involving WECC to which the person is not legally entitled. For purposes of determining whether stock constitutes a material financial interest, see Paragraph F(6) below.

2. Organizational conflicts of interest exist if an Employee, or a Family Member, has a relationship with an organization or interest group that would cause a reasonable person to believe such Employee's judgment, loyalty, or objectivity might be influenced in a way that is adverse to the interests of WECC.

3. Where there is any question about potential conflicts of interest, the Employee shall disclose to the Chief Executive Officer as soon as possible and prior to when WECC takes action with respect to that matter, the material facts concerning the Employee's personal conflict of interest, and refrain from participating in, or from

attempting to influence the action of any Directors or Employee(s) of WECC regarding those matters in which the Employee has a conflict of interest.

4. No Employee may be an employee, director of, or consultant to or provide services to or be associated in any way with any WECC Member without full disclosure to, and written consent of, the Chief Executive Officer. To the extent that an Employee becomes aware that a Family Member is or will in the future be engaged in activity described in this Paragraph F(4), the Employee shall promptly notify the Chief Executive Officer, who shall review all the material facts and determine whether they constitute a conflict of interest pursuant to Paragraphs F(1) and F(2), above.

5. No Employee shall participate in any electric energy transaction other than for ordinary personal use except to the extent necessary to, and consistent with, the functions of WECC. Participation in an energy transaction includes, but is not limited to, purchasing, selling, marketing, or brokering of electricity, ancillary services, electricity transmission or electricity distribution. To the extent that an Employee becomes aware that a Family Member is or will in the future be engaged in activity described in this Paragraph F(5), the Employee shall promptly notify the Chief Executive Officer who shall review all the material facts and determine whether they constitute a conflict of interest pursuant to Paragraphs F(1) and F(2), above.

6. All Employees shall promptly disclose to the CEO and the Chair of the Board any direct or indirect financial interest in excess of $5,000 (including the direct or indirect ownership of securities) held by the Employee or a Family Member living with the Employee[2] in any Electric Line of Business entity as defined in Section 3.15 of the Bylaws doing business in the Western Interconnection. Upon such disclosure, the CEO and the Chair of the Board shall determine whether such financial interest constitutes a conflict of interest, or the appearance thereof, in light of the duties of the Employee, the ability to divest such financial interest without undue hardship and the totality of the circumstances. In response to such disclosure, the CEO and the Chair may impose such remedies as are reasonable under the circumstances and consistent with section 9.3 of the Bylaws. Such remedies may include, but are not limited to, restrictions on the Employee's duties or involvement in certain matters, transfer of the Employee to another position, broader disclosure of the financial interest, voluntary or mandatory divestiture of the interest (in whole or in part) or other remedies. Pursuant to section 9.3.2 of the Bylaws, if an Employee (not a Family Member) receives a gift or inheritance of securities of a Member of WECC, or if a new Member joins WECC in which the

2 Nothing in this section shall require an Employee to investigate the financial interests of Family Members not living with the Employee. However, to the extent known to the Employee, the financial interests of a Family Member not living with the Employee may create a potential conflict of interest (or appearance thereof) subject to Sections II(B) and/or II(F)(1) of these standards, in which case disclosure pursuant to Section II(F)(3) is appropriate.

Employee (not a Family Member) holds securities, the Employee must resign or divest such securities within six months thereafter. For the purposes of this section, none of the following shall constitute a direct or indirect financial interest:

a. An interest that exists through diversified mutual funds;

b. An interest that exists for six months following receipt of a gift or inheritance of securities of a Market Participant or acceptance of employment with WECC, whichever is later (provided that employees of the WSCC shall have two years from WECC organizational meeting to divest securities in their possession as of that date);

c. An interest that exists through a pre-existing participation in a qualified defined benefits pension plan or health benefits plan of a Market Participant so long as the benefits under such plan do not vary with the economic performance or value of the securities of such Market Participant.

Appendix C

WECC Dispute Resolution Procedures

C. DISPUTE RESOLUTION.

C.1 Obligation To Comply with Dispute Resolution Procedures. If any dispute concerning one or more issues identified in Section C.2 below arises between a Member and one or more other Members, or between one or more Members and WECC, all of the parties to the dispute shall, to the extent permitted by law, be obligated to comply with the dispute resolution procedures specified in these Bylaws (except to the extent all of the parties to the dispute may agree otherwise as provided in Section C.4 below). Only Members and WECC have the right to invoke the provisions of this Appendix C and, except where all affected parties have separately agreed otherwise with respect to a particular dispute, only Members and WECC are obligated to carry out the dispute resolution procedures set forth herein. Any dispute subject to the provisions of this Appendix C to which WECC is made a party shall be subject to the additional requirements specified in Section C.3 below if the dispute is initiated by a party other than WECC. To the extent permitted by law (and except as otherwise permitted by the provisions of Section C.6.3), no party to a dispute subject to the provisions of this Appendix C may pursue any other available remedy with respect to the dispute until all of the parties to the dispute have fully complied with the dispute resolution procedures specified herein, *provided, however,* that if any party to a dispute subject to the provisions of this Appendix C refuses to comply with the dispute resolution procedures specified herein, all other parties to the dispute shall subsequently be relieved of any further obligation to comply with these dispute resolution procedures before pursuing other remedies in connection with that dispute.

C.2 Issues Subject to Dispute Resolution Procedures. Any dispute between or among the parties identified in Section C.1 above (that the parties to the dispute do not resolve through negotiations between or among themselves) shall be subject to the dispute resolution procedures set forth in this Appendix C if the dispute concerns: (i) the application, implementation, interpretation, or fulfillment of any guidelines, criteria, policies, procedures, or Bylaws of WECC or the North American Electric Reliability Council (or any successor organization); or (ii) any matter specified in Section C.6.2 below; except that any matter that is subject to the jurisdiction of the WECC Compliance Hearing Body is not subject to the requirements of this Appendix C. Notwithstanding the foregoing provisions of this Section C.2, however, neither WECC nor any Member shall be obligated to comply with the dispute resolution procedures of these Bylaws if: (a) the dispute is between two or more Members (or WECC), all of which, at the time of the dispute, are parties to the WECC Reliability Management System Agreement and the matter is within the scope of the dispute resolution procedures set forth in that agreement; or (b) the dispute is between two or more Members, all of which, at the time of the dispute, are parties to a separate agreement or treaty or where an applicable tariff, rate schedule, or other legal obligation of one of the parties provides for the parties to resolve the dispute in a manner other than in accordance with the provisions of this Appendix C of the Bylaws.

C.3 Limitations on Members' Rights To Make WECC a Party to a Dispute. In addition to the other provisions of this Appendix C of the Bylaws, any dispute (other than a dispute initiated by WECC) to which WECC is made a party shall be subject to the limitations set forth in Sections C.3.1 and C.3.2 below.

C.3.1 Bases for Using Dispute Resolution Procedures To Challenge WECC Action. Subject to any limitation set forth in these Bylaws or in applicable statute, regulation or FERC order, one or more Members may use the dispute resolution procedures specified in this Appendix C to challenge any final action of WECC only on one or more of the following bases: (i) the action is contrary to applicable law or regulation; (ii) the action is contrary to WECC's Articles of Incorporation or these Bylaws (including WECC's purposes as set forth in those documents); (iii) the action was taken in violation of applicable procedures of WECC governing that action; or (iv) the action encompasses a decision in which there was plain error material to the decision. For purposes of this Appendix C, action taken by WECC shall be deemed final if: (a) the action has been taken or adopted or approved or accepted by WECC's Board of Directors (other than by a motion specifically providing that the action is conditional or will have temporary application not to exceed six months); (b) all conditions specified to make any conditional action of WECC's Board of Directors effective have been fulfilled; or (c) the action has been taken or adopted or approved or accepted by a committee, subcommittee, task force, or other group or person acting under authority of WECC without any provision making the action subject to further approval or adoption or acceptance by the Board of Directors. Nothing contained in this Appendix C shall limit any rights any Member (or any other party) may have under applicable law or regulation to initiate or participate in an administrative or legal action to which WECC is made a party in accordance with applicable provisions of law or regulation.

C.3.2 Obligation to Bear WECC's Share of Facilitator Costs. If one or more Members initiate a dispute under this Appendix C to challenge an action of WECC, the Member(s) initiating the challenge shall be obligated to bear all of the costs of facilitators' services incurred to comply with the requirement of Section C.5 below, except to the extent WECC agrees to pay a share of the costs of facilitators' services.

C.4 Ability to Modify Dispute Resolution Procedures by Agreement. Any provision of the dispute resolution procedures set forth in this Appendix C may be modified, waived, or omitted by agreement of all of the parties to the dispute. Parties to a dispute subject to these provisions are obligated to comply with its procedures unless all of the parties to the dispute agree to do otherwise. The manner in which the dispute resolution procedures set forth in this Appendix C may be varied include (by way of example and not as limitation): the manner of selecting a facilitator or arbitrator; the procedures or time lines to be followed during mediation or arbitration; the grounds or forum or right to appeal an arbitrator's decision; the manner of allocating fees and costs associated with the dispute; whether the parties are obligated to proceed to arbitration if the dispute is not resolved through mediation; and whether a decision rendered through arbitration is binding on the parties. In addition, any dispute that does not fall within the scope specified in Section C.2 above may be resolved according to the procedures set forth in Appendix C of these Bylaws if all of the parties to the dispute agree to do so.

C.5 Mediation.

C.5.1 Notice to Other Parties and WECC's Chief Executive Officer. To initiate the dispute resolution process with respect to a dispute governed by the provisions of

this Appendix C, the Member or WECC that has elected to initiate the dispute shall deliver to all other parties to the dispute and to WECC's Chief Executive Officer (whether or not WECC is a party to the dispute) written notice invoking the dispute resolution procedures set forth in this Appendix C (a "Dispute Notice").

C.5.1.1 The Dispute Notice shall: (i) include a brief, general description of the matter(s) in dispute; (ii) include a complete list of all other Members the party submitting the Dispute Notice intends to make a party to the dispute; and (iii) state whether or not WECC is to be made a party to the dispute.

C.5.1.2 Within five business days of receiving a Dispute Notice, any party to the dispute may elect to deliver a brief supplemental description of the dispute to WECC's Chief Executive Officer.

C.5.1.3 Within 10 business days of receiving an initial Dispute Notice, WECC's Chief Executive Officer shall: (a) publish (or cause to be published) in WECC's newsletter or on its electronic bulletin board a notice containing a list of the parties to the dispute and a summary of the descriptions of the matter(s) in dispute provided by the parties to the dispute; and (b) deliver to each party to the dispute a copy of WECC's then-current standing list of qualified facilitators, knowledgeable in the matters addressed by WECC (as approved by the Board of Directors).

C.5.1.4 No person may be listed on WECC's standing list of qualified facilitators unless the person has agreed to: (i) disclose, at any time the

person is selected to serve as a facilitator under this Appendix C, any personal or financial interest the facilitator may have with respect to the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the facilitator's immediate family members); (ii) disclose any relationship the facilitator may have with any party to the dispute that is not permitted under Section C.5.2 below; and (iii) abide by all applicable provisions of these Bylaws, including restrictions on disclosure of matters discussed and information exchanged during mediation as provided in Section C.5.3 below.

C.5.2 Selection of a Facilitator. Within 10 calendar days after the delivery of a Dispute Notice, the parties to the dispute shall select a neutral facilitator by mutual agreement. If the parties to the dispute cannot agree on a facilitator within 10 calendar days after delivery of a Dispute Notice, the facilitator shall be selected from WECC's standing list of qualified facilitators as follows: The parties to the dispute shall take turns striking names from WECC's standing list of qualified facilitators until there is only one name remaining. (The parties to the dispute shall draw lots to determine the order in which they take turns striking names.) The last person whose name remains on the list shall serve as the facilitator. No facilitator other than a facilitator chosen by agreement of all the parties to the dispute may (i) have a personal or financial interest in the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the facilitator's immediate family

members); or (ii) be (or have an immediate family member who is) a past or present director, commissioner, officer, employee, consultant, agent, or other representative of any of the parties to the dispute. If the facilitator selected through the process of striking names specified above is disqualified under the preceding sentence, the facilitator whose name was stricken last shall serve in his or her place. In addition, if WECC is a party to a dispute initiated by one or more Members, turns striking names from the standing list of qualified facilitators shall alternate between WECC on the one hand and all other parties to the dispute on the other.

C.5.3 Mediation Process. The facilitator and representatives of all of the parties to the dispute shall meet within 14 calendar days after the facilitator has been selected and attempt in good faith to negotiate a resolution to the dispute. Each party's representative designated to participate in the mediation process must have the authority to settle the dispute (or, at a minimum, be authorized to negotiate on behalf of the party and make recommendations with respect to settlement of the dispute if final authority to approve a settlement is reserved to a party's board, executive committee, commission, or other governing body). At the parties' initial meeting with the facilitator, the facilitator shall, after soliciting input from the parties to the dispute, set the schedule for further meetings among the parties to the dispute (subject to the 60-day maximum mediation period specified in Section C.5.6 below). The parties to the dispute shall comply with the schedule set by the facilitator and attempt in good faith at every meeting to negotiate a resolution to the dispute. To the extent permitted by law, neither the facilitator nor any party to the dispute may publicly disclose, rely on, or introduce as evidence in any subsequent arbitration, FERC proceeding, Canadian Regulatory

Authority proceeding, proceeding before a Mexican Regulatory Authority, appeal, or litigation concerning the same or any related dispute: (i) any views expressed or suggestions made by another party to the dispute with respect to a possible settlement of the dispute; (ii) admissions made by another party to the dispute in the course of the mediation proceedings; (iii) proposals made or views expressed by the facilitator; or (iv) the fact that another party to the dispute has or has not indicated willingness to accept a proposal for settlement made by the facilitator. In those cases in which a party to a dispute subject to the provisions of this Appendix C of the Bylaws is a membership organization (including WECC, if applicable), nothing in the preceding sentence shall prohibit that organization from reasonably communicating with its members and governing body to share general information about the dispute, such as the parties, status, disputed issues, and positions of each of the parties with respect to the disputed issues.

C.5.4 Referral for Resolution. With the consent of all parties to the dispute, a resolution may include referring the matter to a technical body (such as a technical advisory panel of WECC) for resolution or an advisory opinion, to arbitration, directly to FERC or, in a dispute involving a Canadian Member, directly to the appropriate Canadian Regulatory Authority, or, in a dispute involving a Mexican Member, directly to the appropriate Mexican Regulatory Authority.

C.5.5 Mediation Participation by WECC Staff When WECC Not a Party. If, during the course of mediation to which WECC is not a party, the facilitator or any party to the dispute wishes to solicit the views of WECC concerning the application, implementation, interpretation, or fulfillment of any guidelines, criteria, standards, policies, or procedures of WECC, the facilitator may request or permit the submission of WECC staff views only if: (i) any participation by WECC staff

takes place exclusively in the presence of all parties to the dispute; (ii) participating WECC staff members agree to be equally available upon request to all parties to the dispute; and (iii) participating WECC staff members agree to comply with the restrictions on disclosure contained in Section C.5.3.

C.5.6 Mediation Deemed at Impasse After 60 Days. If the parties to the dispute have met and negotiated in good faith in accordance with the schedule set by the facilitator but have not succeeded in negotiating a resolution of the dispute within 60 calendar days after the first meeting with the facilitator pursuant to Section C.5.3 above, the parties to the dispute shall be deemed to be at impasse and, except as otherwise provided in Section C.5.6.2 below, shall also be deemed to have fulfilled their obligations under Section C.1 of these Bylaws to fully comply with the dispute resolution provisions before pursuing any other available remedy. If any party participating in the mediation process is subject to a contractual or statutory limitations period with respect to the matter in dispute, and the limitations period will expire before the 60-day period for mediation under this Section C.5.6 is completed, then the parties shall be deemed at impasse on the seventh calendar day preceding the expiration of the shortest applicable limitations period.

C.5.6.1 Disputes Not Subject to Provisions of Section C.6.2. Unless the matter in dispute is subject to the provisions of Section C.6.2 below, at any time after the parties to the dispute are deemed at impasse, the dispute may be submitted to binding arbitration in accordance with the procedures set forth in Section C.7 of these Bylaws (but only by agreement of all of the parties to the dispute). If the matter in dispute is subject to the provisions of Section C.6.2 below, the parties' obligations with respect to submitting the matter to binding arbitration under Sections C.6 and C.7 of these Bylaws shall be as specified in Section C.5.6.2 below. In

all other cases, if the parties to the dispute do not agree to submit the dispute to binding arbitration in accordance with the procedures set forth in Section C.7 of these Bylaws, any party to the dispute may at any time thereafter pursue any other remedy available under regulation, law, or equity (subject to the restrictions on disclosure set forth in Section C.5.3 above).

C.5.6.2 Disputes Covered by Section C.6.2. If the parties to a dispute concerning a matter subject to the provisions of Section C.6.2 either: (i) are deemed at impasse after attempting to resolve the matter through mediation as provided in Sections C.5.1 through C.5.6 above; or (ii) have agreed to submit the matter directly to binding arbitration without attempting to resolve the matter through mediation as provided in Sections C.5.1 through C.5.6 above, the parties to the dispute shall submit the matter to binding arbitration in accordance with the procedures set forth in Sections C.6 and C.7 of these Bylaws.

C.5.7 Costs of Facilitator's Services. Except as otherwise provided under Section C.3.2, the costs of the facilitator's services shall be born equally by all parties to the dispute unless the parties to the dispute agree otherwise, but the parties also intend that the costs of mediation should be taken into account in any resolution proposed through the mediation process.

C.5.8 Notice to WECC of Completion of Mediation. Within 10 calendar days after either: (i) reaching a negotiated resolution through the mediation process set forth in Section C.5; or (ii) reaching deemed impasse in accordance with Section C.5.6 above, the parties to the dispute shall jointly deliver to WECC's Chief Executive Officer a written notice briefly describing the outcome of the mediation process. Promptly after receiving written notice describing the outcome of a mediation conducted in accordance with Section C.5, WECC's Chief Executive Officer shall

publish (or cause to be published) in WECC's newsletter or on its electronic bulletin board a brief description of the outcome of the mediation, together with a list of all of the parties to the dispute.

C.6 General Provisions Relating to Binding Arbitration.

C.6.1 Matters for Which Binding Arbitration is Elective. Except with respect to any dispute that concerns one or more matters specified in Section C.6.2 below, the binding arbitration procedures set forth in Section C.7 may be invoked only by agreement of all of the parties to the dispute to be arbitrated and are solely for the convenience of WECC and its Members. If a dispute governed by this Appendix C does not concern a matter specified in Section C.6.2 below, a party to the dispute shall be deemed to have fulfilled its obligations to comply with Appendix C of these Bylaws (irrespective of whether the parties to the dispute agree to proceed with binding arbitration) to the extent that either: (i) that party has fully performed the obligations set forth in Sections C.1 through C.5.8; or (ii) all of the parties to the dispute have agreed to a different process for resolving the dispute and the agreed-upon process has been fully carried out.

C.6.2 Matters for Which Binding Arbitration Is Obligatory. If a dispute is governed by Appendix C of these Bylaws and is not resolved through the process of mediation in accordance with Sections C.5.1 through C.5.6 above, the parties shall be obligated to submit the matter to binding arbitration in accordance with the procedures set forth in Section C.7 (subject to the limitations on the arbitrator's authority set forth in Section C.6.3 below) if the dispute concerns one or more of the following matters:

C.6.2.1 a decision of WECC's Board of Directors or a Committee of the Board acting on the recommendation of, or on a matter within the jurisdiction of, the Operating Transfer Capability Policy Group ("OTCPG") or successor;

C.6.2.2 a transmission path rating, or a modification to a transmission path rating, assigned to one or more transmission paths operated by a Member (or jointly operated by more than one Member);

C.6.2.3 transmission access, pursuant to Sections 10.1.2, 10.1.3, and 10.5; or

C.6.2.4 any matter that, by vote of both WECC's Board of Directors and WECC's Membership, is designated as a matter to be subject to the provisions of Section C.6.2 of these Bylaws, provided that any matter submitted to WECC's Membership pursuant to this provision must be approved by at least the number of votes required to amend these Bylaws under Section 13.2.

C.6.3 Limitations on Arbitrator's Authority with Respect to Matters Specified in Section C.6.2. Unless all of the parties to a dispute agree otherwise, an arbitrator rendering a decision with respect to any matter specified in Section C.6.2 above shall have no authority to consider or award remedies for past economic harm or damages of any kind, including without limitation actual or direct damages; indirect, consequential, or incidental damages; or exemplary or punitive damages. Nothing in this Section C.6.3 shall: (i) limit any rights that a party to a dispute concerning a matter specified in Section C.6.2 above may have to pursue legal claims for damages or other economic remedies after the arbitrator has rendered

his or her decision on that matter (within the scope of his or her authority under this Section C.6.3); or (ii) limit an arbitrator's authority under Section C.8 below to shift costs or impose monetary sanctions for "good cause" (as that term is defined in Section C.8).

C.6.4 Arbitration Decisions Not To Modify Underlying Rights and Obligations. Unless all of the parties to a dispute agree otherwise, the resolution through binding arbitration of any dispute governed by this Appendix C shall not have the effect of increasing, decreasing, or otherwise modifying WECC's or any Member's obligation to abide by, or ability to enforce or impose penalties or sanctions with respect to, any guidelines, criteria, standards, policies, procedures, decisions, or Bylaws of WECC or any limitation on the foregoing, whether established by law; regulation; judicial, executive, or administrative order, decree, or decision; tariff; contract; course of performance; treaty; or otherwise.

C.6.5 Laws Relating to Binding Arbitration. WECC and its Members recognize that some Members may be subject to laws (including without limitation United States federal or state laws, Canadian or provincial laws, or Mexican laws) that limit or define those Members' ability to agree in advance to be subject to binding arbitration. If a Member has the right or obligation under applicable law to refuse to submit to binding arbitration in connection with any dispute that would otherwise be subject to binding arbitration under Section C.6.2 of these Bylaws, that Member shall not be obligated to comply with the binding arbitration procedures set forth in Sections C.6 and C.7. Any Member subject to any law or other legally binding authority that may limit (or permit the Member to limit) its

obligation to comply with the provisions requiring binding arbitration under Sections C.6 and C.7 or to fully comply with a valid arbitrator's decision rendered in accordance with this Appendix C shall provide notice to this effect to all other disputing parties and WECC's Chief Executive Officer upon initiation of any dispute involving that Member if the dispute is subject to Section C.6.2. Upon receiving a notice under Section C.6.5, any other party to the dispute shall thereafter be relieved of any obligation to comply with the provisions Sections C.6 and C.7 in connection with that dispute, except to the extent that the Member giving notice agrees to be fully bound by procedures governing and results of any arbitration proceeding. If there are more than two parties to a dispute covered by the preceding sentence, however, then all parties to the dispute other than the party giving notice under Section C.6.5 shall make good faith efforts to establish a mutually acceptable approach for resolving among themselves whatever aspects of the dispute can reasonably be resolved through the procedures set forth in this Appendix C without the participation of the party giving notice under Section C.6.5. If any Member fails to submit to binding arbitration, or fails to abide by a valid arbitrator's decision rendered in accordance with this Appendix C, that Member shall thereafter have no right to enforce any of the provisions of Section C.6.2 (concerning obligations to submit specified disputes to binding arbitration) against any other Member or WECC until such time as the WECC Board of Directors, or a delegate designated by the Board, determines that it is appropriate to restore the Member's ability to enforce the provisions of Section C.6.2.

C.6.6 Consistency with Laws, Regulatory Jurisdiction and Orders, Etc. Nothing contained in this Appendix C and no arbitrator's decision rendered in accordance with Section C.7 shall be construed to require or shall otherwise operate to cause any Member or WECC to incur any obligation or take any action that is contrary to: (i) any applicable law or regulation; (ii) any applicable authority, order, decree, rule, or decision of a regulatory, judicial, administrative, executive, or other governmental body having jurisdiction over one or more of the matters or parties subject to this Appendix C or covered by an arbitrator's decision; or (iii) any applicable rate schedule, tariff, treaty, or valid, pre-existing contractual obligation with which any party subject to this Appendix C or covered by an arbitrator's decision is legally obligated to comply.

C.7 Arbitration Procedures.

C.7.1 Notice to WECC of Initiation of Binding Arbitration. Within 10 calendar days after all of the parties to a dispute have agreed (or become obligated under Section C.6.2 above) to submit the dispute to binding arbitration under Sections C.6 and C.7, the parties to the dispute shall deliver written notice to WECC's Chief Executive Officer (an "Arbitration Notice").

C.7.1.1 The Arbitration Notice shall: (i) include a brief, general description of the issues to be arbitrated; and (ii) identify all parties who have agreed (or become obligated) to submit the dispute to binding arbitration under Sections C.6 and C.7.

C.7.1.2 Within five business days of receiving an Arbitration Notice, WECC's Chief Executive Officer shall: (a) publish (or cause to be published) in

WECC's newsletter or on its electronic bulletin board a notice containing a list of the parties to the arbitration and the parties' brief, general description of the issues to be arbitrated; and (b) deliver to each party to the dispute a copy of WECC's then-current standing list of qualified arbitrators, knowledgeable in matters addressed by WECC (as approved by the Board of Directors).

C.7.1.3 No person may be listed on WECC's standing list of qualified arbitrators unless the person has agreed to: (a) disclose, at any time the person is selected to serve as a arbitrator under this Appendix C, any personal or financial interest the arbitrator may have with respect to the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the arbitrator's immediate family members); (b) disclose any relationship the arbitrator may have with any party to the dispute that is not permitted under Section C.7.2 below; (c) assemble a complete record of the arbitration process and the materials received as evidence by the arbitrator if any of the parties to the dispute elect to appeal or contest the arbitrator's decision; and (d) abide by all applicable provisions of and procedures specified by Sections C.6 and C.7.

C.7.2 Selection of an Arbitrator. Within 10 calendar days after all of the parties to a dispute have agreed (or become obligated) to submit the dispute to binding arbitration under Sections C.6 and C.7, the parties to the dispute shall select an arbitrator by mutual agreement. If the parties cannot agree on an arbitrator within

10 calendar days after agreeing to arbitrate their dispute, the arbitrator shall be selected from WECC's standing list of qualified arbitrators as follows: The parties to the dispute shall take turns striking names from WECC's standing list of qualified arbitrators until there is only one name remaining. (The parties to the dispute shall draw lots to determine the order in which they take turns striking names.) The last person whose name remains on the list shall serve as the arbitrator. No arbitrator other than an arbitrator chosen by agreement of all the parties to the dispute may (i) have a personal or financial interest in the matter(s) in dispute (including any indirect personal or financial interest that could arise because of interests or relationships affecting any of the arbitrator's immediate family members); or (ii) be (or have an immediate family member who is) a past or present director, commissioner, officer, employee, consultant, agent, or other representative of any of the parties to the dispute. If the arbitrator selected through the process of striking names specified above is disqualified under the preceding sentence, the arbitrator whose name was stricken last shall serve in his or her place.

C.7.3 Initial Statements and Proposed Arbitration Decisions. Within 10 calendar days after the selection of an arbitrator under Section C.7.2 above, each party to the dispute shall submit a statement in writing to all other parties to the dispute and to the arbitrator. Each disputing party's statement shall set forth in reasonable detail the nature of the dispute, the issues to be arbitrated, and the party's reasonable, good faith proposal for resolving the dispute. As provided in Section C.5.3 above, to the extent permitted by law, no party to an arbitration conducted under

Sections C.6 and C.7 shall publicly disclose, rely on, or introduce as evidence in any arbitration, FERC proceeding, Canadian Regulatory Authority proceeding, proceeding before a Mexican Regulatory Authority, appeal, or litigation concerning the same or any related dispute any information required to be kept confidential by the terms of Section C.5.3.

C.7.4 Procedural Matters. The arbitrator shall determine discovery procedures, how evidence shall be taken, what written submittals may be made, and other such procedural matters, taking into account the complexity of the issues involved, the extent to which factual matters are disputed and the extent to which the credibility of witnesses is relevant to a resolution. Each party to the dispute shall produce all evidence determined by the arbitrator to be relevant and material to the issues presented. If such evidence involves proprietary or confidential information, the party submitting the evidence shall petition the arbitrator for a protective order, and to the extent the arbitrator determines there is good cause the arbitrator shall issue an appropriate protective order and all parties to the dispute shall comply with the protective order. The arbitrator may elect to resolve the arbitration matter solely on the basis of written evidence and arguments.

C.7.5 Out-of-Court Sworn Testimony. At the request of any disputing party, the arbitrator shall have the discretion to allow that party to examine witnesses through sworn out-of-court testimony (referred to in the United States as "deposition" and in Canada as "discovery") to the extent the arbitrator deems the evidence sought to be relevant and appropriate. In general, out-of-court witness examinations shall be limited to a maximum of three per party and shall be held

within 30 calendar days after the making of a request. Each witness examination shall be limited to a maximum of three hours' duration. The arbitrator shall have the discretion to permit the number and duration of examination sessions allowed under this Section C.7.5 to be increased, and to extend the 30-day time limit, upon request for good cause shown. All objections are reserved for the arbitration hearing except for objections based on privilege and proprietary or confidential information.

C.7.6 Intervention by Other Parties. Unless all of the parties to the dispute agree otherwise, no one (whether a Member, WECC, or any other entity or person) that is not a party to a dispute at the initiation of arbitration under Sections C.6 and C.7 shall have the right to intervene in the arbitration. Any party wishing to intervene in an arbitration under Sections C.6 and C.7 may petition the arbitrator for permission to intervene, provided that the petition is submitted to the arbitrator not more than 30 calendar days after notice of the arbitration is posted by WECC's Chief Executive Officer in accordance with Section C.7.1. The arbitrator shall have the discretion to permit a party to intervene if the arbitrator determines that the party petitioning to intervene has a direct and substantial interest in the outcome of the arbitration. In exercising his or her discretion concerning a requested intervention, the arbitrator shall also consider any additional complexity or delay that may be caused by allowing the intervention and also any other remedies available to the party requesting intervention. Any party that is granted the privilege of intervening in an arbitration under Sections C.6 and C.7 shall be permitted to intervene subject to the same terms, conditions,

limitations, rights, and obligations of all other parties to the dispute, including without limitation the binding effect of arbitrator's decision, limitations on rights of appeal, the obligation to share equally in the costs of the arbitrator, and the obligation to be subject to the provisions of Section C.8.

C.7.7 Consideration of WECC Criteria, Etc. The Arbitrator shall give due consideration to the reliability criteria, standards, guidelines, policies, and procedures of WECC and the North American Electric Reliability Council (or any successor organization) to the extent they are relevant to resolution of the matter(s) in dispute. If the arbitrator's decision will include interpretation of any of WECC's reliability criteria, standards, guidelines, policies, and procedures, (and WECC is not a party to the arbitration), the arbitrator shall, before rendering his or her decision, consult with WECC (subject to the provisions of Section C.7.10 below) concerning the interpretation of WECC's applicable reliability criteria, standards, guidelines, policies, and procedures.

C.7.8 Evidence and Rebuttal. The arbitrator shall consider all issues material to the matter(s) in dispute. The arbitrator shall take evidence submitted by the parties to the dispute in accordance with procedures established by the arbitrator and may request additional information the arbitrator deems material to the resolution of the dispute. With the consent of all parties to the dispute, the arbitrator's request for additional information may include the opinion of any individual or organization with recognized expertise in the matter(s) in dispute, subject to the following conditions: (i) any verbal communication with an expert consulted by the arbitrator must take place exclusively in the presence of all parties to the

dispute and copies of any written communications must be provided to all parties to the dispute; (ii) any expert consulted by the arbitrator must agree to be equally available upon request to all of the parties to the dispute; (iii) any expert consulted by the arbitrator must agree to comply with the restrictions on disclosure contained in Section C.5.3; and (iv) all parties to the dispute shall be afforded a reasonable opportunity to question the expert and to rebut any additional information submitted by the expert at the request of the arbitrator.

C.7.9 Arbitrator's Decision. The arbitrator shall make all reasonable efforts to complete hearings (if applicable) and submissions of written evidence not more than 90 calendar days after receiving initial statements submitted under Section C.7.3 above. As soon as practicable, but in no event more than 30 calendar days after the completion of hearings and evidence submittals, the arbitrator shall render his or her final decision for resolving the dispute. By agreement of all of the parties to the dispute or at the discretion of the arbitrator for good cause, the foregoing deadline for delivery of the arbitrator's decision may be extended. The arbitrator's decision shall be based on the arbitrator's good faith determination of a resolution that will: (i) be consistent with any laws, rules, and regulations applicable to the matter(s) in dispute; (ii) be consistent with any valid pre-existing agreements among the parties to the dispute that bear on the matter(s) in dispute; (iii) not require any party to the dispute to take action that is not in compliance with any of WECC's reliability criteria, standards, guidelines, policies, and procedures; and (iv) best serve to promote or maintain reliable operation of the interconnected Bulk Electric System of the Western Interconnection, without

imposing inequitable burdens or benefits on any of the parties to the dispute or others that may be affected by implementation of the arbitrator's decision. The arbitrator shall deliver to each of the parties to the dispute, along with his or her decision, a written statement including specific findings of fact, conclusions of law (if applicable), and an explanation of the arbitrator's basis for rendering his or her decision. Subject to any protective order that may have been issued under Section C.7.4 above, WECC's Chief Executive Officer shall publish (or cause to be published) in WECC's newsletter or electronic bulletin board a brief summary of the arbitrator's decision. An arbitrator's decision that is not appealed shall not be deemed to be precedential in any other arbitration related to a different dispute.

C.7.10 WECC Staff Participation in Arbitration When WECC Not a Party. If, during the course of binding arbitration conducted under Sections C.6 and C.7 (in which WECC is not a party) the arbitrator or any party to the dispute wishes to solicit the views of WECC staff concerning the application, implementation, interpretation, or fulfillment of any guidelines, criteria, standards, policies, or procedures of WECC, the arbitrator may request or permit the submission of WECC staff views only with the consent of all of the parties to the dispute and only if: (i) any participation by WECC staff takes place exclusively in the presence of all parties to the dispute; (ii) participating WECC staff members agree to be equally available upon request to all parties to the dispute; and (iii) participating WECC staff members agree to comply with the restrictions on disclosure contained in Section C.5.3.

C.7.11 Compliance and Costs. Unless one or more of the parties to the dispute initiates and notifies all other parties to the dispute that it has initiated a process to contest or appeal the arbitrator's decision under Sections C.9 through C.13, upon the decision by the arbitrator, the parties to the dispute shall, within the time frame specified by the arbitrator, and, subject to Section C.6.6 above, take whatever action is required to comply with the arbitrator's decision to the extent the arbitrator's decision does not require regulatory action. To the extent the arbitrator's decision affects jurisdictional rates, terms and conditions of service, or facilities or otherwise requires local, state, federal, or provincial approval or regulatory action, or a FERC filing or a Canadian Regulatory Authority filing by a Canadian Member or a Mexican Regulatory Authority filing by a Mexican Member, the affected Member (or WECC, if WECC is the party with the obligation to seek regulatory action) shall, within the time frame specified by the arbitrator, submit the arbitrator's decision or an appropriate filing to implement the arbitrator's decision and support the appropriate authority's acceptance or approval of the arbitrator's decision or implementation filing, except in cases where any party to the dispute has given notice of its intent to contest or appeal the arbitrator's decision. All costs associated with the arbitration (not including costs associated with attorney and expert witness fees incurred by the parties to the dispute) shall be divided equally among the parties to the dispute unless: (i) all of the parties to the dispute agree to an alternate method of allocating costs; or (ii) in rendering his or her decision, the arbitrator exercises his or her discretion

under Section C.8 below to assess fees, costs, or other monetary sanctions against one or more of the parties to the dispute for good cause.

C.7.12 Entry of Judgment. At any time after an arbitrator has rendered his or her decision in an arbitration conducted under Sections C.6 and C.7 (provided that the time provided for initiating an appeal under Sections C.11.1 and C.12 below has expired and no appeal or other means of contesting the arbitrator's decision has been initiated), judgment on the decision rendered by the arbitrator may be entered by any court of competent jurisdiction (subject to the provisions of Sections C.6.3, C.6.4, and C.6.6 above). If the award is against the United States, a party to the arbitration may apply to the United States District Court for the district in which the principal office of the applicable United States department or agency is located for an order confirming the award pursuant to 5 U.S.C. § 580.

C.8 Arbitrator's Discretion to Shift Costs or Impose Sanctions for Cause. Each party to any dispute submitted to arbitration under Sections C.6 and C.7 shall bear its own costs and fees associated with representation and participation in the arbitration process, and shall share equally in the arbitrator's fees except that the arbitrator shall have the discretion, to the extent permitted by law, to require one or more of the parties to the dispute to pay part or all of the costs and fees (including without limitation attorneys' and arbitrator's fees) of one or more other parties to the dispute, or to impose monetary sanctions on some other basis that is reasonable under the circumstances, for good cause. As used in this Section C.8, "good cause" means conduct involving serious abuse of or failure to comply with the dispute resolution process set forth in this Appendix C, willfully undertaken to harass or delay other parties to the dispute or to substantially impede the

arbitrator's ability to render a decision consistent with the provisions set forth in Section C.7.9.

C.9 Rights to Appeal Arbitration Decisions. Except to the extent otherwise provided by applicable United States state or federal law, applicable Canadian or provincial law, or applicable Mexican law, a party to a dispute resolved by arbitration under Sections C.6 and C.7 may appeal or contest the arbitrator's decision only on one or more of the bases specified in Section C.9.1 below and only in accordance with the procedures set forth in Sections C.9.2 through C.13.

C.9.1 Grounds for Appealing Arbitration Decisions. A party to a dispute resolved by arbitration under Sections C.6 and C.7 may contest or appeal the arbitrator's decision only on the basis that: (i) the arbitrator's decision is contrary to applicable law or regulation (including without limitation the FPA or FERC's then-applicable standards or policies, or comparable types of provisions that may apply under applicable Canadian, provincial, Mexican, or other laws and regulations); (ii) the arbitrator's decision is demonstrably arbitrary and capricious and without support in the record assembled during the arbitration; (iii) the arbitrator failed to afford one or more parties to the dispute an opportunity for a fair and meaningful hearing; (iv) the arbitrator engaged in serious misconduct in connection with the arbitration; (v) the arbitrator exceeded the authority conferred upon him or her under this Appendix C or as otherwise established by agreement of all the parties to the dispute; or (vi) the arbitrator's decision is contrary to the provisions of Section C.6.6.

C.9.2 Matter and One or More Parties to Dispute Subject to FERC Jurisdiction. If (i) the subject matter of a dispute arbitrated under Sections C.6 and C.7 is within the jurisdiction of FERC, and (ii) the conditions specified in Section C.12.1 or C.12.2 are satisfied, the rights of the parties to contest or appeal the arbitrator's decision shall be as set forth in Sections C.10 and C.12 below (subject also to the provisions of Section C.9.1 above). Notwithstanding the foregoing, nothing herein shall be construed or operate to require any Canadian or Mexican party or any other party that is not a "public utility" within the meaning of the FPA to make any filing with FERC under Sections 205 or 206 of the FPA.

C.9.3 All Parties and Matters in Dispute Subject to Jurisdiction of a Canadian Regulatory Authority. If all of the parties to an arbitrated dispute are subject to the jurisdiction of a particular Canadian Regulatory Authority, and if all matters in dispute are also subject to the jurisdiction of the same Canadian Regulatory Authority, any disputing party may appeal an arbitrator's decision to that Canadian Regulatory Authority, where such Canadian Regulatory Authority has jurisdiction to hear the appeal, or to the appropriate Canadian court. Any appeal to a Canadian Regulatory Authority or Canadian court shall be subject to the provisions set forth in Sections C.10 and C.11 below.

C.9.4 All Parties and the Matter in Dispute Subject to Jurisdiction of a Mexican Regulatory Authority. If all of the parties to an arbitrated dispute are subject to the jurisdiction of a particular Mexican Regulatory Authority, and if all matters in dispute are also subject to the jurisdiction of the same Mexican Regulatory Authority, any disputing party may appeal an arbitrator's decision to the

appropriate Mexican Regulatory Authority, subject to the provisions set forth in Sections C.10 and C.11 below.

C.9.5 Appeal to Court. If none of the preceding provisions concerning appealing or contesting an arbitrator's decision before FERC, a Canadian Regulatory Authority, or a Mexican Regulatory Authority apply to an arbitrated dispute, any party to an arbitrator's decision rendered in accordance with the provisions of Sections C.6 and C.7 may appeal the arbitrator's decision to a court of competent jurisdiction as provided under Section C.13 below.

C.10 Appealing or Contesting Arbitrator's Decision to FERC or a Presiding Authority. Subject to the conditions specified in Sections C.9.1 through C.9.5 above, any disputing party may appeal or contest an arbitrator's decision to FERC or an appropriate Presiding Authority as follows:

C.10.1 Record on Appeal. Except as otherwise provided in Section C.10.3 below, any appeal or action to contest an arbitrator's decision to FERC or a Presiding Authority shall be based solely upon the record assembled by the arbitrator. All parties to arbitrations conducted under Sections C.6 and C.7 intend that: (i) the FERC or other Presiding Authority should afford substantial deference to the factual findings of the arbitrator; (ii) the portion, if any, of the arbitrator's decision relating to issues not of first impression (i.e., matters previously decided by the FERC or other Presiding Authority or a court of competent jurisdiction in cases involving comparable facts and circumstances) should be afforded appropriate deference by the FERC or other Presiding Authority; and (iii) the

portion, if any, of the arbitrator's decision relating to issues of first impression should be afforded no deference by the FERC or other Presiding Authority.

C.10.2 No Expansion of Record on Appeal. Except as otherwise provided in Section C.10.3 below, no Member, non-Member, or WECC that has been a party to an arbitration under Sections C.6 and C.7 shall seek to expand the factual record before FERC or a Presiding Authority beyond that assembled by the arbitrator.

C.10.3 Exceptions to Limitations on Record on Appeal. If the arbitrator fails to assemble a complete record of the evidence submitted with respect to an arbitrated decision that is appealed pursuant to Sections C.9 through C.13, the parties to the appeal shall, notwithstanding the provisions of Sections C.10.1 and C.10.2 above, have the right to supplement the arbitrator's record before FERC or the Presiding Authority with any materials received into evidence by the arbitrator but omitted from the record assembled by the arbitrator. If an arbitrator's decision is appealed under Section C.9.1(iii) or (iv) above on the grounds that the arbitrator improperly excluded evidence so as to materially prejudice the outcome of the arbitration with respect to one or more of the parties to the dispute, any party to the appeal may submit the evidence asserted to be improperly excluded, but only as a basis to request that FERC or the Presiding Authority vacate the arbitrator's decision and remand the matter to the arbitrator (or, if FERC or the Presiding Authority determines that the arbitrator engaged in serious misconduct, to a newly selected arbitrator) for reconsideration of the matter with inclusion of the improperly excluded evidence. If an arbitrator's decision is appealed under Section C.9.1(iv)

above on the grounds of serious misconduct by the arbitrator, any party to the appeal may offer new evidence relating to the arbitrator's alleged misconduct.

C.11 Procedures for Appeals to Presiding Authority. If any party to an arbitration under Sections C.6 and C.7 desires to appeal an arbitrator's decision to an appropriate Presiding Authority, it shall provide written notice to that effect to all other parties to the arbitration, the arbitrator, and WECC's Chief Executive Officer within 14 calendar days following the date of the arbitrator's decision. If notice of appeal is timely provided:

C.11.1 Within 30 calendar days after the date of the appealing party's first notice of appeal, the party providing notice of appeal shall file its statement of position regarding the appeal with the Presiding Authority, together with the complete evidentiary record of the arbitration and a copy of the arbitrator's decision. The statement of position shall state that the appeal requested has been the subject of an arbitration pursuant to this Agreement.

C.11.2 Within 30 calendar days after the date of the appealing party's first notice of appeal, any other party that was a party to the arbitration may file its statement of position regarding the appeal with the Presiding Authority.

C.11.3 Copies of all materials filed with the Presiding Authority by any party during the course of an appeal shall be delivered to all other parties to the arbitration and to WECC's Chief Executive Officer.

C.11.4 Implementation of the arbitrator's decision shall be deemed stayed pending an appeal unless and until, at the request of a disputing party, the Presiding Authority issues an order shortening or extending the stay of implementation.

C.11.5 WECC's Chief Executive Officer shall publish (or cause to be published) a summary of each appeal in WECC's newsletter or electronic bulletin board.

C.11.6 The Members and WECC intend that any Presiding Authority's order resulting from an appeal under Sections C.9 and C.11 shall be subject to judicial review pursuant to laws governing the Presiding Authority and the matter in dispute that provide for judicial review of Presiding Authority action.

C.12 Procedures for Contesting or Appealing Arbitrator's Decision Before FERC. If any party to a dispute arbitrated under Sections C.6 and C.7 elects, subject to the limitations set forth in Sections C.9.1 through C.9.5 above, to contest or appeal an arbitrator's decision before FERC, the party so electing shall provide written notice to that effect to all other parties to the arbitration, the arbitrator, and WECC's Chief Executive Officer within 14 calendar days following the date of the arbitrator's decision. The provisions contained in Sections C.10.1, C.10.2, and C.10.3 above shall apply with respect to the record of the arbitration submitted to FERC. In addition, the following provisions shall apply:

C.12.1 FERC Filing by Prevailing Party. If the arbitrator's decision requires the prevailing party to take action that must have FERC approval or involves the provision of FERC-jurisdictional service by the prevailing party, the prevailing party shall file the arbitrator's decision or make an appropriate filing with FERC to implement the arbitrator's decision. Provided that it has given notice as required under Section C.12 above, any non-prevailing party may contest the prevailing party's filing in accordance's with FERC's applicable rules and regulations.

C.12.2 Complaint to FERC by Prevailing Party. If the arbitrator's decision requires a non-prevailing party to take action that must have FERC approval or involves the provision of FERC-jurisdictional service by any non-prevailing party, then, if the non-prevailing party has given notice as required under Section C.12 above, the prevailing party may submit the arbitrator's decision to FERC in the form of a complaint.

C.13 Appeal to Court. If none of the provisions that govern appealing or contesting an arbitrator's decision before FERC, a Canadian Regulatory Authority, or a Mexican Regulatory Authority as set forth in Sections C.9.2, C.9.3, or C.9.4 above apply, any disputing party may appeal an arbitrator's decision to any court of competent jurisdiction, subject to the conditions specified in Section C.9.1 above. Except as otherwise provided in Section C.10.3 above (substituting the words "court of competent jurisdiction" for "FERC or the Presiding Authority"), any appeal to a court shall be based solely upon the record assembled by the arbitrator, and no Member, non-Member, or WECC who is a party to an arbitration under Sections C.6 and C.7 shall seek to expand the factual record before the court beyond that assembled by the arbitrator.

Appendix of Additional Definitions Relating to
Alternative Dispute Resolution Provisions

Arbitration Notice has the meaning specified in Section C.7.1 of these Bylaws.

Canadian Regulatory Authority. The agency or agencies established under the laws of Canada or the applicable Provinces of Canada and having jurisdiction over facilities, interconnections, transmission rates, charges, terms, and conditions of service of a Canadian Member.

Dispute Notice has the meaning specified in Section C.5.1 of these Bylaws.

FERC. The Federal Energy Regulatory Commission or a successor agency.

FPA. The Federal Power Act (16 U.S.C. §§ 824 *et. seq.*), as it may be amended from time to time.

Mexican Regulatory Authority. The agency or agencies established under the laws of Mexico or the applicable states of Mexico and having jurisdiction over facilities, interconnections, transmission rates, charges, terms, and conditions of service of a Mexican Member.

Presiding Authority. As used in Sections C.10 and C.11, the term "Presiding Authority" has the following meanings: with respect to an appeal to an appropriate Canadian Regulatory Authority, "Presiding Authority" means the presiding Canadian Regulatory Authority or Canadian court with jurisdiction to hear the appeal; and with respect to an appeal to an appropriate Mexican Regulatory Authority, "Presiding Authority" means the presiding Mexican Regulatory Authority or Mexican court with jurisdiction to hear the appeal.

Attachment 5

Amended Exhibit C

of the Delegation Agreement between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council

Clean Version

Exhibit C – Regional Standard Development Procedure

Exhibit C shall set forth WECC's standards development procedure, which NERC agrees meets the following common attributes:

COMMON ATTRIBUTE 1

Proposed regional reliability standards shall be subject to approval by NERC, as the electric reliability organization, and by FERC before becoming mandatory and enforceable under Section 215 of the FPA in the United States. In Canada and Mexico, regional standards must be approved by applicable governmental authorities before becoming mandatory in those respective jurisdictions. No regional reliability standard shall be effective within the WECC area unless filed by NERC with FERC, and any applicable authorities in Canada and Mexico, and approved by FERC and any applicable authorities in Canada and Mexico.

COMMON ATTRIBUTE 2

WECC regional reliability standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk power system of the North American continent. A WECC reliability standard shall be more stringent than a continent-wide reliability standard, including a regional difference that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the bulk power system. A regional reliability standard that satisfies the statutory and regulatory criteria for approval of proposed North American reliability standards, and that is more stringent than a continent-wide reliability standard, would generally be acceptable.

COMMON ATTRIBUTE 3

WECC regional reliability standards, when approved by FERC and applicable authorities in Canada and Mexico, shall be made part of the body of NERC reliability standards and shall be enforced upon all applicable bulk power system owners, operators, and users within the WECC area, regardless of membership in the region.

COMMON ATTRIBUTE 4

Requester — The requester is the sponsor of the regional reliability standard request and may assist in the development of the standard. Any member of WECC, or group within WECC, shall be allowed to request that a regional reliability standard be developed, modified, or withdrawn. Additionally, any entity (person, organization, company, government agency, individual, etc.) that is directly and materially affected by the

reliability of the bulk power system in the WECC area shall be allowed to request a regional reliability standard be developed, modified, or withdrawn.

COMMON ATTRIBUTE 5

WECC Standards Committee — The WECC Standards Committee (WSC) manages the standards development process. The WSC will consider which requests for new or revised standards shall be assigned for development (or existing standards considered for deletion). The WSC will advise the WECC board on standards presented for adoption.

COMMON ATTRIBUTE 6

Ballot body — The ballot body consists of WECC members and non-members that have been determined eligible for the WECC Standards Voting Sectors. Each member of the ballot body is eligible to vote on Regional Reliability Standards and Regional Criteria, except that Participating Stakeholders may only vote on Regional Criteria that could result in a sanction to a non-WECC member. The WSC is responsible for overseeing the voting process for each document balloted.

COMMON ATTRIBUTE 7

WECC will coordinate with NERC such that the acknowledgement of receipt of a standard request identified in step 1, notice of comment posting period identified in step 5, and notice for vote identified in step 9 can be concurrently posted on both the WECC and NERC websites.

COMMON ATTRIBUTE 8

An acceptable standard request shall contain a description of the proposed regional reliability standard subject matter containing sufficiently descriptive detail to clearly define the purpose, scope, impacted parties, and other relevant information of the proposed standard.

COMMON ATTRIBUTE 9

Within 60 days of receipt of a completed standard request, the WSC shall determine the disposition of the standard request.

COMMON ATTRIBUTE 10

The WSC may take one of the following actions:

- Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The WSC may, at its discretion, expand or narrow the scope of the standard request under consideration.
- Reject the standard request. If the WSC rejects a standard request, a written explanation for rejection will be delivered to the requester within 30 days of the decision.
- Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the WSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the WSC.

COMMON ATTRIBUTE 11

Any standard request that is accepted by the WSC for development of a standard (or modification or deletion of an existing standard) shall be posted for public viewing on the WECC website within 30 days of acceptance by the committee.

COMMON ATTRIBUTE 12

The WSC will select members of the drafting team.

COMMON ATTRIBUTE 13

At the direction of the WSC, the standards process manager shall facilitate the posting of the draft standard on the WECC website, along with a draft implementation plan and supporting documents, for a no less than a 45-day comment period. The standards process manager shall provide notice to WECC stakeholders and other potentially interested entities, both within and outside of the WECC area, of the posting using communication procedures then currently in effect or by other means as deemed appropriate.

COMMON ATTRIBUTE 14

The drafting team shall prepare a summary of the comments received and the changes made to the proposed standard as a result of these comments. The drafting team shall summarize comments that were rejected by the drafting team and the reason(s) that these comments were rejected, in part or whole. The summary, along with a response to each comment received will be posted on the WECC website no later than the next posting of the proposed standard.

COMMON ATTRIBUTE 15

Upon recommendation of the WSC, the standards process manager shall post the proposed standard and implementation plan for ballot and shall announce the vote to approve the standard, including when the vote will be conducted and the method for voting. Once the notice for a vote has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued.

COMMON ATTRIBUTE 16

The standards process manager shall schedule a vote by the ballot pool. The vote shall commence no sooner than 15 days following the issuance of the notice for the vote.

COMMON ATTRIBUTE 17

The WECC ballot pool shall consist of Ballot Body entities that have opted to vote on a specific standard. The ballot pool shall be able to vote on the proposed standard during a period of not less than 15 days.

COMMON ATTRIBUTE 18

. Each standard action requires formation of a ballot pool of interested members of the registered ballot body.

COMMON ATTRIBUTE 19

A weighted majority vote of the Ballot Pool is required for a draft standard to be approved by the WECC membership and Participating Stakeholders. Abstentions and negative votes cast without an explanation shall not count toward the results but will be counted in determining whether a quorum of the Ballot Pool is achieved.

COMMON ATTRIBUTE 20

The WECC Board may only substantively modify the proposed regional reliability standard in accordance with its backstop authority as authorized by the WECC Bylaws.

COMMON ATTRIBUTE 21

Once a regional reliability standard is approved by the board, the standard will be submitted to NERC for approval and filing with FERC and applicable authorities in Canada and Mexico.

COMMON ATTRIBUTE 22

- **Open -** Participation in the development of a regional reliability standard shall be open to all organizations that are directly and materially affected by the WECC bulk power system reliability. There shall be no undue financial barriers to participation. Participation shall not be conditioned upon membership in WECC, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements. Meetings of drafting teams shall be open to the WECC members and others.

COMMON ATTRIBUTE 23

- **Balanced -** The WECC standards development process strives to have an appropriate balance of interests and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter.

COMMON ATTRIBUTE 24

- **Inclusive** — Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the bulk power system in the WECC area shall have a right to participate by: a) expressing a position and its basis, b) having that position considered, and c) having the right to appeal.

COMMON ATTRIBUTE 25

- **Fair 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 Participating Stakeholders.

COMMON ATTRIBUTE 26

- **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.

COMMON ATTRIBUTE 27

- Does not unnecessarily delay development of the proposed reliability standard.

COMMON ATTRIBUTE 28

Each standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

COMMON ATTRIBUTE 29

While reliability standards are intended to promote reliability, they must at the same time accommodate competitive electricity markets. Reliability is a necessity for electricity markets, and robust electricity markets can support reliability. Recognizing that bulk power system reliability and electricity markets are inseparable and mutually interdependent, all regional reliability standards shall be consistent with NERC's market interface principles. Consideration of the market interface principles is intended to ensure that standards are written such that they achieve their reliability objective without causing undue restrictions or adverse impacts on competitive electricity markets.

COMMON ATTRIBUTE 30

To ensure uniformity of regional reliability standards, a regional reliability standard shall consist of the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of standards. This discipline is necessary to achieving standards that are measurable, enforceable, and consistent.

COMMON ATTRIBUTE 31

All mandatory requirements of a regional reliability standard shall be within the standard. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself.

COMMON ATTRIBUTE 32

Applicability	Clear identification of the functional classes of entities responsible for complying with the standard, noting any specific additions or exceptions. If not applicable to the entire WECC area, then a clear identification of the portion of the bulk power system to which the standard applies. Any limitation on the applicability of the standard based on electric facility requirements should be described.

COMMON ATTRIBUTE 33

Measure(s)	Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.

COMMON ATTRIBUTE 34

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible for providing the data or information for measuring performance or

	outcomes. • The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating data or information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Measurement data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Attachment 6

Amended Exhibit C

of the Delegation Agreement between

North American Electric Reliability Corporation and

Western Electricity Coordinating Council

Redline Version

Exhibit C – Regional Standard Development Procedure

Exhibit C shall set forth WECC's standards development procedure, which NERC agrees meets the following common attributes:

COMMON ATTRIBUTE 1

Proposed regional reliability standards shall be subject to approval by NERC, as the electric reliability organization, and by FERC before becoming mandatory and enforceable under Section 215 of the FPA in the United States. In Canada and Mexico, regional standards must be approved by applicable governmental authorities before becoming mandatory in those respective jurisdictions. No regional reliability standard shall be effective within the WECC area unless filed by NERC with FERC, and any applicable authorities in Canada and Mexico, and approved by FERC and any applicable authorities in Canada and Mexico.

COMMON ATTRIBUTE 2

WECC regional reliability standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk power system of the North American continent. A WECC reliability standard shall be more stringent than a continent-wide reliability standard, including a regional difference that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the bulk power system. A regional reliability standard that satisfies the statutory and regulatory criteria for approval of proposed North American reliability standards, and that is more stringent than a continent-wide reliability standard, would generally be acceptable.

COMMON ATTRIBUTE 3

WECC regional reliability standards, when approved by FERC and applicable authorities in Canada and Mexico, shall be made part of the body of NERC reliability standards and shall be enforced upon all applicable bulk power system owners, operators, and users within the WECC area, regardless of membership in the region.

COMMON ATTRIBUTE 4

Requester — The requester is the sponsor of the regional reliability standard request and may assist in the development of the standard. Any member of WECC, or group within WECC, shall be allowed to request that a regional reliability standard be developed, modified, or withdrawn. Additionally, any entity (person, organization, company, government agency, individual, etc.) that is directly and materially affected by the

reliability of the bulk power system in the WECC area shall be allowed to request a regional reliability standard be developed, modified, or withdrawn.

COMMON ATTRIBUTE 5

WECC Standards Committee ~~and Standing Committees~~ — The WECC Standards Committee (WSC) manages the standards development process. The WSC will consider which requests for new or revised standards shall be assigned for development (or existing standards considered for deletion). ~~The WSC, with assistance from the standing committees,~~The WSC will advise the WECC board on standards presented for adoption.

COMMON ATTRIBUTE 6

Ballot body — The ballot body consists of WECC members and non-members that have been determined eligible for the WECC ~~Standard~~Standards Voting Sectors. Each member of the ballot body is eligible to vote on Regional Reliability Standards and Regional Criteria~~.~~, except that Participating Stakeholders may only vote on Regional Criteria that could result in a sanction to a non-WECC member. The WSC is responsible for overseeing the voting ~~on~~process for each ~~standard.~~document balloted.

COMMON ATTRIBUTE 7

WECC will coordinate with NERC such that the acknowledgement of receipt of a standard request identified in step ~~2~~1, notice of comment posting period identified in step ~~4~~5, and notice for vote identified in step ~~6 below are~~9 can be concurrently posted on both the WECC and NERC websites.

COMMON ATTRIBUTE 8

An acceptable standard request shall contain a description of the proposed regional reliability standard subject matter containing sufficiently descriptive detail to clearly define the purpose, scope, impacted parties, and other relevant information of the proposed standard.

COMMON ATTRIBUTE 9

Within ~~14~~60 days of receipt of a completed standard request, the WSC shall determine the disposition of the standard request.

COMMON ATTRIBUTE 10

The WSC may take one of the following actions:

- Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The WSC may, at its discretion, expand or narrow the scope of the standard request under consideration.
- Reject the standard request. If the WSC rejects a standard request, a written explanation for rejection will be delivered to the requester within ~~14~~30 days of the decision.
- Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the WSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the WSC.

COMMON ATTRIBUTE 11

Any standard request that is accepted by the WSC for development of a standard (or modification or deletion of an existing standard) shall be posted for public viewing on the WECC website within 30 days of acceptance by the committee.

COMMON ATTRIBUTE 12

The WSC will select members of the drafting team.

COMMON ATTRIBUTE 13

At the direction of the WSC, the standards process manager shall facilitate the posting of the draft standard on the WECC website, along with a draft implementation plan and supporting documents, for a no less than a 45-day comment period. The standards process manager shall provide notice to WECC stakeholders and other potentially interested entities, both within and outside of the WECC area, of the posting using communication procedures then currently in effect or by other means as deemed appropriate.

COMMON ATTRIBUTE 14

The ~~WSC, with assistance from the~~ drafting team ~~as it requests,~~ shall prepare a summary of the comments received and the changes made to the proposed standard as a result of these comments. The ~~WSC~~drafting team shall summarize comments that were rejected by the ~~WSC~~drafting team and the reason(s) that these comments were rejected, in part or whole. The summary, along with a response to each comment received will be posted on the WECC website ~~within 30 days of~~no later than the ~~close~~next posting of the ~~comment period.~~proposed standard.

COMMON ATTRIBUTE 15

Upon recommendation of the WSC, the standards process manager shall post the proposed standard and implementation plan for ballot and shall announce the vote to approve the standard, including when the vote will be conducted and the method for voting. Once the notice for a vote has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued.

COMMON ATTRIBUTE 16

The standards process manager shall schedule a vote by the ~~WECC lead standing committee].~~ballot pool. The vote shall commence no sooner than ~~[30]~~15 days following the issuance of the notice for the vote. ~~Voting shall begin no sooner than [7] calendar days following the Joint Session of the Standing Committees at which the draft standard was considered.~~

COMMON ATTRIBUTE 17

The WECC ballot pool shall consist of Ballot Body entities that have opted to vote on a specific standard. The ballot pool shall be able to vote on the proposed standard during a period of not less than 15 ~~business~~ days.

COMMON ATTRIBUTE 18

~~All Ballot Body members are eligible to participate in voting on proposed new standards, standard revisions or standard deletions.~~ . Each standard action requires formation of a ballot pool of interested members of the registered ballot body.

COMMON ATTRIBUTE 19

A weighted majority vote of the Ballot Pool is required for a draft standard to be approved by the WECC membership and Participating Stakeholders. Abstentions and ~~non-responses~~negative votes cast without an explanation shall not count toward the results but will be counted in determining whether a quorum of the Ballot Pool is achieved.

COMMON ATTRIBUTE 20

The WECC Board may only substantively modify the proposed regional reliability standard in accordance with its backstop authority as authorized by the WECC Bylaws.

COMMON ATTRIBUTE 21

Once a regional reliability standard is approved by the board, the standard will be submitted to NERC for approval and filing with FERC and applicable authorities in Canada and Mexico.

COMMON ATTRIBUTE 22

- **Open** - Participation in the development of a regional reliability standard shall be open to all organizations that are directly and materially affected by the WECC bulk power system reliability. There shall be no undue financial barriers to participation. Participation shall not be conditioned upon membership in WECC, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements. Meetings of drafting teams shall be open to the WECC members and others.

COMMON ATTRIBUTE 23

- **Balanced** - The WECC standards development process strives to have an appropriate balance of interests and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter.

COMMON ATTRIBUTE 24

- **Inclusive** — Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the bulk power system in the WECC area shall have a right to participate by: a) expressing a position and its basis, b) having that position considered, and c) having the right to appeal.

COMMON ATTRIBUTE 25

- **Fair 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 Participating Stakeholders.

COMMON ATTRIBUTE 26

- **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.

COMMON ATTRIBUTE 27

- Does not unnecessarily delay development of the proposed reliability standard.

COMMON ATTRIBUTE 28

Each standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

COMMON ATTRIBUTE 29

While reliability standards are intended to promote reliability, they must at the same time accommodate competitive electricity markets. Reliability is a necessity for electricity markets, and robust electricity markets can support reliability. Recognizing that bulk power system reliability and electricity markets are inseparable and mutually interdependent, all regional reliability standards shall be consistent with NERC's market interface principles. Consideration of the market interface principles is intended to ensure that standards are written such that they achieve their reliability objective without causing undue restrictions or adverse impacts on competitive electricity markets.

COMMON ATTRIBUTE 30

To ensure uniformity of regional reliability standards, a regional reliability standard shall consist of the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of standards. This discipline is necessary to achieving standards that are measurable, enforceable, and consistent.

COMMON ATTRIBUTE 31

All mandatory requirements of a regional reliability standard shall be within the standard. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself.

COMMON ATTRIBUTE 32

Applicability	Clear identification of the functional classes of entities responsible for complying with the standard, noting any specific additions or exceptions. If not applicable to the entire WECC area, then a clear identification of the portion of the bulk power system to which the standard applies. Any limitation on the applicability of the standard based on electric facility requirements should be described.

COMMON ATTRIBUTE 33

Measure(s)	Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.

COMMON ATTRIBUTE 34

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible for providing the data or information for measuring performance or outcomes. • The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating data or information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Measurement data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 23, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Petition to Approve the Western Electricity Coordinating Council Data Request Process
Docket No. RR15-__-___

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC"), in accordance with the *NERC Rules of Procedure* Section 1604.2,[1] respectfully submits the attached Western Electricity Coordinating Council ("WECC") Data Request Process to the Federal Energy Regulatory Commission ("FERC" or the "Commission") for approval.

With respect to Regional Entity data requests, the *NERC Rules of Procedure* Section 1604 provides that a Regional Entity may develop its own procedures for requesting data or information, so long as any such procedures include at least the same procedural elements as are included in Section 1600. Such Regional Entity procedures must also be submitted to NERC for approval and, upon approval, NERC must file the proposed procedures for approval to FERC and other applicable governmental authorities.

[1] The Commission-approved *NERC Rules of Procedure* Section 1604.2 states:

> 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 Applicable 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 Applicable Governmental Authority.

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

On May 15, 2014, the WECC Board of Directors reviewed a proposed version of the WECC Data Request Process that was written to permit WECC staff to issue mandatory data requests for reliability data to entities in the Western Interconnection. WECC's Board of Directors deferred a decision on approving the process in order to allow its Member Advisory Committee ("MAC") to review and provide input. On June 25, 2014, the WECC Board of Directors approved the attached WECC Data Request Process, including amendments made by MAC during the review period. The MAC amendments added a provision to clarify that the process is not binding on entities outside of the United States. However, WECC may request comparable data or information from those entities on a voluntary basis.

On June 30, 2014, WECC submitted the proposed process to the NERC Board of Trustees for approval. On August 14, 2014, the NERC Board of Trustees approved the attached WECC Data Request Process.

Following FERC's approval of WECC's Data Request Process, WECC anticipates it may seek approval by its Board of Directors of such a data request as early as March 2015. Given the amount of time required to move a request through the process, and because the process included in the attachment is not controversial, NERC respectfully requests expedited action of this petition from the Commission by December 31, 2014.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins
Associate General Counsel
North American Electric Reliability Corporation
1325 G Street NW, Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
Holly.Hawkins@nerc.net

Counsel for North American Electric Reliability Corporation

ATTACHMENT

WECC Data Request Process

INTRODUCTION

Pursuant to Section 215 of the Federal Power Act and Section 1600 of the North American Electric Reliability Corporation ("NERC") Rules of Procedure, Western Electricity Coordinating Council ("WECC") has the authority to request data or information that is necessary to meet its obligations as a Regional Entity from owners, operators, and users of the Bulk Power System in the United States. This process is not binding on entities outside of the United States. However, WECC may request comparable data or information from those entities on a voluntary basis.

SCOPE

This WECC Data Request Process ("Process") shall not apply to or interfere with Requirements contained in any Reliability Standard to provide data or information. This Process shall also not apply to data or information requested in connection with a compliance or enforcement action or any procedures adopted applicable to such compliance or enforcement actions.

PROCESS

1. **Submission to NERC and FERC**: WECC shall provide a proposed request for data or information or a proposed modification to a previously-authorized request, including the information specified in Section 2 below as applicable, to NERC and the Federal Energy Regulatory Commission's ("FERC" or "Commission") Office of Electric Reliability ("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 NERC and the FERC Office of Electric Reliability is for the information of NERC and the Commission. WECC is not required to receive any approval from NERC or the Commission prior to posting the proposed request or modification for public comment in accordance with Section 2 below or issuing the request or modification to Reporting Entities following approval by the WECC Board of Directors.

2. **Posting for Comment**: WECC 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.
    a. 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;
        ii. how the data or information will be used;
        iii. how the availability of the data or information is necessary for WECC to meet its obligations as a Regional Entity;
        iv. a description of how the data or information will be collected and validated;
        v. a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("Reporting Entities");
        vi. the schedule or due date for the data or information;

vii. a description of any restrictions on WECC's dissemination of the data or information; and
viii. an estimate of the relative burden imposed on the Reporting Entities to accommodate the data or information request.

b. 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 Section 2.a above that require updating as a result of the modifications.

3. **Submission to the WECC Board of Directors**: After the close of the comment period, WECC shall make any revisions it deems appropriate to the proposed request for data or information in light of the comments received. WECC shall submit the proposed request for data or information, as revised, along with the comments received, and an evaluation of the comments and revisions, to the WECC Board of Directors.

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

5. **Minor Revisions to Data Requests**: WECC may make minor changes to an authorized request for data or information without WECC Board of Director approval. However, if a Reporting Entity objects in writing to such changes to WECC within 21 days of issuance of the modified request, such changes shall require WECC Board of Director approval before they are implemented.

6. **Authorization and Appeals**: Authorization of a request for data or information shall be final unless, within thirty (30) days of the decision by the WECC Board of Directors, an affected party appeals the authorization to the NERC Board of Trustees. Determinations of the NERC Board of Trustees may be appealed to the Commission.

7. **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 this Process, WECC may request that NERC 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. Such requests shall be made through non-public submissions to NERC and the Commission.

8. **Confidentiality**: If the approved data or information request includes a statement that the requested data or information will be treated as confidential, then the applicable

provisions of Section 1500 of the NERC Rules of Procedure will apply without further action by a Submitting Entity. A Submitting Entity may designate any other data or information in the request as Confidential Information pursuant to the provisions of Section 1500. WECC shall treat all such data or information in accordance with Section 1500.

APPROVAL AND ADOPTION

WECC BOARD OF DIRECTORS EFFECTIVE _____

Custodian	*General Counsel*
Review Cycle	*2 years*
Last Reviewed Date	*[Date]*

20141106-3036 FERC PDF (Unofficial) 11/06/2014

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RD14-12-000

November 6, 2014

North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005

Attention: Stacey Tyrewala, Senior Counsel
North American Electric Reliability Corporation

Reference: Petition for Approval of Proposed Reliability Standards FAC-001-2 (Facility Interconnection Requirements) and FAC-002-2 (Facility Interconnection Studies)

Dear Ms. Tyrewala:

On August 22, 2014, the North American Electric Reliability Corporation (NERC) filed a petition (Petition) seeking approval of proposed Reliability Standards FAC-001-2 (Facility Interconnection Requirements) and FAC-002-2 (Facility Interconnection Studies), the associated implementation plan, violation risk factors and violation security levels, and the retirement of currently-effective Reliability Standards FAC-001-1 and FAC-002-1.

In its Petition, NERC states that the proposed Reliability Standards are intended to improve Bulk-Power System reliability by ensuring that there is appropriate coordination regarding the interconnection of facilities.[1] NERC explains that the standard drafting team's revisions to the currently-effective Reliability Standards FAC-001-1 and FAC-002-1 eliminate redundancies and clarify the actions required in the standards.[2] NERC further states that proposed Reliability Standard FAC-001-2 sets forth the requirements

[1] NERC Petition at 3.

[2] *Id.* at 4.

20141106-3036 FERC PDF (Unofficial) 11/06/2014

related to transmission owners and applicable generation owners[3] for making facility interconnection requirements available so that entities seeking to interconnect have the necessary information, and proposed Reliability Standard FAC-002-2 ensures that the reliability impact of interconnecting new or materially modified facilities is studied.[4]

Proposed Reliability Standard FAC-001-2 requires each transmission owner and applicable generator owner to document facility interconnection requirements, and to make them available upon request to entities seeking to interconnect. In addition, proposed Reliability Standard FAC-001-2 requires each transmission owner and applicable generator owner to include procedures for coordinating studies to determine the impact of interconnecting facilities on existing interconnections as well as on affected systems.

Proposed Reliability Standard FAC-002-2 requires each transmission planner and each planning coordinator to study the reliability impact of interconnecting new--or materially modifying existing-- generation, transmission, or electricity end-user facilities on affected systems. In particular, proposed Reliability Standard FAC-002-2 requires transmission planners and planning coordinators to perform steady-state, short-circuit, and dynamic studies to evaluate system performance under both normal and contingency conditions. In addition, proposed Reliability Standard FAC-002-2 requires each generator owner seeking to interconnect, each transmission owner, each distribution provider, and each load-serving entity that is seeking to interconnect new--or materially modifying existing--transmission facilities or end-user facilities to coordinate and cooperate on studies with its transmission planner and planning coordinator.

NERC's filing was noticed on August 26, 2014, with interventions, comments, and protests due on or before September 25, 2014. No interventions, comments or protests were filed.

NERC's uncontested filing is hereby approved pursuant to the relevant authority delegated to the Director, Office of Electric Reliability under 18 C.F.R. § 375.303 (2014), effective as of the date of this Order.

This action shall not be construed as approving any other application, including proposed revisions of Electric Reliability Organization or Regional Entity rules or procedures pursuant to 18 C.F.R. § 375.303(a)(2)(i). Such action shall not be deemed as

---

[3] An "applicable generation owner" is a generation owner "with a fully executed Agreement to conduct a study on the reliability impact of interconnecting a third party Facility to the Generator Owner's existing Facility that is used to interconnect to the Transmission System." Section 4.1.2.1 of Reliability Standard FAC-001-2 and section 4.1.6.1 of Reliability Standard FAC-002-2.

[4] NERC Petition at 3.

20141106-3036 FERC PDF (Unofficial) 11/06/2014

recognition of any claimed right or obligation associated therewith and such action is without prejudice to any findings or orders that have been or may hereafter be made by the Commission in any proceeding now pending or hereafter instituted by or against the Electric Reliability Organization or any Regional Entity.

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 (2014).

Sincerely,

Michael Bardee, Director
Office of Electric Reliability

Document Content(s)

RD14-12-000.DOCX.....1-3

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF ENERGY MARKET REGULATION

North American Electric Reliability Corporation
Docket No. RR14-6-001

October 28, 2014

Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago, IL 60606

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

Reference: Revisions to the 2015 Budget and Assessments of Peak Reliability, Inc.

Dear Mr. MacBride:

On October 14, 2014, North American Electric Reliability Corporation (NERC) submitted revisions to the 2015 Business Plan and Budget of Peak Reliability, Inc. (Peak), including a revised schedule of assessments that reflects an agreement with the British Columbia Hydro and Power Authority (BC Hydro), pursuant to which BC Hydro's Balancing Authority Area will remain a part of Peak's Reliability Coordination Area.

Notice of this filing was issued on October 15, 2014, with protests and interventions due on or before October 21, 2014. Notices of intervention and unopposed timely filed motions to intervene are granted pursuant to the operation of Rule 214 of the Commission's Rules of Practice and Procedure 18 C.F.R. § 385.214. No protests were filed.

NERC's uncontested filing is accepted pursuant to the relevant authority delegated to the Director, Office of Energy Market Regulation, under 18 C.F.R. § 375.307.

This action shall not be construed as approving any other application, including proposed revisions of Electric Reliability Organization or Regional Entity rules or procedures pursuant to 18 C.F.R. § 375.307(a)(2)(vi). This action does not constitute approval of any service, rate, charge, classification, or any rule, regulation, contract, or practice affecting such rate or service provided for in the filed documents. Such action

shall not be deemed as recognition of any claimed right or obligation associated therewith and such action is without prejudice to any findings or orders that have been or may hereafter be made by the Commission in any proceeding now pending or hereafter instituted by or against the Electric Reliability Organization or any Regional Entity.

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,

Penny S. Murrell, Director
Division of Electric Power Regulation-Central

148 FERC ¶ 61,192
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM14-12-000]

Demand and Energy Data Reliability Standard

(September 18, 2014)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Commission proposes to approve Demand and Energy Data Reliability Standard MOD-031-1 developed by the North American Electric Reliability Corporation, which the Commission has certified as the Electric Reliability Organization responsible for developing and enforcing mandatory Reliability Standards.

DATES: Comments are due **[60 days after publication in the FEDERAL REGISTER].**

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:

Susan Morris (Technical Information)
Office of Electric Reliability, Division of Reliability Standards and Security
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-6803
Susan.Morris@ferc.gov

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
Robert.Stroh@ferc.gov

SUPPLEMENTARY INFORMATION:

148 FERC ¶ 61,192
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Demand and Energy Data Reliability Standard Docket No. RM14-12-000

NOTICE OF PROPOSED RULEMAKING

(September 18, 2014)

1. Pursuant to section 215(d) of the Federal Power Act (FPA),[1] the Commission proposes to approve Reliability Standard MOD-031-1 (Demand and Energy Data) developed by the North American Electric Reliability Corporation (NERC), which the Commission has certified as the Electric Reliability Organization (ERO) responsible for developing and enforcing mandatory Reliability Standards. Reliability Standard MOD-031-1 provides authority for applicable entities to collect demand, energy and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents of that data. In addition, the Commission proposes to approve NERC's proposed definitions for the terms Demand Side Management and Total Internal Demand. The Commission also proposes to approve the associated implementation plan, violation risk factors and violation severity levels, and NERC's proposed retirement of the currently-effective Reliability Standards MOD-016-1.1, MOD-017-0.1, MOD-018-0, MOD-019-0.1, and MOD-021-1 (Existing MOD C Standards).

[1] 16 U.S.C. § 824o(d) (2012).

I. Background

2. 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 are enforced by the ERO, subject to Commission oversight, or by the Commission independently. In 2006, NERC submitted the initial version of Reliability Standards MOD-016-1.1, MOD-017-0.1, MOD-018-0, MOD-019-0.1, MOD-020-0, and MOD-021-1. The Existing MOD C Standards are designed to help ensure that historical and forecasted demand and energy data are available for past event validation and future system assessment. In particular, the Existing MOD C Standards, along with Reliability Standard MOD-020-0, require the collection of actual and forecast demand data necessary to analyze the resource needs to serve peak demand while maintaining a sufficient margin to address operating events.[2] In Order No. 693, the Commission approved the Existing MOD C Standards and Reliability Standard MOD-020-0. In addition, the Commission directed NERC to develop certain modifications to the standards.

II. NERC Petition

3. NERC states that proposed Reliability Standard MOD-031-1 provides planners and operators access to actual and forecast demand and energy data, as well as other

[2] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at PP 1223, 1235, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

related information, needed to perform resource adequacy studies.[3] NERC explains that the proposed Reliability Standard also supports the continued development of the reliability assessments prepared by NERC. NERC states that the proposed Reliability Standard improves the Existing MOD C Standards by: (1) streamlining them to clarify data collection requirements; (2) including transmission planners as applicable entities that must report demand and energy data; (3) requiring applicable entities to report weather normalized annual peak hour actual demand data from the previous year to allow for meaningful comparison with forecasted values; and (4) requiring applicable entities to provide an explanation of how their demand side management forecasts compare to actual demand side management for the prior calendar year and how their peak demand forecasts compare to actual demand for the prior calendar year with due regard to any relevant weather-related variations.[4]

4. Proposed Reliability Standard MOD-031-1 contains four requirements. Requirement R1 mandates that each planning coordinator or balancing authority that identifies a need for the collection of demand and energy data shall develop and issue a data request for such data to the relevant entities in its area. The requirement mandates that the data request identify: (i) the entities responsible for providing the data; (ii) the data to be provided by each entity; and (iii) the schedule for providing the data.

---

[3] NERC Petition at 3. The proposed MOD Reliability Standard is not attached to the NOPR. The complete text of the Reliability Standard is available on the Commission's eLibrary document retrieval system in Docket No. RM14-12 and is posted on the ERO's web site, *available at*: http://www.nerc.com.

[4] NERC Petition at 4.

Requirement R2 obligates the entities identified in a Requirement R1 data request to provide the requested data to their planning coordinator or balancing authority. Requirement R3 requires that the planning coordinator or the balancing authority provide the data collected under Requirement R2 to their Regional Entity, if requested, to facilitate NERC's development of reliability assessments. Requirement R4 requires entities to share their demand and energy data with any applicable entity that demonstrates a reliability need for such data, subject to applicable confidentiality, regulatory or security restrictions.[5]

5. The term Demand Side Management is currently defined in the NERC Glossary as: "[t]he term for all activities or programs undertaken by a Load-Serving Entity or its customers to influence the amount or timing of electricity they use." NERC proposes to modify the definition of "Demand Side Management" as "[a]ll activities or programs undertaken by any applicable entity to achieve a reduction in Demand." NERC states that, consistent with the Commission directive in Order No. 693, the proposed definition for Demand Side Management is not limited to "activities or program undertaken by Load Serving Entities or its customers" but is expanded to include "activities or programs undertaken by any applicable entity."[6]

6. NERC requests that the Commission approve the proposed Reliability Standard, the proposed new and modified NERC Glossary terms and the retirement of the Existing

[5] *Id.* at 5.

[6] *Id.* at 15-16.

MOD C Standards, effective on the first day of the first calendar quarter that is twelve months after Commission approval. NERC states that the 12-month implementation period is designed to provide applicable entities sufficient time to transition from compliance with the Existing MOD C Standards to proposed Reliability Standard MOD-031-1.[7]

III. Discussion

7. Pursuant to section 215(d)(2) of the FPA, the Commission proposes to approve Reliability Standard MOD-031-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We also propose to approve the new and modified glossary definitions, implementation plan, associated violation risk factors and violation severity levels as well as the retirement of the Existing MOD C Standards, as requested by NERC.

8. The Commission believes that the proposed Reliability Standard MOD-031-1 continues to provide planners and operators access to complete and accurate demand and energy data to allow such entities to conduct their own resource adequacy analyses to serve peak demand. The proposed Reliability Standard also appears to provide for consistent documentation and information sharing practices for demand and energy data, and promotes efficient planning practices across the industry and supports the identification of needed system reinforcements. The Commission believes that proposed Reliability Standard MOD-031-1 improves the Existing MOD C Standards by providing

[7] *Id.* at 31.

applicable entities the authority to collect demand and energy data, and related information, to support reliability assessments and also includes transmission planners as applicable entities that must report demand and energy data. Furthermore, the proposed Reliability Standard requires applicable entities to provide an explanation of current and previous demand side management forecasts and how their peak demand forecasts compare to actual demand for the prior calendar year.

9. While we propose to approve Reliability Standard MOD-031-1, we seek comment on the collection of data through mechanisms other than data requests. Requirements R1 through R3 specifically reference the obtaining of data through data requests as follows:

> R1. Each Planning Coordinator or Balancing Authority that identifies a need for the collection of Total Internal Demand, Net Energy for Load, and Demand Side Management data shall develop and issue a data request to the applicable entities in its area. The data request shall include:...
>
> R2. Each Applicable Entity identified in a data request shall provide the data requested by its Planning Coordinator or Balancing Authority in accordance with the data request issued pursuant to Requirement R1.
>
> R3. The Planning Coordinator or the Balancing Authority shall provide the data collected under Requirement R2 to the applicable Regional Entity within 75 calendar days of receiving a request for such data, unless otherwise agreed upon by the parties.

In its petition, NERC states that Requirement R1 applies when a planning coordinator or balancing authority "identifies a need" for the collection of demand and energy data.[8] According to NERC, this language of Requirement R1:

[8] NERC Petition at 22.

> is intended to reflect that certain Planning Coordinators and Balancing Authorities may not need to collect Demand and energy data through a data request issued pursuant to the proposed Reliability Standard. That is because certain Planning Coordinators and Balancing Authorities obtain the data through alternative mechanisms or develop the data themselves. For instance, many Planning Coordinators, such as independent system operators (ISOs) and regional transmission organizations (RTOs), collect the necessary data and information from entities within their footprint pursuant to requirements in their Open Access Transmission Tariffs. Additionally, ISOs/RTOs are often in a better position to develop the necessary Demand and energy forecasts or aggregate the historical data than the entities in their area. Accordingly, the requirement is drafted so as to only require a Planning Coordinator or Balancing Authority to issue a data request if there is a need to do so.[9]

10. The Commission understands NERC's explanation to mean that, while a planning coordinator or balancing authority may collect demand and energy forecast data under a tariff or other arrangement, the planning coordinator or balancing authority always retains the option to seek the necessary data through a Requirement R1 data request if, for example, the data are not forthcoming through other means. The Commission seeks comment on this understanding. Further, the Commission seeks clarification from NERC and other commenters whether a planning coordinator or balancing authority that receives data "through alternative mechanisms" remains obligated to provide such data (i.e., within the scope of Requirement R1) to a Regional Entity upon request, as set forth in Requirement R3.

[9] *Id.* at 22-23.

IV. Information Collection Statement

11. The collection of information contained in this Notice of Proposed Rulemaking (NOPR) is subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[10] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[11] 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 a 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.

12. We solicit comments on the need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques. Specifically, the Commission asks that any revised burden or cost estimates submitted by commenters be supported by sufficient detail to understand how the estimates are generated.

13. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE,

[10] 44 U.S.C. 3507(d) (2012).

[11] 5 CFR 1320.11.

Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

14. Comments concerning the information collection proposed in this NOPR and the associated burden estimates should be sent to the Commission in this docket and may also be sent to the Office of Management and Budget, Office of Information and Regulatory Affairs [Attention: Desk Officer for the Federal Energy Regulatory Commission]. For security reasons, comments should be sent by e-mail to OMB at the following e-mail address: oira_submission@omb.eop.gov. Please reference FERC-725L and the docket number of this Notice of Proposed Rulemaking (Docket No. RM14-12-000) in your submission.

15. The Commission proposes to approve Reliability Standard MOD-031-1, which will replace MOD-016-1.1, MOD-017-.01, MOD-018-0, MOD-019-0.1 and MOD-021-1 (Existing MOD C Standards). As stated above, the Existing MOD C Standards were approved by the Commission in Order No. 693. All information collection estimates associated with the collection of demand and energy data and subsequent retention were assessed in Order No. 693 and will not be repeated here. The proposed Reliability Standard expands the actual data to be submitted in two areas: (1) weather normalized annual peak hour actual demand for the prior calendar year if this demand varies due to weather-related conditions (e.g., temperature, humidity or wind speed); and (2) summaries detailed in Requirement R1, Subparts 1.5.4 and 1.5.5. The additional data and summaries will increase reporting and preparation time for some applicable entities. Most entities already normalize their actual demand data based on weather. However,

some entities may have a one-time cost of determining the method to "weather normalize" the actual demand data. Accordingly, the information collection costs will consist of an annual cost for all applicable entities and, for a small percentage, additional costs will occur during the first year of implementation.

Public Reporting Burden: Reliability Standard MOD-031-1 requires each "Applicable Entity" to provide the data requested by its planning coordinator or balancing authority in accordance with the data request issued pursuant to Requirement R1.[12] Our estimate below regarding the number of respondents is based on the NERC Compliance Registry as of July 31, 2014. According to the NERC Compliance Registry, NERC has registered 478 distribution providers, 469 load-serving entities, 179 transmission planners and 107 balancing authorities. However, under NERC's compliance registration program, entities may be registered for multiple functions, so these numbers incorporate some double counting. The total number of unique entities that may be identified as a data provider (e.g. applicable entity) in accordance with proposed Reliability Standard MOD-031-1 will be approximately 561 entities registered in the United States as a distribution provider, load-serving entity, transmission planner and/or balancing authority.[13] The Commission estimates the annual reporting burden and cost as follows:

[12] Requirement R1, Subpart 1.1 refers to "Applicable Entities" as the list of transmission planners, balancing authorities, load-serving entities and distribution providers that are required to provide the data.

[13] This estimate assumes all of the unique entities will be identified to provide demand and energy data.

	Number and Type of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Avg. Burden & Cost Per Response (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent[14] (5)÷(1)**
(One-time) Determine method to weather normalize annual peak hour actual demand.	28[15] (DP, LSE, TP and/or BA)[16]	1	28	240 hrs. & $14,309	6,720 hours & $400,646	$14,309
(On-going) Develop summary in accordance w/ Requirement R1, Subparts 1.5.4 and 1.5.5.	561 (DP, LSE, TP and/or BA)	1	561	8 hrs. & $477	4,488 hours & $267,575	$477
TOTAL			589		11,208 hours & $668,221	

[14] The estimated hourly costs (salary plus benefits) are based on Bureau of Labor Statistics (BLS) information (*available at* http://bls.gov/oes/current/naics3_221000.htm#17-0000) for an electrical engineer ($59.62/hour).

[15] This value represents the number of entities that have not already determined a method to weather normalize annual peak actual demand data. We estimate approximately 5 percent of the applicable entities fall into this category.

[16] DP = distribution provider, LSE = load-serving entity, TP = transmission planner and BA = balancing authority, are functions the applicable entities perform in conjunction or individually. We estimate the total number of unique entities performing one or more of these functions to be 561.

Title: Mandatory Reliability Standards for the Bulk-Power System: MOD Reliability Standards.

Action: Proposed FERC-725L.

OMB Control No: 1902-0261

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: One-time and ongoing.

Necessity of the Information: Reliability Standard MOD-031-1, if adopted, would implement the Congressional mandate of the Energy Policy Act of 2005 to develop mandatory and enforceable Reliability Standards to better ensure the reliability of the nation's Bulk-Power System. Specifically, the purpose of the proposed Reliability Standard is to provide authority for applicable entities to collect demand, energy and related data to support reliability studies and assessments and to enumerate the responsibilities and obligations of requestors and respondents of that data.

Internal Review: The Commission has reviewed the requirements pertaining to the proposed Reliability Standard for the Bulk-Power System and determined that the proposed requirements are necessary to meet the statutory provisions of the Energy Policy Act of 2005. These requirements conform to the Commission's plan for efficient information collection, communication and management within the energy industry. The Commission has assured itself, by means of internal review, that there is specific, objective support for the burden estimates associated with the information requirements.

V. Regulatory Flexibility Act Certification

16. The Regulatory Flexibility Act of 1980 (RFA)[17] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities. As shown in the information collection section, the proposed Reliability Standard applies to 561 entities. Comparison of the applicable entities with the Commission's small business data indicates that approximately 249 are small entities.[18] Of these, the Commission estimates that approximately five percent, or twelve of these small entities expect to be affected by the new requirements of the proposed Reliability Standard.[19]

17. Proposed Reliability Standard MOD-031-1 is designed to replace, consolidate and improve upon the Existing MOD C Standards in addressing the collection and aggregation of demand and energy data necessary to support reliability assessments performed by the ERO and Bulk-Power System planners and operators. The reliability of the Bulk-Power System is dependent on having an adequate amount of resources and transmission infrastructure available to serve peak demand while also maintaining a

[17] 5 U.S.C. 601-612 (2012).

[18] The Small Business Administration sets the threshold for what constitutes a small business. Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. The possible categories for the applicable entities have a size threshold ranging from 250 employees to 1,000 employees. For the analysis in this proposed rule, we are using the 1,000 employee threshold for each applicable entity type.

[19] *See* n.15 *supra*.

sufficient margin to address operating events.[20] The Commission estimates that the small entities that will be affected by proposed Reliability Standard MOD-031-1 will incur one-time compliance costs ranging up to $14,309 (i.e. the cost of determining the method of weather normalizing annual peak hour actual demand), plus the annual development of summary narratives in accordance with Requirement R1, Subparts 1.5.4 and 1.5.5, resulting in costs of $477. These costs represent an estimate of the costs a small entity could incur if the entity is identified as an applicable entity; the entity's annual peak hour actual demand varies due to weather-related conditions; and the entity has not yet determined a method for weather normalizing actual demand data. The Commission does not consider the estimated costs per small entity to have a significant economic impact on a substantial number of small entities. Accordingly, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities.

VI. Environmental Analysis

18. 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.[21] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment.

[20] NERC Petition at 2.

[21] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs., Regulations Preambles 1986-1990 ¶ 30,783 (1987).

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.[22] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VII. Comment Procedures

19. 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 after publication in the FEDERAL REGISTER**]. Comments must refer to Docket No. RM14-12-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

20. 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.

21. 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.

22. 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

[22] 18 CFR 380.4(a)(2)(ii).

below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VIII. Document Availability

23. 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 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

24. 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.

25. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at 202-502-6652 (toll free at 1-866-208-3676) or email 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

By direction of the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

OFFICE OF ELECTRIC RELIABILITY

North American Electric Reliability Corporation
Docket No. RD14-13-000

November 4, 2014

North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, D.C. 20005

Attention: Brady A. Walker
Associate Counsel for North American Electric Reliability Corporation

Reference: Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard NUC-001-3

Dear Mr. Walker:

On September 15, 2014, the North American Electric Reliability Corporation (NERC) filed a petition (Petition) seeking approval of the proposed Reliability Standard NUC-001-3 (Nuclear Plant Interface Coordination), the associated implementation plan, violation risk factors and violation security levels, and the retirement of currently-effective Reliability Standard NUC-001-2.1.

Proposed Reliability Standard NUC-001-3 requires coordination between nuclear plant generator operators and transmission entities for the purpose of ensuring safe operation and shutdown of nuclear power plants. The proposed Reliability Standard NUC-001-3 indicates that it is applicable to all nuclear plant generator operators and all transmission entities (including transmission operators, transmission owners, transmission planners, transmission service providers, balancing authorities, reliability coordinators, planning coordinators, distribution providers, load-serving entities, generator owners, and generator operators) that are responsible for providing services related to nuclear plant interface requirements. The Petition states that the proposed Reliability Standard represents the implementation of recommendations made by the five-year review team to revise the currently-effective Reliability Standard

NUC-001-2.1.[1] The Petition further states that the proposed standard includes several improvements, many of which are intended to provide clarity by improving the structure and language over the currently-effective Reliability Standard.[2]

NERC's filing was noticed on September 16, 2014, with interventions, comments and protests due on or before October 15, 2014. Dominion Resources Services, Inc. filed a motion to intervene raising no issues.

NERC's uncontested filing is hereby approved pursuant to the relevant authority delegated to the Director, Office of Electric Reliability under 18 C.F.R. § 375.303 (2014), effective as of the date of this Order.

This action shall not be construed as approving any other application, including proposed revisions of Electric Reliability Organization or Regional Entity rules or procedures pursuant to 18 C.F.R. § 375.303(a)(2)(i). Such action shall not be deemed as recognition of any claimed right or obligation associated therewith and such action is without prejudice to any findings or orders that have been or may hereafter be made by the Commission in any proceeding now pending or hereafter instituted by or against the Electric Reliability Organization or any Regional Entity.

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 (2014).

Sincerely,

Michael Bardee, Director
Office of Electric Reliability

[1] NERC Petition at 6.

[2] *Id.* at. 8.

149 FERC ¶ 61,027
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, Tony Clark,
and Norman C. Bay.

Reliability Standard for Geomagnetic Disturbance Operations — Docket No. RM14-1-001

ORDER NO. 797-A

ORDER DENYING REHEARING

(Issued October 16, 2014)

1. In Order No. 797, the Commission approved Reliability Standard EOP-010-1 (Geomagnetic Disturbance Operations) submitted by the North American Electric Reliability Corporation (NERC).[1] Foundation for Resilient Societies (Foundation) filed a request for rehearing of Order No. 797.[2] For the reasons discussed in the body of this order, we deny rehearing.

2. A number of Foundation's arguments are denied here because they address a later stage of efforts on geomagnetic disturbances (i.e., NERC's future filing of Second Stage GMD Reliability Standards) and Foundation may seek to present those arguments at an appropriate time in response to that filing. More generally, we acknowledge the concerns expressed by Foundation and others that, given the still evolving scientific and engineering knowledge on geomagnetic disturbances (GMDs) and the gaps in understanding of this issue, our decision on the Second Stage GMD Reliability Standards

[1] *Reliability Standard for Geomagnetic Disturbance Operations*, Order No. 797, 79 Fed. Reg. 35,911 (June 25, 2014), 147 FERC ¶ 61,209 (2014).

[2] On August 18, 2014, Foundation moved to supplement its request for rehearing. As Foundation's supplement was filed beyond the 30 days allowed by statute, 16 U.S.C. § 825l(a) (2012), the Federal Power Act does not allow us to consider the supplement here. *See also* 18 C.F.R. § 385.713(b) (2014)*; Public Service Company of New Hampshire*, 134 FERC ¶ 61,041, at P 7 n.13 (2011).

should at least be based on as much information as is currently known and available. In this regard, we expect interested parties to present all relevant information and analyses so our decision can be based on a full record of current knowledge on GMD issues.

I. Background

A. Order No. 779

3. In Order No. 779, the Commission directed NERC, pursuant to section 215(d)(5) of the Federal Power Act (FPA),[3] to develop and submit for approval proposed Reliability Standards that address the impact of GMDs on the reliable operation of the Bulk-Power System.[4] The Commission determined that the potentially severe, wide-spread impact on the reliable operation of the Bulk-Power System that can be caused by GMD events, and the then absence of Reliability Standards to address GMD events, justified the development of Reliability Standards.

4. The Commission ordered NERC to implement the directive in two stages. In the first stage, the Commission directed NERC to submit, within six months of the effective date of Order No. 779, one or more Reliability Standards (First Stage GMD Reliability Standards) that require owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System. The Commission directed that NERC, for the Second Stage GMD Reliability Standard, provide more comprehensive protections by requiring applicable entities to protect their facilities against a benchmark GMD event.

B. NERC Petition

5. On November 13, 2013, NERC petitioned the Commission to approve Reliability Standard EOP-010-1 and its associated violation risk factors and violation severity levels, implementation plan, and effective dates. NERC maintained that Reliability Standard EOP-010-1 satisfied the Commission's directive in Order No. 779 corresponding to the development and submission of the First Stage GMD Reliability Standards.

---

[3] 16 U.S.C. § 824o(d)(5) (2012).

[4] *Reliability Standards for Geomagnetic Disturbances*, Order No. 779, 78 Fed. Reg. 30,747 (May 23, 2013), 143 FERC ¶ 61,147, *reh'g denied*, 144 FERC ¶ 61,113 (2013).

C. NOPR

6. On January 16, 2014, the Commission issued a Notice of Proposed Rulemaking proposing to approve Reliability Standard EOP-010-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest based on the Commission's review of NERC's petition and supporting exhibits.[5] The NOPR stated that Reliability Standard EOP-010-1 satisfied the directive in Order No. 779 that NERC submit one or more Reliability Standards that require owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System.

7. In response to the NOPR, interested entities filed 20 comments.

D. Order No. 797

8. In Order No. 797, the Commission adopted the NOPR proposal to approve Reliability Standard EOP-010-1. The Commission determined that Reliability Standard EOP-010-1 addressed the directive in Order No. 779 that NERC submit one or more Reliability Standards that require owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System. The Commission also determined that the requirements in Reliability Standard EOP-010-1 were consistent with the guidance in Order No. 779 that NERC develop Reliability Standards that, rather than require specific operational procedures, require responsible entities to develop and implement entity-specific operational procedures because owners and operators of the Bulk-Power System are most familiar with their own equipment and system configurations. The Commission further determined that Reliability Standard EOP-010-1 required coordination of operational procedures and processes, overseen by a functional entity with a wide-area perspective (i.e., reliability coordinators), which was also consistent with the Commission's guidance in Order No. 779.

[5] *Reliability Standard for Geomagnetic Disturbance Operations*, Notice of Proposed Rulemaking, 79 Fed. Reg. 3547 (Jan. 22, 2014), 146 FERC ¶ 61,015 (2014) (NOPR).

II. Discussion

9. The Commission denies Foundation's rehearing request, for the reasons discussed below.

A. Applicability Criteria of Reliability Standard EOP-010-1

Order No. 797

10. Reliability Standard EOP-010-1 applies to reliability coordinators and transmission operators with a "Transmission Operator Area that includes a power transformer with a high side wye-grounded winding with terminal voltage greater than 200 kV." In Order No. 797, the Commission determined that the applicability criteria in Reliability Standard EOP-010-1 are technically justified and consistent with Order No. 779, both in terms of using a 200 kV threshold for determining applicable transmission operators and not including balancing authorities and generator operators as applicable entities.[6] Order No. 797 determined that the NERC petition and White Paper Supporting Network Applicability provided an adequate technical basis to conclude that transformers operating at 200 kV and below are likely to have a limited impact on the Bulk-Power System during a GMD event.[7] Order No. 797 also determined that NERC's petition and White Paper Supporting Functional Entity Applicability adequately justified excluding generator operators and balancing authorities from the applicability criteria of Reliability Standard EOP-010-1.[8]

Request

11. Foundation contends that the Commission erred in approving the applicability criteria in Reliability Standard EOP-010-1. Foundation maintains that the 200 kV threshold in the applicability criteria is arbitrary because a report from the Oak Ridge National Laboratory "make[s] the case that networks operating below 200 kV were in

[6] *See* Order No. 797, 147 FERC ¶ 61,209 at PP 16, 24-29 (citing NERC Petition, Exhibit D (White Paper Supporting Network Applicability); NERC Petition, Exhibit E (White Paper Supporting Functional Entity Applicability)).

[7] *See* Order No. 797, 147 FERC ¶ 61,209 at P 25 (citing NERC Petition, Exhibit E (White Paper Supporting Network Applicability)).

[8] *See* Order No. 797, 147 FERC ¶ 61,209 at PP 28-29 (citing NERC Petition, Exhibit E (White Paper Supporting Functional Entity Applicability)).

fact impacted by a moderate solar storm on March 13, 1989."[9] Foundation also cites to "PowerWorld modeling results," discussed in Foundation's NOPR comment, that, according to Foundation, show that "reactive power in networks at 200 kV and above left out more than 40 percent of cumulative reactive power (MVAR) consumed in solar storm modeling scenarios for some regions."[10]

12. In addition, Foundation contends that the 200 kV threshold is inconsistent with the 100 kV threshold in the Commission-approved definition of bulk electric system. Foundation also asserts that the applicability criteria improperly exclude balancing authorities and generator operators because Reliability Standard EOP-010-1 unreasonably relies on reliability coordinators to perform certain functions that reliability coordinators are unlikely to be able to perform. Foundation further contends that the exclusion of generator operators from the applicability criteria, and the lack of geomagnetic induced current monitoring and blocking requirements, does not "assure reliable 'black start' for all nuclear generating facilities."[11]

Commission Determination

13. We deny Foundation's rehearing requests regarding the applicability criteria of Reliability Standard EOP-010-1.

---

[9] Foundation Rehearing Request at 5 (citing Oak Ridge National Laboratory, Electromagnetic Pulse: Effects on the U.S. Power Grid: Meta-R-319 (January 2010), *available at* http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-319.pdf (Oak Ridge Report)).

[10] Foundation Rehearing Request at 5. Foundation also argues that excluding balancing authorities is unreasonable because a report from the Electric Infrastructure Council (EIS) "indicates above-average risks of regional blackouts from solar storms in high latitude nations such as Canada." Foundation Comments at 15. Foundation did not address the EIS report in its NOPR comments. Moreover, the pages in the EIS report cited by Foundation only include a survey of GMD regulations and mitigation efforts in various countries, but do not address whether balancing authorities should be added to the applicable entities under Reliability Standard EOP-010-1. Electric Infrastructure Council, The International E-Pro Report (September 2013) at 117-118, *available at* http://eiscouncil.org/images/upload/media/The%20International%20EPRO%20Report.pdf.

[11] Foundation Rehearing Request at 18.

14. We first deny Foundation's request for rehearing of the 200 kV threshold in the applicability criteria of Reliability Standard EOP-010-1.[12] Order No. 797 determined that NERC's petition and White Paper Supporting Network Applicability "provide[d] an adequate technical basis to conclude that transformers operating at 200 kV and below are likely to have a limited impact on the Bulk-Power System during a GMD event."[13] Foundation does not contest the data in NERC's White Paper Supporting Network Applicability. Instead, Foundation contends that even a limited impact on the Bulk-Power System is inconsistent with the definition of "reliable operation" in FPA section 215 because "reliable operation" means that the Bulk-Power System must be operated so that "instability uncontrolled separation, or cascading failures of such system will not occur…." However, the Commission held in Order No. 779 that the "Second Stage GMD Reliability Standard should not impose 'strict liability' on responsible entities for failure to ensure the reliable operation of the Bulk-Power System in the face of a GMD event of unforeseen severity, as some commenters fear."[14] In addition, the "limited impact" discussed in Order No. 797 referred to the modelling analysis described in the White Paper Supporting Network Applicability, which showed only a minimal difference in geomagnetic induced current levels on transformers operating at voltages higher than 200 kV when transformers operating at 200 kV and below were excluded from the model.[15] Thus, the White Paper reasonably demonstrated that the exclusion of

[12] As the Commission noted in Order No. 797, the applicability criteria determine which transmission operators must comply with Reliability Standard EOP-010-1 (i.e., those with a power transformer with a high side wye-grounded winding with terminal voltage greater than 200 kV in the transmission operator area). Order No. 797, 147 FERC ¶ 61,209 at P 26. While the 200 kV threshold excludes transmission operators operating transformers 200 kV and below, the 200 kV threshold does not mean that applicable transmission operators will ignore reactive power supplies operating at 200 kV or below on their systems when developing the required GMD Operating Procedures or Operating Processes. *Id.*

[13] Order No. 797, 147 FERC ¶ 61,209 at P 25.

[14] Order No. 779, 143 FERC ¶ 61,147 at P 84.

[15] Order No. 797, 147 FERC ¶ 61,209 at P 27.

transformers operating at 200 kV or below on factors such as maximum transformer geomagnetic induced current, average transformer geomagnetic induced current, maximum VAR absorption and average VAR absorption was minimal.[16]

15. We also disagree with Foundation's assertion that the 200 kV applicability threshold is inconsistent with the Commission-approved definition of bulk electric system. Foundation misconstrues the purpose of the bulk electric system definition. The bulk electric system definition is the first step in determining what entities are subject to a NERC Reliability Standard. As the Commission stated in Order No. 693, the "[Electric Reliability Organization (ERO)] will identify those entities that must comply with Reliability Standards in three steps: (1) the ERO will identify and register those entities that fall under its definition of bulk electric system; (2) each registered entity will register in one or more appropriate functional categories and (3) each registered entity will comply with those Reliability Standards applicable to the functional categories in which it is registered." [17] In addition, Order No. 693 contemplated the use of electric facility characteristics to further refine the types of registered entities subject to Reliability

[16] Regarding Foundation's reference to the "PowerWorld modeling results," Foundation's NOPR comment only references PowerWorld in Appendix 1 (Comments of the Foundation for Resilient Societies relating to Proposed Standards for "Operating Procedures" to protect the bulk power system from geomagnetic disturbances – Proposed NERC Standard EOP-010-1) where Foundation states, without citation, that "PowerWorld has estimated that less than 60% of total MVAR enters the bulk power system through transformers at 230 kV or higher, in both New England and in Michigan." Foundation NOPR Comments at Appendix A1-5. This statement, however, does not support Foundation's argument that the 200 kV applicability threshold for transformers in Reliability Standard EOP-010-1 is arbitrary. Foundation's rehearing request also cites to the Oak Ridge Report, but the two cited pages do not support Foundation's rehearing request. Page 4-12 of the Oak Ridge Report addresses extra high-voltage (EHV) transformers operating at 765 kV, 500 kV, or 345 kV; it does not refer to transformers operating between 100 kV and 200 kV. Similarly, page 2-30 of the Oak Ridge Report only discusses GMD-related damage to a transformer operating at 500 kV.

[17] Order No. 797, 147 FERC ¶ 61,209 at P 25 n.36 (citing *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at PP 97-98, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007) (explaining that each Reliability Standard will identify the set of users, owners and operators that must comply with that standard and "NERC has indicated that in the future it may add to a Reliability Standard limitations on applicability based on electric facility characteristics such as generator nameplate ratings.")).

Standards. Since Order No. 693, the Commission has approved the use of electric facility characteristics in other NERC Reliability Standards. For example, the Reliability Standard on vegetation management also contains a 200 kV threshold.[18]

16. We next deny Foundation's request for rehearing regarding the exclusion of balancing authorities and generator operators from the applicability criteria of Reliability Standard EOP-010-1. In Order No. 797, the Commission considered and rejected Foundation's comment that balancing authorities should be listed as applicable entities because reliability coordinators allegedly cannot communicate quickly with transmission operators, generator operators, and balancing authorities. The Commission, citing NERC's Reliability Functional Model Technical Document and Reliability Standard COM-002-2, Requirement R1, stated that reliability coordinators are responsible for real-time system reliability and often must respond quickly or even immediately to Bulk-Power System events with little or no warning.[19] The Commission determined that there was no evidence from which to conclude that, unlike with other types of disturbances on the Bulk-Power System, reliability coordinators could not respond to a GMD event.

17. Foundation's rehearing request provides no basis to revisit that determination. Citing Reliability Standard IRO-001-1.1, Requirement R8, Foundation in its rehearing request, contends that the "likelihood that [generator operators and balancing authorities] will reliably execute the directives of Reliability Coordinators during fast-moving and wide-area solar storms is greatly diminished" because the Reliability Standard "allows Transmission Operators, Balancing Authorities, and Generator Operators to ignore the directives of Reliability Coordinators" under certain conditions.[20] However, Reliability

---

[18] *See Revisions to Reliability Standard for Transmission Vegetation Management*, Order No. 777, 78 Fed. Reg. 18,817 (Mar. 28, 2013), 142 FERC ¶ 61,208 (2013) (approving the use of a 200 kV applicability threshold in Reliability Standard FAC-003-2); *see also Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013) (approving the use of electric facility characteristics in the applicability criteria of Reliability Standard CIP-002-5).

[19] Order No. 797, 147 FERC ¶ 61,209 at P 28 (citing Reliability Standard COM-002-2, Requirement R1 ("Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators … [and] [s]uch communications shall be staffed and available for addressing a real-time emergency condition.)).

[20] Foundation Rehearing Request at 14.

Standard IRO-001-1.1, Requirement R8 does not allow transmission operators, balancing authorities, and generator operators to ignore a reliability coordinator's directives. Reliability Standard IRO-001-1.1, Requirement R8 provides that generator operators, transmission operators and balancing authorities, among other entities, "shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements." In instances where compliance with a reliability coordinator's directive violates safety, equipment, or regulatory or statutory requirements, generator operators, transmission operators and balancing authorities cannot simply ignore the directive but, instead, "shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions."

18. We also reject Foundation's assertion that two-way communications between reliability coordinators and generator operators would be unreliable during a GMD event. In Order No. 797, the Commission stated that Reliability Standard COM-002-2, Requirement R1 requires reliability coordinators, transmission operators, balancing authorities, generator operators, and reliability coordinators to have the technical capacity to communicate and coordinate with each other. We are not persuaded that reliability coordinators and generator operators could not comply with this requirement during a GMD event. To support its position regarding the alleged unreliability of two-way communications during a GMD event, Foundation cites Order No. 779, which only stated, by way of background, that GMD events in the past have "impacted" communication systems.[21] Foundation also cites a report addressing man-made electromagnetic pulses, which, as we stated in Order No. 797, are not at issue in this

[21] Order No. 779, 143 FERC ¶ 61,147 at P 6 (citing Oak Ridge National Laboratory, Electric Utility Industry Experience with Geomagnetic Disturbances at xiii (1991), *available at* http://www.ornl.gov/~webworks/cpr/v823/rpt/51089.pdf ("This disturbance, which results in distortions to the earth's magnetic field, can be of varying intensity and has in the past impacted the operation of pipelines, communications systems, and electric power systems.")).

rulemaking.[22] Even recognizing that GMD events could impact communication systems, Foundation has not established that reliability coordinators and generator operators would be unable to comply with Reliability Standard COM-002-2, Requirement R1 during a GMD event.

19. We further reject Foundation's contention that generator operators should be included within the scope Reliability Standard EOP-010-1 to ensure that sufficient black start resources exist to "bring back nuclear operations in time to safeguard radioactive materials."[23] In Order No. 797, the Commission credited NERC's justification for the exclusion of generator operators because some generator operators "would not have the technical basis for taking steps [to mitigate GMDs] on [their] own and would instead take steps based on the [reliability coordinator's] or [transmission operator's] Operating Plans, Processes, or Procedures."[24] Foundation does not contest that determination. Instead, Foundation appears to link the inclusion of generator operators in the applicability criteria of Reliability Standard EOP-010-1with the adoption of additional requirements that generator operators perform mandatory geomagnetic induced current monitoring and blocking. As discussed below, we believe that such requirements would be inconsistent with the Commission's guidance in Order No. 779 regarding the First Stage GMD Reliability Standards.[25]

---

[22] Foundation Rehearing Request at 19 (citing Report of the EMP Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures (April 2008) at 43 ("The communications and control systems' functionality are at high risk of disruption and damage themselves during an EMP attack.")); Order No. 779, 143 FERC ¶ 61,147 at P 14 n.20 (determining that the impact of electromagnetic pulses was outside the scope of Order No. 779).

[23] Foundation Rehearing Request at 18.

[24] Order No. 797, 147 FERC ¶ 61,209 at P 16 (citing NERC Petition at 4).

[25] In Order No. 797, the Commission also recognized NERC's statement that generator owners and generator operators will be considered for inclusion in the Second Stage GMD Reliability Standards, "which will require applicable entities to conduct vulnerability assessment and develop appropriate mitigation strategies . . . [and that] [s]uch mitigation strategies could include the development of Operating Procedures for applicable [generator owners] and [generator operators]." *Id.* We also note that the Nuclear Regulatory Commission has the statutory responsibility for licensing and regulating commercial nuclear facilities operating in the United States. *See* 42 U.S.C. § 5801 *et seq.*

20. In sum, we deny Foundation's request for rehearing concerning the applicability criteria of Reliability Standard EOP-010-1.

B. Requirements of Reliability Standard EOP-010-1

Order No. 797

21. In Order No. 797, the Commission determined that Reliability Standard EOP-010-1 satisfied the directive in Order No. 779 that NERC submit one or more Reliability Standards that require owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System. The Commission also determined that the requirements in Reliability Standard EOP-010-1 are consistent with the guidance in Order No. 779 that NERC develop Reliability Standards that, rather than require specific operational procedures, require responsible entities to develop and implement entity-specific operational procedures because owners and operators of the Bulk-Power System are most familiar with their own equipment and system configurations. Further, the Commission determined that Reliability Standard EOP-010-1 required coordination of operational procedures and processes, overseen by a functional entity with a wide-area perspective (i.e., reliability coordinators), which was also consistent with the guidance in Order No. 779.[26]

Request

22. Foundation contends that the Commission erred in approving the requirements of Reliability Standard EOP-010-1. First, Foundation characterizes Reliability Standard EOP-010-1 as a "lowest common denominator" Reliability Standard because it lacks specific requirements such as "mandatory exercises, unscheduled drills, authentication of de-energizing orders, or practice of GMD operating procedures."[27] Second, Foundation contends that Order No. 797 failed to address Foundation's NOPR comments regarding the "lack of mandatory mitigative actions and lack of mandatory external review of GMD Operating Plans of Reliability Coordinators" in Reliability Standard EOP-010-1. Third, Foundation contends that the Commission erred in not requiring the installation of geomagnetic induced current monitoring and blocking devices in Reliability Standard EOP-010-1. Fourth, Foundation contends that the Commission erred by relying on a future Second Phase GMD Reliability Standard to correct the alleged defects with Reliability Standard EOP-010-1. Fifth, Foundation contends that the Commission erred

[26] *Id.* P 14.

[27] Foundation Rehearing Request at 3.

by not requiring applicable entities to conduct "quantified contingency planning," which Foundation defines as a "mathematical comparison of megawatt capacity of assets at risk during solar storms to power reserves."[28] Sixth, Foundation contends that the Commission erred by not requiring "failover responsibility" between generator operators and transmission operators.

Commission Determination

23. We deny Foundation's rehearing request regarding the requirements of Reliability Standard EOP-010-1.

24. In Order No. 779, the Commission directed NERC to develop First Stage GMD Reliability Standards that require applicable entities to mitigate the risks posed by GMD events to the Bulk-Power System by developing and implementing GMD operational procedures. In doing so, the Commission stated that:

> As we stated in the NOPR, "operational procedures, while not a complete solution, constitute[] an important first step to addressing the GMD reliability gap because they can be implemented relatively quickly." Operational procedures may help alleviate abnormal system conditions due to transformer absorption of reactive power during GMD events, helping to stabilize system voltage swings, and may potentially isolate some equipment from being damaged or misoperated.[29]

25. The Commission provided guidance to NERC as to what should be included in the First Stage GMD Reliability Standards. Specifically, the Commission stated that it was "not directing NERC to develop Reliability Standards that include specific operational procedures … [but instead the First Stage GMD Reliability Standards] should include a mechanism that requires responsible entities to develop and implement operational procedures because owners and operators of the Bulk-Power System are most familiar with their own equipment and system configurations."[30] Accordingly, the Commission's expectations regarding the First Stage GMD Reliability Standards were clearly set forth in Order No. 779. While Foundation filed comments in the Order No. 779 rulemaking process, Foundation did not seek rehearing of Order No. 779.

---

[28] *Id.* at 12.

[29] Order No. 779, 143 FERC ¶ 61,147 at P 36.

[30] *Id.* P 38.

26. Foundation's rehearing request regarding the requirements of Reliability Standard EOP-010-1 rests on a disagreement with the guidance in Order No. 779 that the First Stage GMD Reliability Standards should not require specific operational procedures that all applicable entities must follow. This disagreement is reflected in Foundation's contention that Reliability Standard EOP-010-1 should require applicable entities to implement specific operational procedures (e.g., mandatory exercises, unscheduled drills, "failover responsibility," "quantified contingency planning") and install equipment (e.g., geomagnetic induced current monitoring or blocking equipment). However, such requirements would be inconsistent with the Commission's explanation in Order No. 779 stating that the First Stage GMD Reliability Standards should not contain specific, "one-size-fits-all" operating procedures.[31] Instead, Order No. 779 stated that the First Stage GMD Reliability Standards should "include a mechanism that requires responsible entities to develop and implement operational procedures because owners and operators of the Bulk-Power System are most familiar with their own equipment and system configurations."[32]

27. Foundation contends that the Commission "has established a system of solar storm mitigation that might work for minor solar storms but it is altogether unworkable, unreasonable, imprudent, and unjust to utilize this design for 'operating procedures' in a severe solar storm."[33] However, we believe that Foundation's concern is better addressed in the Second Stage GMD Reliability Standard development process, in which NERC is developing a Reliability Standard that must identify "benchmark GMD events" that specify what severity GMD events a responsible entity must assess for potential impact

[31] For the same reason, we reject Foundation's contention that the GMD operational procedure templates for transmission operators and generator operators, developed by the NERC GMD Task Force, should have been included as requirements in Reliability Standard EOP-010-1. NERC, Geomagnetic Disturbance Operating Procedure Template Transmission Operator, *available at* http://www.nerc.com/docs/pc/gmdtf /Template_ TOP.pdf. While it is reasonable to anticipate that applicable transmission operators will use the transmission operator template as a reference in developing their own operational procedures, we see no reason why that reference should have been included in the requirements of Reliability Standard EOP-010-1.

[32] Order No. 779, 143 FERC ¶ 61,147 at P 38.

[33] Foundation Rehearing Request at 9-10.

on the Bulk-Power System.[34] Further, while Foundation suggests that the Commission meant for the First Stage GMD Reliability Standards to address a "severe solar storm," that was not the case. Rather, in the absence at that time of any mandatory and enforceable Reliability Standards addressing GMD events, the Commission directed NERC in Order No. 779 to develop Reliability Standards that address the risks posed by GMD to the reliable operation of the Bulk-Power System in two stages. With regard to the First Stage GMD Reliability Standards (i.e., the development of operational procedures), the Commission stated that "operational procedures, while not a complete solution, constitute an important first step to addressing the GMD reliability gap because they can be implemented relatively quickly."[35] The Commission expects the Second Stage GMD Reliability Standards, which the Commission allowed NERC more time to develop given its greater complexity, to provide more comprehensive protections by requiring applicable entities to protect their facilities against a benchmark GMD event.[36] Regarding geomagnetic induced current monitoring specifically, in Order No. 797 the Commission determined that geomagnetic induced current monitoring requirements should be addressed in the Second Stage GMD Reliability Standards.[37] We continue to

[34] Order No. 779, 143 FERC ¶ 61,147 at P 54. Foundation contends that the Commission erred by allowing defects in Reliability Standard EOP-010-1 (e.g., the lack of required geomagnetic induced current monitoring) to be remedied in the Second Stage GMD Reliability Standards. As noted above, the lack of specific operational procedures in the First Stage GMD Reliability Standards is not a defect; instead, it is consistent with the Commission's guidance in Order No. 797. Moreover, as noted in Order No, 797, the Commission's approval of Reliability Standard EOP-010-1 was not dependent on what the Commission expected NERC to propose in the Second Stage GMD Reliability Standards. Order No. 797, 147 FERC ¶ 61,209 at P 29 n.47. Moreover, in Order No. 797, the Commission stated that it would "also consider then the need for the Second Stage GMD Reliability Standard's planning requirements to integrate appropriately with the First Stage GMD Reliability Standard's operating requirements." *Id.* P 36 n.52.

[35] Order No. 779, 143 FERC ¶ 61,147 at P 36.

[36] The Commission noted that "[g]iven that the scientific understanding of GMDs is still evolving, we recognize that Reliability Standards cannot be expected to protect against all GMD-induced outages." Order No. 797, 147 FERC ¶ 61,209 at P 84.

[37] Order No. 797, 147 FERC ¶ 61,209 at P 36 ("[W]e directed NERC to develop only operational procedures in the First Stage GMD Reliability Standards, and to develop more comprehensive protections in the Second Stage GMD Reliability Standards. The issue of monitoring requirements properly belongs in the Second Stage GMD Reliability Standards.").

encourage NERC to address the collection, dissemination, and use of geomagnetic induced current data, by NERC, industry or others, in the Second Stage GMD Reliability Standards because such efforts could be useful in the development of GMD mitigation methods or to validate GMD models.

28. We reject Foundation's assertion that Reliability Standard EOP-010-1 lacks "mandatory mitigative actions" or "mandatory external review" because it lacks requirements for "mandatory exercises, unscheduled drills, authentication of de-energizing orders, or practice of GMD operating procedures."[38] While, as discussed above, Reliability Standard EOP-010-1 does not require specific operational procedures, Foundation's assertion that there are no "mitigative actions" or "mandatory external review" is contradicted by the requirements and compliance measures contained in the Reliability Standard. Reliability Standard EOP-010-1, Requirement R1 requires that "[e]ach Reliability Coordinator shall develop, maintain, and implement a GMD Operating Plan that coordinates GMD Operating Procedures or Operating Processes within its Reliability Coordinator Area." Reliability Standard EOP-010-1, Requirement R3 requires that "[e]ach Transmission Operator shall develop, maintain, and implement a GMD Operating Procedure or Operating Process to mitigate the effects of GMD events on the reliable operation of its respective system." Each of these requirements has associated compliance measures to provide the compliance enforcement authority with proof of compliance. For Requirement R1, Measure M1 states that "[e]ach Reliability Coordinator shall have a current GMD Operating Plan meeting all the provisions of Requirement R1; evidence such as a review or revision history to indicate that the GMD Operating Plan has been maintained; and evidence to show that the plan was implemented as called for in its GMD Operating Plan, such as dated operator logs, voice recordings, or voice transcripts." For Requirement R3, Measure 3 states that "[e]ach Transmission Operator shall have a GMD Operating Procedure or Operating Process meeting all the provisions of Requirement R3; evidence such as a review or revision history to indicate that the GMD Operating Procedure or Operating Process has been maintained; and evidence to show that the Operating Procedure or Operating Process was implemented as called for in its GMD Operating Procedure or Operating Process, such as dated operator logs, voice recordings, or voice transcripts." We believe that NERC and Regional Entities possess the necessary technical expertise to review and ensure compliance with the requirements and measures in Reliability Standard EOP-010-1. Accordingly, we reject Foundation's assertion that Reliability Standard EOP-010-1 lacks "mandatory mitigative actions" or "mandatory external review."

[38] Foundation Rehearing Request at 3.

29. With respect to Foundation's contention that Reliability Standard EOP-010-1 should "include provisions for failover responsibilities vesting in Generator Operators and Transmission Operators in their area," we note that Foundation does not explain what it means or proposes by recommending the inclusion of "failover responsibilities," nor did Foundation raise this issue in its NOPR comments.[39] In any case, as discussed above, Reliability Standard EOP-010-1 vests reliability coordinators with the responsibility of coordinating the GMD Operating Procedures or Operating Processes within its Reliability Coordinator Area, consistent with the Commission's guidance in Order No. 779. Thus, we deny Foundation's request for rehearing with respect to this issue.

30. In sum, we deny Foundation's request for rehearing concerning the requirements of Reliability Standard EOP-010-1.

C. Other Alleged Errors

Request

31. Foundation contends that Reliability Standard EOP-010-1 interferes with the authority of the President of the United States and Secretary of Energy. Foundation states that Reliability Standard EOP-010-1 "excludes Generator Operators and Balancing Authorities from mandatory participation; reduces incentives to install and operate geomagnetic induced current monitors; and makes it impractical and perhaps impossible for the President of the United States to exercise existing statutory and constitutional authority to protect the nation from a severe solar storm under existing Article II powers and specific statutory authorities."[40] Foundation also contends that excluding generator operators "from mandatory participation in 'operating procedures' to mitigate solar geomagnetic storms … [and] avoiding a mandate for cost-effective geomagnetic induced current monitoring at [generator step up (GSU)] transformers and key interconnections in the transmission networks of the Bulk-Power System[] creates barriers to effective use by

[39] *Transmission Relay Loadability Reliability Standard*, Order No. 733, 130 FERC ¶ 61,221 (2010), *order on reh'g and clarification*, Order No. 733-A, 134 FERC ¶ 61,127, *order on reh'g and clarification*, Order No. 733-B, 136 FERC ¶ 61,185, at P 57 (2011) (stating that the Commission looks with disfavor on parties raising issues for the first time on rehearing because other parties are not permitted to respond to a request for rehearing).

[40] Foundation Rehearing Request at 16.

the Secretary of Energy of pre-existing emergency interconnection authority [under FPA section 202(c)]."[41]

32. Foundation also contends that the Commission erred by "deferring to NERC on allegations of anti-competitive rulemaking[] and by creating barriers to competition to deliver higher reliability electric transmission services … by effectively grant[ing] Generator Operators a shield against financial liability for failure to participate in GMD operating procedures."[42] Foundation maintains that not requiring the use of geomagnetic induced current monitoring or blocking equipment "discourage[s] [the] purchase of hardware protective equipment for GMD, and [] discourage[s] installation of geomagnetic induced current monitors at all GSU transformers and other GMD-impacted equipment … [with] [t]he indirect impact of these barriers to solar storm protection [being] to render difficult or impossible the competition by one or more transmission companies that may wish to compete to provide higher standards of grid reliability."[43]

Commission Determination

33. We deny Foundation's rehearing request based on Foundation's assertion that Reliability Standard EOP-010-1 might interfere with any authority of the President of the United States and Secretary of Energy, or that Reliability Standard EOP-010-1 creates "anti-competitive barriers" in not requiring the installation of geomagnetic induced current monitoring or blocking equipment.

34. In Order No. 797, the Commission approved Reliability Standard EOP-010-1 pursuant to the Commission's authority under FPA section 215(d)(2). Reliability Standard EOP-010-1 contains no provision that purports to impair any authority of the President of the United States or Secretary of Energy. Foundations' assertion that the requirements of Reliability Standard EOP-010-1, or in this case the lack of specific requirements (i.e., not requiring geomagnetic induced current monitoring or blocking), might discourage the President or Secretary of Energy from exercising any authority is speculative and largely immaterial to the Commission's responsibility to review Reliability Standards pursuant to FPA section 215(d)(2). In addition, we find inadequate support for, and therefore, reject Foundation's claim that the lack of a geomagnetic induced current monitoring or blocking requirement in Reliability Standard EOP-010-1 creates "anti-competitive barriers." As the Commission stated in Order No. 797,

[41] *Id.* at 17.

[42] *Id.* at 20.

[43] *Id.*

"Reliability Standard EOP-010-1 does not preclude users, owners and operators of the Bulk-Power System from taking additional steps that are designed to mitigate the effects of GMD events, provided those additional steps are not inconsistent with the Commission-approved Reliability Standards."[44]

The Commission orders:

The Commission hereby denies rehearing, for the reasons discussed in the body of this order.

By the Commission.

Kimberly D. Bose,
Secretary.

[44] Order No. 797, 147 FERC ¶ 61,209 at P 44.

148 FERC ¶ 61,252
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, Tony Clark,
and Norman C. Bay.

North American Electric Reliability Corporation Docket No. RR13-9-003

ORDER APPROVING SPECIAL ASSESSMENT
FOR PEAK RELIABILITY, INC.

(Issued September 30, 2014)

1. On July 23, 2014, North American Electric Reliability Corporation (NERC) filed a supplemental funding request seeking authority to collect a special assessment to fund the 2014 operations of Peak Reliability, Inc. (Peak Reliability). For the reasons discussed in the body of this order, we approve the special assessment requested by NERC. We also direct Peak Reliability to submit certain informational filings, as discussed below.

I. Background

A. Regulatory History

2. Section 215 of the Federal Power Act (FPA) requires the Commission to certify an Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[1] In July 2006, the Commission certified NERC as the ERO.[2]

[1] 16 U.S.C. § 824o (2012).

[2] *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).

3. FPA section 215(c)(2)(B) provides that the ERO must have rules that "allocate equitably reasonable dues, fees, and other charges among end users for all activities under this section."[3]

B. Peak Reliability 2014 Business Plan and Budget

4. On August 23, 2013, NERC filed the 2014 business plans and budgets for itself; each Regional Entity, including the Western Electricity Coordinating Council (WECC); Western Interconnection Regional Advisory Body; and Peak Reliability.[4]

5. On November 1, 2013, the Commission issued an order, *inter alia*, conditionally accepting the 2014 business plan and budget of Peak Reliability.[5] In that order, the Commission did not authorize Peak Reliability to issue invoices to fund its 2014 operations pending resolution of the WECC bifurcation proceedings in Docket Nos. EL13-52-001, RR13-10-000, and RR13-12-000.[6] On February 12, 2014, the Commission issued an order on compliance approving the bifurcation of WECC and Peak Reliability and authorizing Peak Reliability to issue billing invoices to fund its fiscal 2014 operations consistent with the 2014 Budget Order.[7]

II. Notice and Responsive Pleadings

6. Notice of NERC's July 23, 2014 filing was published in the *Federal Register*, 79 Fed. Reg. 44,761 (2014), with interventions and protests due on or before August 22, 2014. On July 25, 2014, the Commission issued an errata notice shortening the comment due date to August 13, 2014. No comments or protests were received.

---

[3] 16 U.S.C. § 824o(c)(2)(B).

[4] At the time of that proceeding, Peak Reliability was referred to as the Reliability Coordination Company or RC Company.

[5] *North American Electric Reliability Corp.*, 145 FERC ¶ 61,097, at PP 34-35 (2013) (2014 Budget Order).

[6] *Id.*

[7] *North American Electric Reliability Corp.*, 145 FERC ¶ 61,202 (2013), *order on compliance*, 146 FERC ¶ 61,092, at ordering para. (C), *reh'g denied*, 147 FERC ¶ 61,064 (2014).

III. Discussion

7. NERC requests authority to collect a special assessment of $4,030,696 from load-serving entities and designees in the United States portion of the WECC region to fund the 2014 budget of Peak Reliability.[8] NERC maintains that the special assessment is necessary because two Canadian entities, Alberta Electricity System Operator (AESO) and British Columbia Hydro & Power Authority (BC Hydro), have not paid their allocated assessments.[9] NERC contends that the resulting shortfall in funding was unforeseen in 2013, when Peak Reliability's 2014 budget was being developed for submission to the Commission. NERC also contends that the special assessment is warranted to "allow Peak to collect its full approved 2014 assessment and ensure that Peak will have sufficient funding to carry out its [reliability coordinator] and [interchange authority] responsibilities within the Western Interconnection throughout 2014."[10]

8. NERC states that AESO advised Peak Reliability in August 2013 that AESO intended to provide its own reliability coordinator and interchange authority functions effective January 1, 2014.[11] NERC also states that BC Hydro advised Peak Reliability in June 2014 that BC Hydro was "willing to negotiate an agreement for Peak to continue to provide some [reliability coordinator] and [interchange authority] services for the BC Hydro footprint."[12] NERC maintains that, prior to filing this petition, NERC discussed

---

[8] NERC's request is made pursuant to 18 C.F.R. § 39.4(d):

> (d) On a demonstration of unforeseen and extraordinary circumstances requiring additional funds prior to the next [ERO] fiscal year, the [ERO] may file with the Commission for authorization to collect a special assessment. Such filing shall include supporting materials explaining the proposed collection in sufficient detail to justify the requested funding…

[9] NERC states that the uncollected assessments from AESO and BC Hydro total $4,094,340, which constitutes 13.8 percent of Peak Reliability's total 2014 assessment and 12.4 percent of Peak Reliability's total Commission-approved 2014 budget. NERC Petition at 1. NERC states that the difference between the uncollected assessments and the special assessment on load-serving entities in the United States (i.e., $63,644) will be allocated to load-serving entities in the Mexico portion of the WECC region. *Id.* at 3.

[10] *Id.* at 13.

[11] These services were formerly provided by WECC as the reliability coordinator, Peak Reliability's predecessor entity.

[12] NERC Petition at 2.

these issues with Peak Reliability, AESO, and BC Hydro. NERC states that it was advised that Peak Reliability has had ongoing discussions with AESO and BC Hydro "to attempt to reach agreements with each of these entities as to what services and tools, if any, Peak will provide to the AESO and to BC Hydro and what payments the AESO and BC Hydro will make to Peak."[13] NERC represents that no agreement was reached as of the filing date of this petition.

9. According to NERC, Peak Reliability states that "it is not able to effectuate any material reductions in its budgeted 2014 costs in the short term, particularly given the ongoing negotiations and the unknown scope of Peak's ultimate [reliability coordinator] and [interchange authority] responsibilities for the AESO and BC Hydro footprints."[14] NERC concludes that "[b]ased on the information provided to NERC by Peak or otherwise available to NERC, it appears to NERC that, at this juncture, Peak's ability to sustain its operations through the end of 2014 without an infusion of funding to substantially replace the assessments that have not been collected is in question."[15]

10. While NERC contends that a special assessment to replace Peak Reliability's 2014 funding shortfall is necessary, NERC proposes three Commission actions related to the funding request. First, NERC proposes that, by October 31, 2014, Peak Reliability should submit to the Commission a report that summarizes the progress of Peak Reliability's discussions with AESO and BC Hydro and that presents Peak Reliability's plan for reducing the scope of its operations and its costs going forward under the assumption that AESO and BC Hydro do not pay their assessments or pay less than the full amount. Second, NERC proposes that if Peak Reliability has not reached agreements with AESO and BC Hydro by October 31, 2014, Peak Reliability should submit quarterly status reports until agreements are reached. Third, NERC proposes that if Peak Reliability receives any compensation from AESO or BC Hydro for 2014, Peak Reliability should be required to use the amount received as a funding source to reduce its requested assessment in the next year for which it submits a budget.

[13] *Id.* at 9.

[14] *Id.* at 10.

[15] *Id.* at 9-10. According to NERC, Peak Reliability represented that it would have to replace the uncollected assessment revenue "by about mid-November in order to have sufficient funds to continue its operations through the end of 2014." *Id.* at 3.

Commission Determination

11. We approve NERC's request for authority to collect a $4,030,696 special assessment from load-serving entities and designees in the United States portion of the WECC region to fund the 2014 budget of Peak Reliability. Based on the record before us, we find that NERC has demonstrated that Peak Reliability's inability to collect the budgeted assessments from AESO and BC Hydro and the resulting funding shortfall constitute "unforeseen and extraordinary circumstances requiring additional funds prior to the next [ERO] fiscal year."[16]

12. While we approve NERC's request for a special assessment to fund the 2014 operations of Peak Reliability, we also agree with and adopt NERC's proposals. To keep the Commission apprised of the ongoing negotiations between Peak Reliability, AESO, and BC Hydro, we direct Peak Reliability to submit an informational filing by October 31, 2014 that summarizes the progress of Peak Reliability's discussions with AESO and BC Hydro and explains Peak Reliability's plan for reducing the scope of its operations and its costs going forward under the assumption that AESO and BC Hydro do not pay their assessments or pay less than the full amount. If Peak Reliability does not reach agreements with AESO and BC Hydro by October 31, 2014, we direct Peak Reliability to submit informational quarterly status reports until agreements are reached.

13. We also direct that, if Peak Reliability receives any compensation from AESO or BC Hydro for 2014, Peak Reliability use the amount received as a funding source to reduce its requested assessment in the next year for which it submits a budget.[17]

The Commission orders:

(A) NERC's request for authority to collect a special assessment on load-serving entities in the United States portion of the WECC region to fund the 2014 operations of Peak Reliability is hereby approved, as discussed in the body of this order.

(B) Peak Reliability is directed to submit the informational filings, as discussed in the body of this order.

[16] 18 C.F.R. § 39.4(d) (2014).

[17] *See* NERC Petition at 4 and 15.

(C) Peak Reliability is directed to use any compensation received from AESO or BC Hydro as a funding source to reduce its requested assessment in the next year for which it submits a budget, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

149 FERC ¶ 61,028
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, Tony Clark,
and Norman C. Bay.

North American Electric Reliability Corporation Docket No. RR14-6-000

ORDER ON 2015 BUSINESS PLANS AND BUDGETS

(Issued October 16, 2014)

1. On August 22, 2014, North American Electric Reliability Corporation (NERC) filed 2015 business plans and budgets for each Regional Entity,[1] the Western Interconnection Regional Advisory Body (WIRAB), Peak Reliability, Inc. (Peak Reliability), and itself (collectively, NERC Application). For the reasons discussed below, the Commission accepts the 2015 business plans and budgets of NERC, the Regional Entities, WIRAB, and Peak Reliability, as well as the associated attachments and updates. The Commission authorizes NERC to issue billing invoices to fund the fiscal year 2015 operations of the Regional Entities, WIRAB, Peak Reliability, and itself.[2]

I. Background

A. Regulatory History

2. Section 215 of the Federal Power Act (FPA) requires the Commission to certify an Electric Reliability Organization (ERO) to develop mandatory and enforceable

[1] The eight Regional Entities are Florida Reliability Coordinating Council, Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., Reliability*First* Corporation, SERC Reliability Corporation, Southwest Power Pool Regional Entity, Texas Reliability Entity, and Western Electricity Coordinating Council (WECC).

[2] On October 14, 2014, NERC submitted a "Request to Submit Revisions to the 2015 Budget and Assessments of Peak Reliability, Inc. to Reflect Additional Revenues from British Columbia Hydro and Power Authority," in Docket No. RR14-6-001. The Commission will address this filing in a subsequent order.

Reliability Standards, subject to Commission review and approval.[3] In July 2006, the Commission certified NERC as the ERO.[4]

3. FPA section 215(c)(2)(B) provides that the ERO must have rules that "allocate equitably reasonable dues, fees, and other charges among end users for all activities under this section."[5] On February 3, 2006, the Commission issued Order No. 672 to implement the requirements of FPA section 215, which generally provides for Commission authorization of funding for "statutory" functions, (i.e., those functions carried out pursuant to FPA section 215).[6] Among other things, Order No. 672 sets forth requirements for funding the ERO and the approval of an ERO business plan and budget.[7] Moreover, the Commission's regulations require the ERO to file with the Commission the ERO's proposed annual budget for statutory and non-statutory activities 130 days before the beginning of its fiscal year.[8] Further, the ERO's filing must contain the annual budgets of each Regional Entity for statutory and non-statutory activities and provide supporting materials, including the ERO's and each Regional Entity's complete business plan and budget organizational chart. The filing must also explain the proposed collection of all dues, fees, and charges, as well as the proposed expenditure of funds collected.

B. NERC's 2015 ERO Business Plan and Budget Application

4. The NERC Application contains NERC's proposed business plan and budget for the year ending December 31, 2015, as well as the proposed business plans and budgets

---

[3] 16 U.S.C. § 824o (2012).

[4] *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).

[5] 16 U.S.C. § 824o(c)(2)(B).

[6] *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).

[7] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 197.

[8] 18 C.F.R. § 39.4(b) (2014).

of each of the eight Regional Entities, WIRAB, and Peak Reliability for the year ending December 31, 2015.

5. NERC states that the proposed assessment for the total ERO (i.e., NERC, the Regional Entities, and WIRAB) for 2015 is $163,582,428, which includes $55,308,375 for NERC funding; $107,215,895 for Regional Entity funding; and $1,058,158 for WIRAB funding. NERC states that the portion of statutory activities of NERC, the Regional Entities, and WIRAB allocable to the United States is $148,273,401. The proposed assessment for Peak Reliability for 2015 is $41,953,236; the portion of this assessment allocable to the United States is $41,302,627. NERC states that it will continue to allocate costs to end users in the United States based on Net Energy for Load.

6. In addition to the NERC, Regional Entity, WIRAB, and Peak Reliability business plans and budgets, the NERC Application includes various attachments: Discussion of Comments Received During Development of NERC's 2015 Business Plan and Budget (Attachment 13); Calculation of Adjustments for Alberta Electric System Operator, Ontario Independent Electric System Operator, New Brunswick and the Quebec NERC Assessment (Attachment 14); Status Report on NERC's 2014 Goals (Attachment 15); Regional Entity Budget Metrics (Attachment 16); and Metrics on NERC and Regional Entity Administrative (Indirect) Costs Based on the 2014 and 2015 Budgets (Attachment 17).

II. Notice and Responsive Pleadings

7. Notice of NERC's August 22, 2014 filing was published in the *Federal Register*, 79 Fed. Reg. 51,995 (2014), with interventions and protests due on or before September 12, 2014.

8. California Department of Water Resources State Water Project filed a timely motion to intervene. Exelon Corporation (Exelon) filed a timely motion to intervene and comments supporting approval of the NERC Application.

9. On September 17, 2014, WIRAB submitted its advice, recommending that the Commission accept WECC's and Peak Reliability's 2015 business plans and budgets.

III. Discussion

A. Procedural Matters

10. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2014), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

B. Substantive Issues

1. NERC Business Plan and Budget

11. NERC states that it prepared its 2015 business plan and budget, and worked with the Regional Entities in developing their business plans and budgets, through a rigorous process that provided ample opportunity for review and input by the Finance and Audit Committee of the NERC Board of Trustees (NERC Board) and stakeholders. According to NERC, successive versions of the 2015 business plans and budgets were discussed in meetings and conference calls of the Finance and Audit Committee and full NERC Board, in each case with opportunities for stakeholders to make comments.

12. NERC states that its principal goals in 2015 are focused on the following areas: (1) continuing to implement NERC's risk-based strategy, with a focus on a set of current high priority risk projects; (2) physical and cyber security of the Bulk-Power System; (3) continuing to implement NERC's Reliability Assurance Initiative; (4) implementing the revised bulk electric system definition that the Commission has approved; (5) developing and implementing a risk-based registration system; and (6) transforming the NERC Reliability Standards to a steady state.[9]

13. With respect to the Reliability Assurance Initiative, NERC describes that program as "a multiyear effort that involves compliance and enforcement process changes, development of new tools and training materials, and a variety of related efforts."[10] NERC states that it is implementing the Reliability Assurance Initiative "as part of its stated objectives of ensuring [bulk electric system] reliability, improving the efficiency and effectiveness of NERC and Regional Entity compliance and enforcement operations, and reducing unnecessary burdens to registered entities."[11] NERC describes the goal of the risk-based registration program as ensuring that "entities are properly registered or de-registered commensurate with risk to the [bulk electric system], are properly scoped, and are responsible for applicable Reliability Standards along with associated compliance obligations."[12]

---

[9] NERC Application at 7.

[10] *Id.* at Attachment 2 (NERC's Proposed 2015 Business Plan and Budget) at 9.

[11] *Id.*

[12] *Id.* at xiii.

14. NERC states that its 2015 business plan and budget is based on the following program areas: (1) Reliability Standards; (2) Compliance Monitoring and Enforcement Program and Organization Registration and Certification, which is comprised of Regional Entity Assurance and Oversight, Compliance Analysis, Registration and Certification, and Compliance Enforcement; (3) Reliability Assessment and Performance Analysis; (4) Reliability Risk Management, which is comprised of Situation Awareness and Event Analysis; (5) Critical Infrastructure Protection; (6) Electricity Sector Information Sharing and Analysis Center; and (7) Training, Education, and Operator Certification.[13] For these program areas, NERC describes each program, identifies the program's goals and objectives, and provides the number of full-time equivalent employees (FTEs), as well as the amount budgeted for 2015. NERC also provides 2014 approved budget data and 2014 year-end projected data for comparison.

15. NERC's proposed total funding for 2015 is $67,371,264, which is an increase of $13,635,882 (25.4 percent) over the 2014 budget. A significant portion of this increase is attributable to NERC's participation in the Cyber Risk Information Sharing Program (CRISP). NERC explains that CRISP is "a public-private partnership whose purpose is to facilitate timely information sharing of cyber threat information and to develop situation awareness tools that enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of its critical infrastructure."[14] While the CRISP program will result in a significant increase in NERC's 2015 budgeted outlays, the CRISP program will be primarily funded by entities directly participating in the program (similar to the funding of certain training programs through participant fees) rather than through an increased assessment on all load-serving entities or their designees under FPA section 215.[15] Without CRISP, NERC's budget would increase by $1,328,097 (2.4 percent) over its 2014 budget. NERC's proposed 2015 net funding requirement is $55,308,375 (i.e., total budget less funding from other sources), of which $50,046,840 is allocated to the United States.[16] The net funding requirement allocated to the United States is an increase of $3,338,141 (7.1 percent) over the 2014 budget proposal. NERC states that its

[13] NERC Application at 4.

[14] *Id.* at 61.

[15] *Id.* at 7.

[16] *Id.* at 19-21. NERC's other funding sources are penalty payments, third-party funding for CRISP, revenue from services and software, testing and workshop fees, and interest. *Id.* at 13.

proposed total United States net funding requirement is equivalent to $0.000013 per kWh, based on the aggregate Net Energy for Load of the United States in 2013.[17]

16. NERC states that the proposed 2015 business plan and budget reflects a provision for working capital and operating reserve funding in the amount of $1,094,958.[18] Finally, NERC proposes a 2015 staffing level of 192.30 FTEs, which is an increase of 2.8 FTEs over the 2014 budget staffing level.

17. Exelon filed comments supporting the NERC budget, and the funding of CRISP in particular. Exelon states that "CRISP will enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of industry's critical infrastructure."[19]

Commission Determination

18. We find that NERC's 2015 budget is reasonable and the associated costs of NERC's jurisdictional functions are equitably allocated among end users in the United States.[20] We note that while NERC's 2015 budget will increase by 25.4 percent over 2014, the vast majority of that increase is attributable to the CRISP program, which will be significantly funded in 2015 by participating entities rather than through increased assessments. Accordingly, the Commission accepts NERC's 2015 business plan and budget.

2. Regional Entity Business Plans and Budgets

19. NERC's Application includes the 2015 business plans and budgets of each Regional Entity. NERC states that it reviewed the Regional Entity business plans and budgets and concludes that each Regional Entity proposes necessary and adequate resources to carry out its delegated functions.[21]

---

[17] *Id*. at 21.

[18] *Id.* at Attachment 2 (NERC's Proposed 2015 Business Plan and Budget) at xxiii.

[19] Exelon Comments at 2.

[20] 16 U.S.C. § 824o(c)(1)(B).

[21] NERC Application at 28.

Commission Determination

20. The Commission finds that each submission reasonably supports the level of expenditures identified in the budgets. We are satisfied that the Regional Entities are focused on adequately staffing and funding all of their program areas to perform the delegated, statutory functions. Accordingly, the Commission accepts the Regional Entity business plans and budgets.

3. WIRAB Budget

21. WIRAB proposes statutory expenses of $1,013,851 in 2015, which is a $309,881 increase from its 2014 budget. WIRAB also proposes an incremental adjustment for working capital reserves of $45,027. To fund its operations in 2015, WIRAB proposes a statutory assessment of $1,058,158, of which $898,314 would be allocable to end users in the United States.

22. WIRAB notes that its key activities in 2015 include: (1) rectifying shortcomings in grid reliability practices of balancing authorities, transmission operators and other key registered entities; (2) improving the ability of western reliability organizations to identify, analyze, and recommend actions to address current and looming reliability challenges; (3) encouraging WECC and Peak Reliability to adopt more open and transparent data sharing practices; (4) ensuring that both Peak Reliability and WECC can effectively identify and disseminate best practices to maintain physical and cyber security of the Western Interconnection; and (5) collaborating with the Commission and NERC to identify future grid reliability challenges. WIRAB's budget includes four FTEs for 2015, which is an increase of 1.25 FTEs over 2014.

Commission Determination

23. Based on the information provided in the instant filing, the Commission concludes that WIRAB's 2015 budget is reasonable and, accordingly, the Commission accepts the WIRAB 2015 budget.

4. Peak Reliability Business Plan and Budget

24. NERC's Application includes the 2015 business plan and budget for Peak Reliability. NERC states that it has not substantively reviewed and approved Peak Reliability's Business Plan and Budget in the same manner that NERC reviews the business plans and budgets of the Regional Entities.[22]

[22] *Id.* at 110.

25. Peak Reliability's proposed budget for 2015, before provision for working capital, is $38,926,722, which is an increase of $5,968,073 (18.1 percent) over its 2014 budget. Peak Reliability states that the primary drivers of the increase in its statutory budget and personnel count are the new activities Peak Reliability will undertake to address recommendations from the WECC Board-appointed Reliability Coordination Task Force. NERC states that Peak Reliability will employ 161.67 FTEs, which is an increase of 12.57 FTEs.

26. WIRAB recommends approval of Peak Reliability's proposed 2015 budget, asserting that "Peak's 2015 budget will restore the Reliability Coordination function to sound budgeting practices."[23]

Commission Determination

27. Based on the information provided in the instant filing, the Commission concludes that Peak Reliability's 2015 budget is reasonable and, accordingly, the Commission accepts Peak Reliability's 2015 business plan and budget.

The Commission orders:

(A) NERC's 2015 business plan and budget is hereby accepted.

(B) The Regional Entity 2015 business plans and budgets are hereby accepted.

(C) The WIRAB 2015 business plan and budget is hereby accepted for funding.

(D) The Peak Reliability 2015 business plan and budget is hereby accepted.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[23] WIRAB Advice at 3.

149 FERC ¶ 61,061
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, and Tony Clark.

Southern California Edison Company Docket No. IN14-8-000

ORDER APPROVING STIPULATION AND CONSENT AGREEMENT

(Issued October 21, 2014)

1. The Commission approves the attached Stipulation and Consent Agreement (Agreement) between the Office of Enforcement (Enforcement), the North American Electric Reliability Corporation (NERC), and Southern California Edison Company (SCE). This order is in the public interest because it resolves on fair and reasonable terms an investigation of SCE, conducted by Enforcement in coordination with NERC and the Commission's Office of Electric Reliability (OER), into possible violations of Reliability Standards associated with SCE's operation of a portion of the Bulk Power System (BPS) and a blackout that occurred on September 8, 2011. SCE agrees to pay a civil penalty of $650,000, of which $250,000 will be paid to the United States Treasury and NERC, divided in equal amounts, and $400,000 will be invested in reliability enhancement measures that go above and beyond mitigation of the violations and the requirements of the Reliability Standards. SCE also agrees to commit to mitigation and compliance measures necessary to mitigate the violation described in this Agreement, and to make semi-annual compliance reports to Enforcement and NERC for at least one year.

I. Background

2. SCE, a wholly-owned subsidiary of Edison International, is an investor-owned utility providing electricity in central, coastal, and southern California. Among other NERC registrations, SCE operates as a Transmission Owner (TO) and Operator (TOP) within the California Independent System Operator's (CAISO) Balancing Authority area, and has delegated part of its responsibilities as TOP to CAISO under a Coordinated Functional Registration. SCE owns approximately 5,490 circuit miles of transmission lines, including 500, 230, and 161 kV lines. At the time of the event, SCE owned more than 5,600 MW of generation, including a majority share in the San Onofre Nuclear Generating Station (SONGS) in Southern California.[1] SCE's peak load exceeds 22,000 MW. SCE is subject to the Commission's regulation under section 215 of the Federal Power Act (FPA).[2]

[1] In June 2013, SONGS permanently ceased power operations.

[2] 16 U.S.C. § 824o (2012).

3. On March 16, 2007, in Order No. 693,[3] the Commission approved the initial Reliability Standards, which became mandatory and enforceable within the contiguous United States on June 18, 2007.

4. The investigation of SCE arose out of a system disturbance that occurred on the afternoon of September 8, 2011 in the Pacific Southwest, which resulted in cascading outages and left approximately 2.7 million customers (equivalent to five million or more individuals) without power, some for multiple hours extending into the next day. The total load loss for the event was in excess of 30,000 MWh. The event started with a three-phase fault which led to the loss of Arizona Public Service Company's Hassayampa-N. Gila 500 kV transmission line (H-NG). This transmission line is a segment of the Southwest Power Link (SWPL), a major transmission corridor transporting power in an east-west direction, from generators in Arizona, through Imperial Irrigation District's (IID) service territory, into Southern California.

5. With the SWPL's major east-west corridor broken by the loss of H-NG, power flows instantaneously redistributed throughout the electric system in the Pacific Southwest and Southern California, increasing flows through lower voltage systems parallel to the SWPL as power continued to flow on a hot day during hours of peak demand.

6. These redistributed flows traveled through IID's and Western Area Power Administration-Desert Southwest's (Western-DSW) facilities, onto Western Electricity Coordinating Council (WECC)[4] Path 44, an aggregation of five 230 kV transmission lines that deliver power in a north-south direction from SCE's territory in Los Angeles to San Diego. The increased power flows parallel to the SWPL, together with lower than peak generation levels in California and Mexico, led to significant voltage deviations and transmission equipment overloads. The flow redistributions, voltage deviations, and resulting overloads had a cascading effect, as transmission and generation equipment tripped offline in a relatively short time period. Just seconds before the blackout, Path 44 carried all flows into San Diego as well as parts of Arizona and Mexico. This excessive loading on Path 44 initiated an intertie separation scheme owned and operated by SCE at

[3] *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).

[4] At the time of the event, WECC was registered with NERC as the Reliability Coordinator (RC) for all of the entities affected by the event, as well as serving as the Regional Entity (RE) under a delegation agreement with NERC. Since the event, the Regional Entity and Reliability Coordinator functions have been bifurcated, with WECC remaining the Regional Entity, and Peak Reliability becoming the independent Reliability Coordinator. *See Order on Compliance*, 146 FERC ¶ 61,092 (2014) (accepting compliance filings submitted by NERC and WECC and eliminating all final obstacles to bifurcation).

the San Onofre switchyard. Initiation of this intertie separation scheme separated San Diego Gas & Electric (SDG&E) from Path 44, contributed to tripping the SONGS nuclear units offline, and eventually resulted in the complete blackout of San Diego and Comisión Federal de Electricidad's (CFE) Baja California Control Area in Mexico.

7. Before the September 8 event, system conditions had never exceeded the threshold for triggering the intertie separation scheme at the San Onofre switchyard, and SCE had never conducted any studies to assess the scheme's impact on reliability or the scheme's impact on an already severely compromised system.

8. Operation of the scheme simultaneously opened all five 230 kV transmission lines—Path 44—connecting SCE and SDG&E, as it was designed to do, and the resulting cut in power to SDG&E's system caused a rapid frequency decline indicative of a severe imbalance between generation and load in SDG&E's system. This rapid frequency decline affected SDG&E's Underfrequency Load Shedding (UFLS) program. Prior to this point in the event, SDG&E had already lost its intertie to the east, and with the opening of Path 44, SDG&E was effectively separated from the rest of the Western Interconnection.

9. The operation of the separation scheme under the extreme power flow conditions resulted in a sudden change in the angle of the generator rotors at SONGS. This resulted in the activation of turbine control logic to prevent over speed of the equipment which tripped both SONGS units.

II. Investigation

10. On September 9, 2011, the Commission and NERC announced a joint inquiry to determine how the blackout occurred and to make recommendations to avoid similar situations in the future. The inquiry team, comprised of Commission and NERC staff, used on-site visits and interviews, detailed computer modeling, event simulations, and system analyses to make its findings and recommendations for preventing similar events in the future. The inquiry determined that entities responsible for planning and operating the BPS were not prepared to ensure reliable operation or prevent cascading outages in the event of a single contingency. On May 1, 2012, the inquiry team published a report entitled *Arizona-Southern California Outages on September 8, 2011, Causes and Recommendations* (the Report), which is hereby incorporated by reference.[5] The Report discusses a detailed sequence of events, simulations, and findings related to the causes of the cascading outages. The Report also makes twenty-seven recommendations related to next-day planning, seasonal planning, near- and long-term planning, situational

[5] *Arizona-Southern California Outages on September 8, 2011, Causes and Recommendations* (April 2012), *available at* http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

awareness, consideration of bulk electric system (BES) equipment, System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs), and protection systems.

11. Following publication of the Report, Enforcement, OER, and NERC staff reviewed the data gathered during the inquiry for compliance implications. At the direction of the Commission, Enforcement initiated non-public investigations of several entities, including SCE, under Part 1b of the Commission's regulations, 18 C.F.R. Part 1b (2014), which were conducted jointly with NERC.

12. Enforcement and NERC determined that SCE violated the Protection and Control (PRC-) group of Reliability Standards. The PRC standards cover a range of topics related to the protection and control of power systems, including the design, coordination, and maintenance of functional protection systems.

13. Enforcement and NERC determined that SCE failed to adequately coordinate the intertie separation scheme at the San Onofre switchyard with protection systems, including (1) the acceleration limits within the turbine control systems on the two SONGS generators; and (2) the UFLS program of its neighbor, SDG&E, in violation of Reliability Standard PRC-001-1 R4. Enforcement and NERC found SCE's violation to be a serious deficiency undermining reliable operation of the BPS.

III. Stipulation and Consent Agreement

14. Enforcement, NERC, and SCE resolved this matter by means of the attached Agreement. SCE stipulates to the facts recited in the Agreement and agrees to pay a civil penalty of $650,000, of which $250,000 will be paid to the United States Treasury and NERC, divided in equal amounts, and $400,000 will be invested in reliability enhancement measures that go above and beyond the requirements of the Reliability Standards, as described in the Agreement. SCE neither admits nor denies that its actions constituted violations of the Reliability Standards.

15. SCE also agrees to additional mitigation measures, and to submit to compliance monitoring, as specified in the Agreement.

16. In consideration of the appropriate sanction, Enforcement considered that SCE has made significant efforts to date to address reliability concerns identified in the inquiry and investigation and also by SCE on its own initiative. SCE also fully and comprehensively cooperated with Enforcement and NERC during the investigation.

IV. Determination of the Appropriate Sanctions

17. The civil penalty amount is consistent with the Penalty Guidelines.[6] Enforcement considered that the event caused a loss of 10,000 or more MWh of firm load, and SCE

[6] *Enforcement of Statutes, Orders, Rules and Regulations,* 132 FERC ¶ 61,216 (2010).

was allocated a share of the base penalty. The civil penalty amount reflects credit for SCE's full cooperation during the course of the investigation as well as credits for avoiding a trial-type hearing and having an effective compliance program.

18. The Commission concludes that the penalties and other sanctions set forth in the Agreement are a fair and equitable resolution of this matter and are in the public interest. The Commission also concludes that the reliability enhancement measures set forth in the Agreement will enhance the reliability of the BPS and are therefore also fair and in the public interest.

The Commission orders:

The attached Stipulation and Consent Agreement is hereby approved without modification.

By the Commission. Commissioner Bay is not participating.

(S E A L)

Kimberly D. Bose,
Secretary.

.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Southern California Edison Company) Docket No. IN14-8-000

STIPULATION AND CONSENT AGREEMENT

I. INTRODUCTION

1. Staff of the Office of Enforcement (Enforcement) of the Federal Energy Regulatory Commission (Commission), the North American Electric Reliability Corporation (NERC), and Southern California Edison Company (SCE) enter into this Stipulation and Consent Agreement (Agreement) to resolve a non-public investigation conducted by Enforcement and NERC pursuant to Part 1b of the Commission's regulations, 18 C.F.R. Part 1b (2014). The investigation examined possible violations of NERC Reliability Standards by SCE related to a system event in the Pacific Southwest on September 8, 2011 (September 8 event or event). SCE neither admits nor denies that it violated the Reliability Standard described in the Agreement, but agrees to pay a total civil penalty of $650,000, of which $250,000 will be paid to the United States Treasury and NERC, divided in equal amounts, and $400,000 will be invested, subject to Enforcement and NERC approval, by SCE in reliability enhancement measures identified below that go above and beyond the Agreement's mitigation commitments or what that Reliability Standards require (Reliability Enhancements). SCE also commits to mitigation and compliance measures, subject to compliance monitoring, as detailed in the Agreement.

II. STIPULATED FACTS

2. Enforcement, NERC, and SCE hereby stipulate and agree to the following facts.

A. SCE

3. SCE, a wholly-owned subsidiary of Edison International, is an investor-owned utility providing electricity in central, coastal, and southern California. Among other NERC registrations, SCE operates as a Transmission Owner (TO) and Operator (TOP) within the California Independent System Operator's (CAISO) Balancing Authority area, and has delegated part of its responsibilities as TOP, including seasonal, next-day, and current-day planning, to CAISO under a

Coordinated Functional Registration.[1] SCE owns approximately 5,490 circuit miles of transmission lines, including 500, 230, and 161 kV lines. At the time of the event, SCE owned more than 5,600 MW of generation, including a majority share in the San Onofre Nuclear Generating Station (SONGS) in Southern California.[2] SCE's peak load exceeds 22,000 MW.

B. Event Description

4. During an 11-minute period on the afternoon of September 8, 2011, a system disturbance occurred in the Pacific Southwest, resulting in cascading outages and leaving approximately 2.7 million customers without power, some for multiple hours extending into the next day. The total load loss for the event was in excess of 30,000 MWh. The event started with a three-phase fault which led to the loss of Arizona Public Service's (APS's) Hassayampa-N. Gila 500 kV transmission line (H-NG). This transmission line is a segment of the Southwest Power Link (SWPL), a major transmission corridor transporting power in an east-west direction, from generators in Arizona, through the service territory of Imperial Irrigation District (IID), into Southern California.

5. With the SWPL's major east-west corridor broken by the loss of H-NG, power flows instantaneously redistributed throughout the electric system in the Pacific Southwest and Southern California, increasing flows through lower voltage systems parallel to the SWPL as power continued to flow on a hot day during hours of peak demand.

6. These redistributed flows traveled through IID's and Western Area Power Administration – Desert Southwest's (Western-DSW's) territories onto Western Electricity Coordinating Council (WECC)[3] Path 44, an aggregation of five 230 kV

---

[1] JRO00009 was originally entered into on September 11, 2008 and most recently updated on May 24, 2012. JRO00009 delineates compliance responsibility for the Standards and Requirements associated with the TOP function between CAISO and SCE.

[2] In June 2013, SONGS permanently ceased power operations.

[3] At the time of the event, WECC was registered with NERC as the Reliability Coordinator (RC) for all of the entities affected by the event, as well as serving as the Regional Entity (RE) under a delegation agreement with NERC. Since the event, the Regional Entity and Reliability Coordinator functions have been bifurcated, with WECC remaining the Regional Entity, and Peak Reliability becoming the independent Reliability Coordinator. *See Order on Compliance*, 146 FERC ¶ 61,092 (2014) (accepting compliance filings submitted by NERC and WECC and eliminating all final obstacles to bifurcation). The Agreement will

transmission lines that deliver power in a north-south direction from SCE's territory in Los Angeles to San Diego Gas & Electric (SDG&E). The increased power flows parallel to the SWPL, together with lower than peak generation levels in California and Mexico, led to significant voltage deviations and transmission equipment overloads. The flow redistributions, voltage deviations, and resulting overloads had a cascading effect, as transmission and generation equipment tripped offline in a relatively short time period. Just seconds before the blackout, Path 44 carried all flows into San Diego as well as parts of Arizona and Mexico. This excessive loading on Path 44 initiated an intertie separation scheme, owned and operated by SCE, located at the San Onofre switchyard.[4] CAISO is responsible for many of the TOP functions for SCE under a Coordinated Functional Registration. Initiation of the intertie separation scheme at the San Onofre switchyard separated SDG&E from Path 44, contributed to tripping the SONGS nuclear units offline, and eventually resulted in the complete blackout of San Diego and Comisión Federal de Electricidad's Baja California Control Area.

7. SCE's role in the September 8 event centers on its ownership and operation of the intertie separation scheme at the San Onofre switchyard that initiated approximately 10 minutes and 40 seconds into the 11-minute event. Operation of the scheme simultaneously opened all five 230 kV transmission lines—Path 44—connecting SCE and SDG&E, as it was designed to do, and the resulting cut in power to SDG&E's system caused a rapid frequency decline indicative of a severe imbalance between generation and load in SDG&E's system. This rapid frequency decline affected SDG&E's Underfrequency Load Shedding (UFLS) program. Prior to this point in the event, SDG&E had already lost its intertie to the east, and with the opening of Path 44, SDG&E was effectively separated from the rest of the Western Interconnection. Before the September 8 event, system conditions had never exceeded the threshold for triggering the intertie separation scheme at the San Onofre switchyard, and SCE had never conducted any studies to assess the scheme's impact on reliability or the scheme's impact on an already severely compromised system.

8. The operation of the separation scheme under the extreme power flow conditions resulted in a sudden change in the angle of the generator rotors at SONGS. This resulted in the activation of turbine control logic to prevent over speed of the equipment which tripped both SONGS units.

---

refer to WECC when relevant to the event, and will otherwise refer to the relevant function (RE or RC) rather than using the entity names WECC or Peak Reliability.

[4] Since the September 8 event, Enforcement and NERC have referred to this intertie separation scheme as the SONGS Separation Scheme.

III. INQUIRY AND INVESTIGATION

9. On September 9, 2011, the Commission and NERC announced a joint inquiry to determine how the blackout occurred and to make recommendations to avoid similar situations in the future. The inquiry team, comprised of Commission and NERC staff, used on-site visits and interviews, detailed computer modeling, event simulations, and system analyses to make its findings and recommendations for preventing similar events in the future. The inquiry determined that entities responsible for planning and operating the Bulk-Power System (BPS) were not prepared to ensure reliable operation or prevent cascading outages in the event of a single contingency. On May 1, 2012, the inquiry team published a report entitled *Arizona-Southern California Outages on September 8, 2011, Causes and Recommendations* (the Report), which is hereby incorporated by reference.[5] The Report discusses a detailed sequence of events, simulations, and findings related to the causes of the cascading outages. The Report also makes twenty-seven recommendations related to next-day planning, seasonal planning, near- and long-term planning, situational awareness, consideration of Bulk Electric System (BES) equipment, system operating limits (SOLs) and Interconnection Reliability Operating Limits (IROLs), and protection systems.

10. Following publication of the Report, Enforcement and NERC reviewed the data gathered during the inquiry for compliance implications. As a result of that review, Enforcement and NERC initiated non-public investigations of several entities, including SCE, under Part 1b of the Commission's regulations, 18 C.F.R. Part 1b (2014). Enforcement and NERC determined that SCE violated Reliability Standard PRC-001-1 R4 and found that this violation undermined the reliability of the BPS and contributed to the September 8 event. Enforcement and NERC recognized, however, that after the event, and during the inquiry and investigation, SCE voluntarily began making improvements in its planning and operations, and implementing recommendations from the Report, that addressed many of the findings arising from the Report. In addition, SCE fully cooperated with Enforcement and NERC during the investigation.

11. As part of the investigation, Enforcement and NERC reviewed SCE's compliance program and discovered that SCE satisfies the criteria for an effective compliance program under the Commission's Penalty Guidelines.[6] Enforcement

---

[5] *Arizona-Southern California Outages on September 8, 2011, Causes and Recommendations* (April 2012), *available at* http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

[6] *Enforcement of Statutes, Orders, Rules and Regulations*, 132 FERC ¶ 61,216, § 1B2.1 (2010).

and NERC considered the following elements of SCE's compliance program: (1) SCE's NERC Compliance Program office is staffed by seventeen full time employees devoted to ensuring compliance with each Reliability Standard; (2) SCE conducts an annual self-assessment of its overall NERC compliance as well as monthly assessments of compliance with specific Reliability Standards; (3) Five of SCE's senior Officers are a part of SCE's NERC Executive Steering Team (EST). The EST team members are fully engaged in the compliance program and attend monthly status meetings with the director of the compliance program; and (4) SCE employees attend annual training sessions on NERC compliance and have opportunities to report and raise compliance issues, including through an anonymous Hotline maintained by a third party.

IV. VIOLATION

12. Enforcement and NERC determined that SCE violated Reliability Standard PRC-001-1 R4 because prior to the September 8 event it did not adequately coordinate the intertie separation scheme at the San Onofre switchyard with protection systems, including (1) the acceleration limits within the turbine control systems on the two SONGS generators; and (2) the UFLS program of its neighbor, SDG&E. Prior to the event, SCE had not conducted studies to assess the scheme's impact on reliability. Prior to the event, SCE also had not conducted studies to assess the scheme's impact on the acceleration of the SONGS units, or the impact to an already severely compromised system. As a result, SCE did not know how the initiation of the scheme would impact reliability, including whether the scheme would result in the tripping of the SONGS generators or how it might affect the ability of SDG&E's UFLS program to arrest extreme frequency decline, as described in paragraphs 6, 7, and 8 above.

V. REMEDIES AND SANCTIONS

13. SCE stipulates to the facts as described in Section II of the Agreement, but neither admits nor denies Enforcement's and NERC's findings that its conduct violated the Reliability Standard specified in Section IV. For purposes of settling any and all civil and administrative disputes within the jurisdiction of the Commission arising from reliability issues related to the September 8 event and Enforcement and NERC's investigation, SCE agrees to the remedies set forth in the following paragraphs.

A. Civil Penalty

14. SCE shall pay a total civil penalty of $650,000, of which $250,000 shall be paid, divided in equal amounts, to the United States Treasury and NERC within ten days of the Effective Date of the Agreement. Enforcement and NERC agree to give SCE a partial civil penalty offset for the remaining $400,000 in exchange for

SCE agreeing to implement the Reliability Enhancements set forth in Section V.B. The value of the Reliability Enhancements is expected to substantially exceed the amount of the offset.

B. Reliability Enhancements

15. In exchange for the $400,000 offset, as Reliability Enhancements, SCE shall provide the RE and/or RC with three Full-Time Equivalent (FTE) technical employees for a total of 6,240 hours to assist the RE and/or RC with their efforts in response to the September 8 event.

16. As part of the Reliability Enhancements, SCE employees will participate in regional study groups and various RE, RC, and/or NERC reliability initiatives, created in response to and for the purpose of improving reliability after the September 8 event. SCE, the RE, and/or RC will agree on the skill set of the employees to be shared and the employees' projects and tasks.

17. The scope and nature of the projects and tasks to be performed by the aforementioned SCE employees shall be approved by Enforcement and NERC, such approval not to be unreasonably withheld. SCE shall complete the Reliability Enhancements by December 31, 2016.

18. If SCE has not performed the Reliability Enhancements by December 31, 2016, or determines, prior to December 31, 2016, that it cannot reach an agreement with the RE and/or RC on the projects or tasks to be performed, SCE shall subtract from $400,000 the cash value of the services, if any, already performed, and pay the remaining sum in equal shares to the United States Treasury and NERC. The calculation of the sum due to Treasury and NERC, including the cash value of the services, and the identification of the services to be credited, are subject to review and approval by Enforcement and NERC.

C. Completed and Required Mitigation

19. SCE commits to the following actions, designed to mitigate the Reliability Standard violations and to improve overall reliability of the BES. As indicated below, SCE affirms that it has already completed most of the mitigation measures and shall complete all remaining mitigation measures no later than December 31, 2015, unless otherwise stated in this Section. In those instances where SCE has already implemented mitigation measures prior to entering into the Agreement, it shall continue operating under the practices and procedures implemented as part of the mitigation, until such time as it implements improved practices and procedures, as determined by Enforcement and NERC. SCE will report on the status of all mitigation measures described in this Section and submit evidence of

status and progress in its compliance monitoring reports to be submitted to Enforcement and NERC pursuant to Section V.C of the Agreement.

i. Mitigation Related to Protection Systems

Protection System Coordination[7]

20. SCE has completed multiple mitigation measures and has also agreed to implement multiple additional mitigating measures aimed at improving its coordination of Covered Protection Systems, including intertie overload separation schemes.[8]

21. Following the September 8 event, SCE undertook an expedited technical and physical evaluation of all its intertie overload separation schemes, to ensure that such schemes and the schemes' settings were properly coordinated across its transmission system. Based on this evaluation and to the extent necessary to ensure proper coordination, SCE changed the settings on some schemes, and disabled and removed others.

22. In addition to any requirements under the Reliability Standards related to protection systems, starting in 2014, SCE agrees to conduct a detailed study of twenty percent of its existing and planned Covered Protection Systems each year with 100 percent of the studies to be completed by December 31, 2018. SCE will prioritize its assessment of intertie overload separation schemes and will complete its assessment of such schemes by December 31, 2015. This assessment shall consider (1) the purpose and limitations of Covered Protection Systems; (2) the necessity of Covered Protection Systems; (3) the classification of Covered Protection Systems; (4) coordination of Covered Protection Systems with other devices and systems; (5) impact of Covered Protection Systems on internal and external elements; (6) whether Covered Protection Systems have unintended reliability consequences; (7) whether SCE's Underfrequency Load Shedding program is effective and consistent with the RE's Off-Nominal Frequency Load

[7] This section on Protection System coordination applies to the following Protection Systems: (1) internal to SCE's system, Special Protection Systems (including intertie overload separation schemes), overload Protection Systems on transmission equipment, and overload Protection Systems that studies show affect the BPS; and (2) external to SCE's system, Protection Systems that are known to affect SCE's operations (referred to as "Covered Protection Systems").

[8] SCE has identified its intertie overload separation schemes that remain in service, and Enforcement, NERC, and SCE maintain a list of such schemes confidentially.

Shedding plan; and (8) affected generators' response to activation of Covered Protection Systems.

23. SCE further agrees to share relevant information, including Covered Protection System settings, from the foregoing assessments with impacted entities and the Reliability Coordinator. To the extent SCE learns from the assessments that any Covered Protection Systems have degraded or have the potential to not operate as designed, SCE will immediately share this information with impacted entities and the Reliability Coordinator.

Effect of Protection Systems on Transmission Facility Loadability

24. SCE agrees to implement mitigation measures aimed at ensuring that its protection system relay settings do not limit the loadability of its transmission facilities. Specifically, in its 2016 Annual Transmission Reliability Assessment, and each year thereafter, SCE will review its transmission facility SOLs to ensure that they account for protection system relay settings and that they are equal to the most limiting operating criteria during all timeframes, including restoration. SCE will also identify instances where its relay trip points are set too close to transmission facility emergency ratings and to develop plans to mitigate such instances.

Protection System Training

25. SCE agrees to broaden its protection system training program. SCE has provided its transmission operators training on internal protection systems since before the September 8 event. Within six months of the Effective Date of the Agreement, SCE agrees to review this training to ensure it covers the purpose and limitations of Covered Protection Systems, the settings of Covered Protection Systems, and the impact of Covered Protection Systems on internal and external elements. SCE also agrees to expand this training within one year of the completion of the assessment described in Paragraph 22 to cover external protection systems, as identified by SCE, the CAISO, or any adjacent entity, that are likely to impact SCE's system reliability.

ii. Mitigation Related to Long-Term Planning

Consideration of Critical System Conditions in Long-Term Planning Assessments

26. Within one year of the Effective Date of the Agreement, SCE agrees to implement several steps (described below in paragraphs 27-30) to ensure that its long-term planning assessments consider critical system conditions, including expected system transfers above firm, expected internal and external generation dispatch, the impact of internal and external facilities, transmission facilities

operated below 100 kV, local distribution facilities operated below 100 kV that are known to impact the BPS, and the impact of active protection and control devices.

27. Regarding expected system transfers above firm, SCE agrees to include in its long-term studies additional sensitivities by varying generation and load to stress system transfers.

28. To ensure it considers expected internal and external generation dispatch levels in its long-term planning studies, SCE agrees to simulate combinations of various generator outages in its transmission area as well as neighboring areas that could impact its system.

29. SCE also agrees to improve its long-term planning process by ensuring that it considers internal and external facilities operated below 100 kV, where those facilities operate in parallel with facilities above 100 kV or have the potential to affect BPS reliability.[9] For example, SCE agrees to begin utilizing the RE's new base case coordination system to develop cases that include 69 kV facilities and to monitor contingencies involving facilities operated at 69 kV and above in SDG&E's, IID's, and APS's territories that have an impact on SCE's system.

30. SCE agrees to update its contingency files of its various Special Protection Systems (SPS)/Remedial Action Schemes (RAS) for its annual long-term planning studies. Also, it will continue to support the work and respond to data requests of the RE's Modeling SPS and Relays Ad-hoc Task Force to incorporate selected relays into base cases.

Analyses and Benchmarking of Past Planning Studies

31. On a going forward basis, SCE agrees to benchmark annually the prior year's planning studies against actual system operating conditions and look and account for higher stress conditions not captured in its annual assessments, such as unusual generation and import patterns, higher than expected load patterns, and contingencies that may have occurred and were not evaluated. SCE agrees to share information from its benchmarking analyses with impacted entities, CAISO, and the Reliability Coordinator.

iii. Mitigation Related to Situational Awareness

Greater Coordination to Improve Situational Awareness

[9] Inclusion of transmission facilities operated below 100 kV in the mitigation measures pursuant to the Agreement shall have no effect on any current or future analysis regarding whether these facilities comprise part of the BPS.

32. SCE agrees to implement various mitigating measures to improve its coordination efforts with neighboring entities as a way of strengthening its situational awareness. When provided with additional system information for coordination, SCE will have greater capability to assess information, including in the next-day and real-time timeframes, that could impact its system.

33. When released by Peak Reliability for usage, SCE agrees to ensure that its operators and operating engineers utilize, on a daily basis, relevant elements of Peak Reliability's new data sharing portal, which contains next-day studies, historical archives, and data from the Western Interconnection Synchrophasor Project. When released for entity use by Peak Reliability the phasor measurement data will provide operators visibility of system conditions in near real-time and may enable early detection of problems that could lead to cascading outages.

Expanded Situational Awareness

34. To the extent SCE has not already done so, within six months of the Effective Date of the Agreement, SCE also agrees to undertake efforts to identify internal and external elements that impact its portion of the BPS, including facilities operated below 100 kV. In addition, to the extent it has not already done so, SCE agrees to identify all internal elements, including elements operated below 100 kV, that impact external BPS elements, and to notify impacted entities and the Reliability Coordinator of such elements. All such elements shall be included in its models for monitoring in its seasonal, next-day, current-day, and real-time studies. SCE has also received and continues to receive Inter-Control Center Communications Protocol (ICCP) data from neighbors to further improve its transmission models with real-time, verified data on facilities that impact its system.

Response to Impaired Situational Awareness

35. Within six months of the Effective Date of the Agreement, SCE agrees to improve its procedures for responding to the impairment of its monitoring capabilities. These procedures maintain plans for the loss of SCADA/EMS, RTCA, and the loss of communication. They also cover plans for communicating with the Reliability Coordinator and neighboring entities in case SCE loses situational awareness. SCE also agrees to revise its procedures governing the exchange of information regarding the loss or change in service status of critical facilities with the Reliability Coordinator and other impacted entities. SCE will complete operator training on all of these new processes within one year of the Effective Date of the Agreement.

D. Compliance Monitoring

36. SCE shall make semi-annual reports to Enforcement and NERC until all of the mitigation measures and Reliability Enhancements, identified in the Agreement, have been fully implemented and verified by Enforcement and NERC. The first semi-annual report shall cover the first six month period after the Effective Date of the Agreement and shall be submitted to Enforcement and NERC staff within thirty days of the expiration of that period. The subsequent report(s) shall be due in six month increments thereafter. Each report shall detail the following: (1) actions taken as of the date of the report to satisfy the terms of the Agreement, including all mitigation items and Reliability Enhancements; (2) actions taken to improve reliability compliance, including investments in new measures and training activities during the reporting period; and (3) any additional violations of Reliability Standards that have occurred and whether and how SCE has addressed those new violations. The reports must include an affidavit executed by an officer of SCE that the compliance reports are true and accurate and also include corroborative documentation or other satisfactory evidence demonstrating or otherwise supporting the content of these reports. Enforcement and NERC staff may require additional semi-annual reporting if circumstances indicate the need for further monitoring or if SCE has not yet completed all the mitigation measures described in this Section.

VI. TERMS

37. The "Effective Date" of the Agreement shall be the date on which the Commission issues an order approving the Agreement without material modification. When effective, the Agreement shall resolve all reliability matters relating to the September 8 event within the jurisdiction of the Commission, and that arose on or before the Effective Date, as to SCE or any affiliated entity.

38. Commission approval of the Agreement without material modification shall release SCE and forever bar the Commission and NERC from holding SCE, any affiliated entity, and any successor in interest to SCE liable for any and all administrative or civil claims arising out of the reliability issues related to the September 8 event or conduct addressed and stipulated to in the Agreement that occurred on or before the Agreement's Effective Date.

39. Failure to make timely civil penalty payments or to comply with the mitigation, Reliability Enhancements, and monitoring agreed to herein, or any other provision of the Agreement, shall be deemed a violation of a final order of the Commission issued pursuant to the Federal Power Act (FPA), 16 U.S.C. §792, *et seq.*, and may subject SCE to additional action under the enforcement provisions of the FPA.

40. If SCE does not make the civil penalty payment described above at the time

agreed by the parties, interest payable to the United States Treasury and NERC shall begin to accrue pursuant to the Commission's regulations at 18 C.F.R. § 35.19(a)(2)(iii) (2014) from the date that payment is due, in addition to the penalty specified above and any other enforcement action and penalty that the Commission or NERC may take or impose.

41. The Agreement binds SCE and its agents, successors, and assignees. The Agreement does not create any additional or independent obligations on SCE, or any affiliated entity, its agents, officers, directors, or employees, other than the obligations identified in the Agreement.

42. The signatories to the Agreement agree that they enter into the Agreement voluntarily and that, other than the recitations set forth herein, no tender, offer or promise of any kind by any member, employee, officer, director, agent or representative of Enforcement, NERC, or SCE has been made to induce the signatories or any other party to enter into the Agreement.

43. Unless the Commission issues an order approving the Agreement in its entirety and without material modification, the Agreement shall be null and void and of no effect whatsoever, and Enforcement, NERC, and SCE shall not be bound by any provision or term of the Agreement, unless otherwise agreed to in writing by Enforcement, NERC, and SCE.

44. SCE agrees that the Commission's order approving the Agreement without material modification shall be a final and unappealable order assessing a civil penalty under the Federal Power Act. SCE waives findings of fact and conclusions of law, rehearing of any Commission order approving the Agreement without material modification, and judicial review by any court of any Commission order approving the Agreement without material modification.

45. The Agreement can be modified only if in writing and signed by Enforcement, NERC, and SCE, and any modifications will not be effective unless approved by the Commission.

46. Each of the undersigned warrants that he or she is an authorized representative of the entity designated, is authorized to bind such entity and accepts the Agreement on the entity's behalf.

47. The undersigned representative of SCE affirms that he or she has read the Agreement, that all of the matters set forth in the Agreement are true and correct to the best of his or her knowledge, information and belief, and that he or she understands that the Agreement is entered into by Enforcement and NERC in express reliance on those representations.

48. The Agreement may be signed in counterparts.

49. The Agreement is executed in triplicate, each of which so executed shall be deemed to be an original.

Agreed to and accepted:

Larry D. Gasteiger
Acting Director, Office of Enforcement
Federal Energy Regulatory Commission

Date: October 2, 2014

Charles A. Berardesco
Senior Vice President, General Counsel and Corporate Secretary
North American Reliability Corporation

Date: 10/01/2014

Pete Dietrich
Senior Vice President , Transmission & Distribuition
Southern California Edison Company

Date: 09/22/2014

149 FERC ¶ 61,140
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM14-15-000; Order No. 802]

Physical Security Reliability Standard

(Issued November 20, 2014)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves Reliability Standard CIP-014-1 (Physical Security). The North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization, submitted Reliability Standard CIP-014-1 for Commission approval in response to a Commission order issued on March 7, 2014. The purpose of Reliability Standard CIP-014-1 is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System against physical attacks. In addition, the Commission directs NERC to develop one modification to Reliability Standard CIP-014-1 and submit an informational filing.

EFFECTIVE DATE: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER]**.

FOR FURTHER INFORMATION CONTACT:

Regis Binder (Technical Information)
Office of Electric Reliability
Division of Reliability Standards and Security

Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (301) 665-1601
Regis.Binder@ferc.gov

Matthew Vlissides (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-8408
Matthew.Vlissides@ferc.gov

SUPPLEMENTARY INFORMATION:

149 FERC ¶ 61,140
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, Tony Clark,
and Norman C. Bay.

Physical Security Reliability Standard Docket No. RM14-15-000

ORDER NO. 802

FINAL RULE

(Issued November 20, 2014)

1. Pursuant to section 215 of the Federal Power Act (FPA), the Commission approves Reliability Standard CIP-014-1 (Physical Security).[1] The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted Reliability Standard CIP-014-1 for Commission approval in response to a Commission order issued on March 7, 2014.[2] The purpose of Reliability Standard CIP-014-1 is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System facilities against physical attacks. In addition to approving Reliability Standard CIP-014-1, as discussed below, the Commission directs NERC to submit an

[1] 16 U.S.C. 824o.

[2] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (March 7 Order).

informational filing and, pursuant to FPA section 215(d)(5), directs NERC to develop a modification to Reliability Standard CIP-014-1.[3]

I. Background

A. Section 215 and Mandatory Reliability Standards

2. Section 215 of the FPA requires the Commission to certify an ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Once approved, the Reliability Standards may be enforced in the United States by the ERO, subject to Commission oversight, or by the Commission independently.[4]

B. March 7 Order

3. In the March 7 Order, the Commission determined that physical attacks on the Bulk-Power System could adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures. Moreover, the Commission observed that the then current Reliability Standards did not specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System. Accordingly, to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System, the Commission directed NERC, pursuant to FPA section 215(d)(5), to develop and file for approval proposed Reliability

[3] 16 U.S.C. 824o(d)(5).

[4] *Id.* 824o(e).

Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System.

4. The March 7 Order indicated that the Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. Specifically, the March 7 Order directed that the Reliability Standards should require: (1) owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities"; (2) owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities; and (3) those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

5. The March 7 Order stated that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator, such as by NERC, the relevant Regional Entity, a reliability coordinator, or another entity.[5] In addition, the March 7 Order indicated that the Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove

[5] March 7 Order, 146 FERC ¶ 61,166 at P 11.

facilities from an owner's or operator's list of critical facilities.[6] The March 7 Order further stated that the determination of threats and vulnerabilities and the security plan should be reviewed by NERC, the relevant Regional Entity, the reliability coordinator, or another entity with appropriate expertise.

6. The March 7 Order stated that, because the three steps of compliance with the contemplated Reliability Standards could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.[7]

7. The Commission directed NERC to submit the proposed Reliability Standards to the Commission for approval within 90 days of issuance of the March 7 Order (i.e., June 5, 2014).

C. NERC Petition

8. On May 23, 2014, NERC petitioned the Commission to approve Reliability Standard CIP-014-1 and its associated violation risk factors and violation severity levels,

[6] *Id.*

[7] *Id.* P 10.

implementation plan, and effective date.[8] NERC maintains that the Reliability Standard is just, reasonable, not unduly discriminatory, or preferential, and in the public interest. In addition, NERC asserts that the proposed Reliability Standard complies with the Commission's directives in the March 7 Order.

9. NERC explains that Reliability Standard CIP-014-1 "serves the vital reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and lessening the overall vulnerability of the Bulk-Power System to physical attacks."[9] NERC maintains that the "appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the Bulk-Power System."[10] The Reliability Standard is applicable to transmission owners that satisfy the Applicability Sections 4.1.1.1, 4.1.1.2, 4.1.1.3, or

[8] NERC explains that, to meet the 90-day deadline in the March 7 Order, the NERC Standards Committee approved waivers to NERC's Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request and draft Reliability Standard. NERC Petition at 13-14. Reliability Standard CIP-014-1 is not attached to this Final Rule. The complete text of Reliability Standard CIP-014-1 is available on the Commission's eLibrary document retrieval system in Docket No. RM14-15-000 and is posted on the ERO's web site, *available at* http://www.nerc.com.

[9] NERC Petition at 15-16.

[10] *Id.* at 18. NERC states that, although the terms "Transmission stations" and "Transmission substations" are sometimes used interchangeably, Reliability Standard CIP-014-1 uses the term "Transmission substation" to refer to a facility contained within a physical border (e.g., a fence or wall) that contains one or more autotransformers. *Id.* According to NERC, the term "Transmission station," as used in Reliability Standard CIP-014-1, refers to a facility that functions as a switching station or switchyard but does not contain autotransformers. *Id.* at 18-19.

4.1.1.4, and to transmission operators. NERC states that the transmission facilities covered by Applicability Sections 4.1.1.1 through 4.1.1.4 match the "Medium Impact" transmission facilities listed in Attachment 1 (Impact Rating Criteria), specifically, the "Medium Impact" facilities described in Sections 2.4, 2.5, 2.6, and 2.7, of Reliability Standard CIP-002-5.1,[11] According to NERC, the "standard drafting team determined that using the criteria for 'Medium Impact' Transmission Facilities set forth in Reliability Standard CIP-002-5.1 is an appropriate applicability threshold as the Commission has acknowledged that it is a technically sound basis for identifying Transmission Facilities, which, if compromised, would present an elevated risk to the Bulk-Power System."[12]

10. Reliability Standard CIP-014-1 has six requirements. Requirement R1 requires applicable transmission owners to perform risk assessments on a periodic basis to identify their transmission stations and transmission substations that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or cascading within an Interconnection. Requirement R1 also requires transmission owners to identify the primary control center that operationally controls each of the identified transmission stations or transmission substations.

11. Requirement R2 requires that each applicable transmission owner have an unaffiliated third party with appropriate experience verify the risk assessment performed

[11] *Id.* at 25 (citing Reliability Standard CIP-002-5.1 (Cyber Security — BES Cyber System Categorization), Attachment 1 (Impact Rating Criteria)).

[12] *Id.*

under Requirement R1. Requirement R2 states that the transmission owner must either modify its identification of facilities consistent with the verifier's recommendation or document the technical basis for not doing so. In addition, Requirement R2 requires each transmission owner to implement procedures for protecting sensitive or confidential information made available to third-party verifiers or developed under the Reliability Standard from public disclosure.

12. Requirement R3 requires the transmission owner to notify a transmission operator that operationally controls a primary control center identified under Requirement R1 of such identification to ensure that the transmission operator has notice of the identification so that it may timely fulfill its obligations under Requirements R4 and R5 to protect the primary control center.

13. Requirement R4 requires each applicable transmission owner and transmission operator to conduct an evaluation of the potential threats and vulnerabilities of a physical attack on each of its respective transmission stations, transmission substations, and primary control centers identified as critical in Requirement R1.

14. Requirement R5 requires each transmission owner and transmission operator to develop and implement documented physical security plans that cover each of their respective transmission stations, transmission substations, and primary control centers identified as critical in Requirement R1.

15. Requirement R6 requires that each transmission owner and transmission operator subject to Requirements R4 and R5 have an unaffiliated third party with appropriate experience review its Requirement R4 evaluation and Requirement R5 security plan.

Requirement R6 states that the transmission owner or transmission operator must either modify its evaluation and security plan consistent with the recommendation, if any, of the reviewer or document its reasons for not doing so. In addition, Requirement R6 requires each transmission owner to implement procedures for protecting sensitive or confidential information made available to third-party reviewers or developed under the Reliability Standard from public disclosure.

D. Notice of Proposed Rulemaking

16. On July 17, 2014, the Commission issued a Notice of Proposed Rulemaking proposing to approve Reliability Standard CIP-014-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[13] In addition, the NOPR proposed to direct NERC to develop two modifications to the Reliability Standard. First, the NOPR proposed to direct NERC to develop a modification to allow applicable governmental authorities (i.e., the Commission and any other appropriate federal or provincial authorities) to add or subtract facilities from an applicable entity's list of critical facilities under Requirement R1.[14] Second, the NOPR proposed to direct NERC to modify the Reliability Standard to remove the term "widespread" as it appears in the phrase "widespread instability" in Requirement R1.[15] The NOPR also proposed to direct

[13] *Physical Security Reliability Standard*, Notice of Proposed Rulemaking, 79 Fed. Reg. 42,734 (July 23, 2014), 148 FERC ¶ 61,040 (2014) (NOPR).

[14] *Id.* P 23.

[15] *Id.* P 29.

NERC to submit two informational filings, one addressing the protection of "High Impact" control centers and the other addressing resiliency measures, to be submitted, respectively, within six months and one year following the effective date of a final rule in this proceeding.[16]

17. In response to the NOPR, the Commission received 33 sets of initial comments and six sets of reply comments. We address below the issues raised in the NOPR and comments. The Appendix to this final rule lists the entities that filed comments in response to the NOPR.

II. Discussion

18. Pursuant to FPA section 215(d)(2), we approve Reliability Standard CIP-014-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission also approves the associated violation risk factors, violation severity levels, implementation plan, and effective date proposed by NERC (i.e., the "first day of the first calendar quarter that is six months beyond" the effective date of the final rule in this proceeding).[17] As discussed below, the Commission determines that Reliability Standard CIP-014-1 satisfies the directives in the March 7 Order concerning the development and submittal of physical security Reliability Standards.

[16] *Id.* PP 35, 57.

[17] NERC Petition, Exhibit B (Implementation Plan) at 1.

19. In addition to approving Reliability Standard CIP-014-1, the Commission adopts in part the NOPR proposal directing NERC to develop and submit modifications to the Reliability Standard concerning the use of the term "widespread" in Requirement R1. The Commission determines that the term "widespread" is unclear with respect to the obligations it imposes on applicable entities; how it would be implemented by applicable entities; and how it would be enforced. Accordingly, the Commission directs NERC, pursuant to FPA section 215(d)(5), to remove the term "widespread" from Reliability Standard CIP-014-1 or, alternatively, to propose modifications to the Reliability Standard that address the Commission's concerns. We direct that NERC submit a responsive modification within six months from the effective date of this final rule.

20. The Commission does not adopt the NOPR proposal that would have required NERC to develop and submit modifications to Reliability Standard CIP-014-1 to allow applicable governmental authorities (i.e., the Commission and any other appropriate federal or provincial authorities) to add or subtract facilities from an applicable entity's list of critical facilities under Requirement R1. We determine that the Commission's enforcement authority under FPA section 215(e), and particularly the use of targeted auditing following implementation of Reliability Standard CIP-014-1, will allow us to address the concerns raised in the NOPR.

21. With respect to the informational filings proposed in the NOPR, the Commission adopts the proposal to direct NERC to make an informational filing addressing whether Reliability Standard CIP-014-1 provides physical security for all "High Impact" control centers, as that term is defined in Reliability Standard CIP-002-5.1, necessary for the

reliable operation of the Bulk-Power System. However, the Commission extends the deadline for that informational filing until two years following the effective date of Reliability Standard CIP-014-1. The Commission, at this time, does not adopt the NOPR proposal to direct NERC to make an informational filing addressing resiliency. Instead, the Commission will continue to consider ways for industry to best inform the Commission of its current and future resiliency efforts, which could take the form of reports and/or technical conferences to address specific areas of concern (e.g., spare parts, fuel security, and advanced technologies).

22. We address below the following issues raised in the NOPR and in the comments: (A) removal of the term "widespread"; (B) applicable governmental authorities' ability to add or subtract facilities from an entity's list of critical facilities; (C) informational filing on "High Impact" control centers; (D) informational filing on resiliency; (E) third-party verification and review; (F) exclusion of generators from the applicability section of Reliability Standard CIP-014-1; (G) confidentiality; (H) other issues raised in comments; (I) violation risk factors and violation severity levels; and (J) implementation plan and effective date.

A. Removal of the Term "Widespread"

March 7 Order

23. The March 7 Order stated that a critical facility is "one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[18]

NERC Petition

24. Reliability Standard CIP-014-1 states that its purpose is to "identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection."[19] Requirement R1 states that the "initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection."

NOPR

25. The NOPR proposed to direct NERC to modify Reliability Standard CIP-014-1 to remove the term "widespread" as it appears in the phrase "widespread instability." The

[18] March 7 Order, 146 FERC ¶ 61,166 at P 6.

[19] NERC Petition at 17.

NOPR stated that the phrase "widespread instability" is undefined by NERC and is inconsistent with the March 7 Order's explanation of "critical facility" and the definition of "reliable operation" in FPA section 215(a)(4).[20]

26. The NOPR stated that the use of "widespread instability" in Requirement R1 could, depending on the meaning of "widespread," narrow the scope (and number) of identified critical facilities under Reliability Standard CIP-014-1 beyond what was contemplated in the March 7 Order. The NOPR also stated that the use of the term "widespread" could potentially render the Reliability Standard unenforceable or lead to an inadequate level of reliability by omitting facilities that are critical to the reliable operation of the Bulk-Power System.

Comments

27. NERC comments that it does not oppose the NOPR directive but that the modification should be developed through NERC's standards development process and NERC should be allowed to propose alternative clarifying language "to ensure the proposed Reliability Standard remains focused on Interconnection impacts and not local

[20] "[A facility] that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System." March 7 Order, 146 FERC ¶ 61,166 at P 6; 16 U.S.C. 824o(a)(4) ("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.").

impacts."[21] NERC states that the term "widespread" was used to focus applicable entities' security efforts on facilities whose loss would have more than a local area impact.

28. SIA, Idaho Power, Pa PUC, SmartSenseCom, Foundation and Pepco support the NOPR proposal because they believe that the term "widespread" is vague or inconsistent with the definition of "reliable operation" in FPA section 215.[22] Pepco, for example, states that the term "widespread" is ambiguous, will require requests for clarification or interpretation and will expose applicable entities to "second-guessing" from auditors. KCP&L, while it does not state that it supports the proposal, acknowledges that the term "widespread" is vague and that the term "introduces interpretive language that may be problematic for compliance and enforcement interpretations as well as unintentionally narrow the scope of facilities."[23]

29. Other commenters do not support the proposed directive largely because they contend that the proposal may have the unintended consequence of expanding the scope of Reliability Standard CIP-014-1 to include localized events that have no impact on an

[21] NERC Comments at 19.

[22] *See* SIA Comments at 2; Idaho Power Comments at 2; Pa PUC Comments at 5; Pepco Comments at 4-5; SmartSenseCom Comments at 7-8; Foundation Reply Comments at 7.

[23] KCP&L Comments at 4.

Interconnection.[24] APS, SCE, SDG&E, and G&T Cooperatives also maintain that while the term "widespread" is not defined by NERC, it appears elsewhere in the Reliability Standards, including in NERC's definition of "Cascading" and in the TPL Reliability Standards, and is understood by industry. Associations also state that the Commission should withdraw the NOPR proposal; however, Associations state that, in the alternative, the Commission should clarify that removal of the term "widespread" is not intended to bring within the scope of Reliability Standard CIP-014-1 "a substation or station unless the applicable Transmission Owner determines through technical studies and analyses that include the application of engineering judgment and practice that the loss of such facility would have a critical impact on the operation of the [bulk electric system] in the event the asset is rendered inoperable or damaged."[25] NARUC states that the proposal will add costs without necessarily improving reliability.

30. ITC, while agreeing that the term "widespread" is not well-defined and would render the Reliability Standard vague, contends that the definition of critical facility in Requirement R1 should be replaced by defining as critical all physical facilities that

[24] *See* APS Comments at 3; SCE Comments at 3; SDG&E Comments at 4-5; TVA Comments at 9-10; Tallahassee Comments at 1; Oncor Comments at 3-4; Ohio PUC Comments at 4-5; BPA Comments at 3; NARUC Comments at 11; G&T Cooperatives Comments at 8-11; Southern Comments at 7-10.

[25] Associations Comments at 14-15; *see also* APS Comments at 3-4, Southern Comments at 11.

contain "High Impact" or "Medium Impact" BES Cyber Systems as those terms are defined in Reliability Standard CIP-002-5.1.

Commission Determination

31. The Commission adopts the NOPR proposal in part and directs NERC to remove the term "widespread" from Reliability Standard CIP-014-1 or, alternatively, to propose modifications to the Reliability Standard that address the Commission's concerns. The differing views expressed in the comments validate the concern raised in the NOPR that the meaning of the term "widespread" is unclear and subject to interpretation.

32. We stated in the March 7 Order that "the Reliability Standards that we are ordering today apply only to critical facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.[26] We affirm the March 7 Order's statement that "[m]ethodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment."[27]

33. However, incorporating the undefined term "widespread" in Reliability Standard CIP-014-1 introduces excessive uncertainty in identifying critical facilities under Requirement R1.[28] As the Commission stated in the March 7 Order, only an instability

[26] March 7 Order, 146 FERC ¶ 61,166 at P 6 n.5.

[27] *Id.* P 6.

[28] *See Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160, at P 67 (2013), *order*

(continued ...)

that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1. The March 7 Order did not intend to suggest that the physical security Reliability Standards should address facilities that do not have a "critical impact on the operation of the interconnection." This understanding is, we believe, unintentionally absent in Requirement R1 because the requirement only deems a facility critical when, if rendered inoperable or damaged, it could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The definition in Requirement R1 should not be dependent on how an applicable entity interprets the term "widespread" but instead should be modified to make clear that a facility that has a critical impact on the operation of an Interconnection is critical and therefore subject to Requirement R1.

34. While some commenters contend that the meaning of the term "widespread" is well-understood by industry, we find that there is ample evidence in the record to support the conclusion that the term is susceptible to different interpretations by applicable entities. Notably, KCP&L states that, while it was a participant in the standards drafting process for Reliability Standard CIP-014-1, it agrees that the term requires interpretation. Moreover, KCP&L and Pepco share our concern that compliance enforcement authorities

---

granting clarification in part and denying rehearing, Order No. 791-A, 146 FERC ¶ 61,188 (2014) (directing removal or clarification "identify, assess and correct" language).

may find it difficult to consistently enforce compliance with Requirement R1 without a clear understanding of the term's meaning.

35. Accordingly, pursuant to FPA section 215(d)(5), the Commission directs NERC to develop a modification to Reliability Standard CIP-014-1 that either removes the term "widespread" from Requirement R1 or, in the alternative, proposes changes that address the Commission's concerns. Further, we direct that NERC submit a responsive modification within six months from the effective date of this final rule. We recognize that certain entities commented on how NERC could modify Reliability Standard CIP-014-1 to address the Commission's stated concerns.[29] However, we conclude that it is appropriate to allow NERC to develop and propose a modification in the first instance. With respect to ITC's more general comments regarding the scope of critical facilities in Requirement R1, we address the potential for applying the impact designations in Reliability Standard CIP-002-5.1 to Reliability Standard CIP-014-1, Requirement R1 in the section below regarding the NOPR's proposed informational filing on "High Impact" control centers.

[29] *See*, *e.g.*, BPA Comments at 2; Ohio PUC Comments at 5; TVA Comments at 9, ITC Comments at 9.

B. Applicable Governmental Authority's Ability to Add or Subtract Facilities from an Entity's List of Critical Facilities

March 7 Order

36. In the March 7 Order, the Commission stated that:

> [T]he risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities….[30]

NERC Petition

37. Reliability Standard CIP-014-1 does not include a procedure that allows the Commission to add or subtract facilities from an applicable entity's list of critical facilities under Requirement R1. Instead, NERC states that the Commission has the existing authority to enforce NERC Reliability Standards pursuant to FPA section 215(e)(3).[31] NERC explains that a transmission owner must be able to demonstrate that its method for performing its risk assessment under Requirement R1 "was technically sound and reasonably designed to identify its critical Transmission stations and Transmission substations."[32] NERC maintains that if "in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity or

[30] March 7 Order, 146 FERC ¶ 61,166 at P 11.

[31] NERC Petition at 37.

[32] *Id.*

[the Commission] finds that the entity's transmission analysis was patently deficient and the Requirement R2 verification process did not cure those deficiencies, they could use their enforcement authority to compel Transmission Owners to re-perform the risk assessment using assumptions designed to identify the appropriate critical facilities."[33]

NOPR

38. The NOPR stated that Reliability Standard CIP-014-1 does not include a procedure that allows the Commission to add or subtract facilities from an applicable entity's list of critical facilities. The NOPR stated that if the Commission determined through an audit of an applicable entity, or through some other means, that a critical facility does not appear on the entity's list of critical facilities, there is no provision in Reliability Standard CIP-014-1 to allow the Commission to require its inclusion. In the NOPR, the Commission proposed to direct NERC to modify the physical security Reliability Standard to "include a procedure that would allow applicable governmental authorities, i.e., the Commission and any other appropriate federal or provincial authorities, to add or subtract facilities from an applicable entity's list of critical facilities."[34]

[33] *Id.*

[34] NOPR, 148 FERC ¶ 61,040 at P 23.

Comments

39. NERC asserts that the Commission should not adopt the NOPR proposal. NERC maintains that the proposal is unnecessary because it duplicates existing Commission compliance monitoring and enforcement authority.[35] Moreover, NERC contends that the NOPR's concerns surrounding the use of existing compliance and enforcement methods to ensure compliance with Requirement R1 are unsubstantiated. NERC states that if the NOPR proposal is adopted, then the Commission must better justify the reasons for the directive and limit and clarify the scope and content of the proposed directive.

40. Pa PUC, Foundation, SmartSenseCom and Paschall state that they support the NOPR proposal.[36] Other commenters do not oppose the proposal but maintain that it should be clarified or modified if adopted by the Commission.[37]

41. The majority of commenters do not support the NOPR proposal for various legal and policy reasons.[38] Associations' comments are representative of this viewpoint in that

[35] NERC Comments at 8 ("the Commission can use its broad enforcement authority to make certain that the applicable entity re-performs the risk assessment on whatever timeline the Commission deems appropriate or face penalties or sanctions under the FPA").

[36] Pa PUC Comments at 5; Foundation Comments at 3; SmartSenseCom Comments at 6; Paschall Comments at 2.

[37] *See* G&T Cooperatives Comments at 3-8; ITC Comments at 12; NYPSC Comments at 5-7; Pepco Comments at 5-7; Idaho Power Comments at 1-2.

[38] *See* Southern Comments at 2-7; Trade Associations Comments at 5-12; GridWise Comments at 3-9; Duke Comments at 3-5; NARUC Comments at 4; KCP&L Comments at 2-4; SDG&E Comments at 3-4; Oncor Comments at 2-3; Entergy

(continued ...)

they address: (1) the statutory authority to modify critical facility lists or otherwise allow the Commission (or any other governmental authority) an operational role in the performance of a Reliability Standard; (2) how the Commission would afford entities due process in determining whether to direct the addition or removal of facilities while still maintaining confidentiality; and (3) what constitutes "any other appropriate federal or provincial authorities" and the legal authority and advisability of delegating responsibility to another government entity. Like NERC, Associations contend that the Commission already possesses the compliance and enforcement authority to ensure that applicable entities comply with Requirement R1.[39] Specifically, Associations state that the "Commission has sufficient existing enforcement authority under the FPA to take actions to address concerns raised in the NOPR regarding the sufficiency of decisions made to identify critical facilities under CIP-014-1 … includ[ing] the use of traditional enforcement authority under Section 215(e)(3), including audits and investigations,

---

Comments at 1; TAPS Comments at 3-9; APS Comments at 2-3; BPA Comments at 2; SCE Comments at 2; Ohio PUC Comments at 3-4; TVA Comments at 6-9; CEA Comments at 3-9; NU Utilities Comments at 1.

[39] Associations Comments at 9; *see also* TAPS Comments at 5 ("If the Commission finds a Registered Entity's risk assessment study to be inadequate because it lacks a critical facility, the Registered Entity will be in violation of [Requirement] R1 of the Physical Security standard … [t]he Commission could then direct a specific method of compliance … and impose daily penalties until the Registered Entity complies. If despite the threat of penalties, the Commission were concerned about the need for timely action, it could order the Registered Entity to come into compliance within a specified reasonable timeframe.").

which it has used on several occasions."[40] Associations also request a technical conference in two years that addresses the implementation of Reliability Standard CIP-014-1.

Commission Determination

42. Based on our review of the comments, we determine not to adopt the NOPR proposal.

43. We are persuaded by commenters that the NOPR directive would present NERC, as the entity that would have to develop the proposed modification, and the Commission, which would have to approve any NERC proposal, with a number of substantial policy issues. Ultimately, we believe that the NOPR proposal would require NERC and the Commission to expend resources that could be better applied elsewhere.

44. The Commission, instead, will focus its resources on carrying out compliance and enforcement activities to ensure that critical facilities are identified under Requirement R1. In its comments, NERC indicated that NERC staff will submit to the NERC Board of Trustees a report three months following implementation of Requirements R1, R2 and R3 concerning the scope of facilities identified as critical, including the number of facilities identified as critical and their defining characteristics.[41] NERC also committed

[40] Associations Comments at 9.

[41] NERC Comment at 27-28. NERC's post-implementation reports are further discussed below.

to sending this report to Commission staff.[42] Based on the results reported by NERC, we expect Commission staff to audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities. At this time, we will not direct Commission staff to convene a technical conference on implementation of Reliability Standard CIP-014-1 in two-years' time, as requested by Associations. We may revisit that proposal at a later time.

C. Informational Filing on "High Impact" Control Centers

March 7 Order

45. The March 7 Order stated that a "critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[43] The March 7 Order, while not mandating that a minimum number of facilities be deemed critical under the physical security Reliability Standards, explained that the "Commission

[42] *Id.* at 28.

[43] March 7 Order, 146 FERC ¶ 61,166 at P 6.

expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."[44]

NERC Petition

46. NERC states that Reliability Standard CIP-014-1 addresses the protection of primary control centers, which NERC defines as facilities that "operationally control[] a Transmission station or Transmission substation when the electronic actions from the control center can cause direct physical actions at the identified Transmission station or Transmission substation, such as opening a breaker."[45]

47. NERC maintains that "[c]ontrol centers that provide back-up capability and control centers that cannot operationally control a critical Transmission station or Transmission substation do not present similar direct risks to Real-time operations if they are the target of a physical attack," and thus they are not covered by Reliability Standard CIP-014-1.[46] NERC explains that the destruction of a back-up control center would "have no direct reliability impact in Real-time as the entity can continue operation … from its primary control center."[47] With respect to control centers that do not physically operate Bulk-Power System facilities, such as control centers operated by reliability

[44] *Id.* P 6, n.6.

[45] NERC Petition at 19.

[46] *Id.*

[47] *Id.* at 20.

coordinators, NERC states that, while "certain monitoring and oversight capabilities might be lost as a result of a physical attack on such control centers, the Transmission Owner or Transmission Operator that operationally controls the critical Transmission station or Transmission substation would be able to continue operating its transmission system to prevent widespread instability, uncontrolled separation, or Cascading within an Interconnection."[48]

48. NERC acknowledges that certain control centers categorized as "High Impact" or "Medium Impact" under Reliability Standard CIP-002-5.1 (Cyber Security — BES Cyber System Categorization) would not be covered control centers under Reliability Standard CIP-014-1.[49] NERC explains that this situation:

> reflects the different nature of cyber security risks and physical security risks at control centers … [a] primary cyber security concern for control centers is the corruption of data or information and the potential for operators to take action based on corrupted data or information … [and] [t]his concern exists at control centers that operationally control Bulk-Power System facilities and those that do not. As such, there is no distinction in CIP-002-5.1 between these control centers … however, such a distinction is appropriate in the physical security context.[50]

49. NERC points out that Reliability Standard CIP-006-5 already requires physical security protections that are "designed to restrict physical access to locations containing

---

[48] *Id.* at 20-21.

[49] Reliability Standard CIP-002-5.1 (Cyber Security – BES Cyber System Categorization), Attachment 1 (Impact Rating Criteria).

[50] NERC Petition at 22 n.55.

High and Medium Impact Cyber Systems," which include control centers and backup control centers for reliability coordinators, balancing authorities, transmission operators and generation operators irrespective of their ability to operationally control Bulk-Power System facilities.[51]

NOPR

50. The NOPR proposed to direct NERC to make an informational filing within six months of the effective date of a final rule in this proceeding indicating whether the development of Reliability Standards that provide physical security for all "High Impact" control centers, as that term is defined in Reliability Standard CIP-002-5.1, is necessary for the reliable operation of the Bulk-Power System.

51. The NOPR stated that primary and back-up control centers of functional entities other than transmission owners and operators identified as "High Impact" may warrant assessment and physical security controls under this Reliability Standard because a successful attack could prevent or impair situational awareness, especially from a wide-area perspective, or could allow attackers to distribute misleading and potentially harmful data and operating instructions that could result in instability, uncontrolled separation, or cascading failures.

52. The NOPR stated that the proposed informational filing should address whether there is a need for consistent treatment of "High Impact" control centers for cybersecurity

[51] *Id.* at 21.

and physical security purposes through the development of Reliability Standards that afford physical protection to all "High Impact" control centers. The NOPR also stated that the development of physical security protections for all "High Impact" control centers would not be without precedent because, as noted above, Reliability Standard CIP-006-5 already requires that "High Impact" control centers have some physical protections, including restrictions on physical access, to protect BES Cyber Assets. However, the NOPR further stated that the security measures required by Reliability Standard CIP-006-5 may not be comparable to those required by Reliability Standard CIP-014-1, and thus may not be sufficient to "deter, detect, delay, assess, communicate, and respond to potential threats and vulnerabilities" as required in Requirement R5 of Reliability Standard CIP-014-1. Further, the NOPR stated that Reliability Standard CIP-006-5 does not require an "unaffiliated third party review" of the evaluation and security plan required by Reliability Standard CIP-014-1.

Comments

53. NERC states that it does not oppose submitting an informational filing to address whether "High Impact" control centers warrant assessment and physical security controls under Reliability Standard CIP-014-1. However, NERC requests that the Commission modify the NOPR proposal to give NERC at least 12 months from the effective date of a final rule in this proceeding to submit the informational filing.

54. Other commenters, while not necessarily agreeing that all "High Impact" control centers should be subject to Reliability Standard CIP-014-1, support the NOPR proposal for various reasons.[52] Associations state that the informational filing "will provide a more granular mapping of the strategic considerations embedded in the CIP standards … as well as consideration of the issues relating to control centers not covered by CIP-014-1."[53] MISO and SDG&E state that the informational filing could be a useful way for identifying areas of possible improvement in the future. Some commenters, including Associations, recommend that the Commission direct NERC to submit the informational filing as critical energy infrastructure information (CEII).

55. ITC supports the proposed informational filing but states that the Commission should widen the scope of the informational filing to assess the benefits of extending Reliability Standard CIP-014-1 to all "High Impact" and "Medium Impact" BES Cyber Assets. ITC states that the definition of "critical" assets is insufficiently comprehensive because it fails to provide physical security for facilities that contain crucial Cyber Assets. ITC further states that identifying critical facilities under Requirement R1 is unnecessary because applicable entities already have a list of facilities containing "High Impact" and "Medium Impact" Cyber Assets, which could also serve as the list of critical

[52] *See* Associations Comments at 16; KCP&L Comments at 4; Foundation Comments at 7; SDG&E Comments at 5; Pa PUC Comments at 6; SCE Comments at 4; MISO Comments at 6-7.

[53] Associations Comments at 16.

facilities for the purposes of Reliability Standard CIP-014-1. SIA agrees that Requirement R1 should be modified to include all "High Impact" control centers.

56. Commenters opposed to the NOPR proposal contend that the informational filing is unnecessary or would be burdensome.[54] Trade Associations state that Reliability Standard CIP-014-1 correctly focuses on the protection of primary control centers that operationally control transmission stations or substations identified under Requirement R1. Idaho Power states that Reliability Standard CIP-006-5 contains enough physical access controls to meet the expectations of "deter, detect, delay, assess, communicate, and respond" because there are extensive monitoring and alerting requirements that must be applied to all "High Impact" control centers. Reclamation states that Reliability Standard CIP-014-1 will capture all "High Impact" control centers as currently drafted. Pepco states that an informational filing would divert resources from implementation and compliance with Reliability Standard CIP-014-1.

Commission Determination

57. The Commission adopts the NOPR proposal and directs NERC to submit an informational filing that addresses whether there is a need for consistent treatment of "High Impact" control centers for cybersecurity and physical security purposes through the development of Reliability Standards that afford physical protection to all "High Impact" control centers. The Commission, however, modifies the NOPR proposal and

[54] Trade Associations Comments at 12; Pepco Comments at 7.

extends the due date for the informational filing to two years following the effective date of Reliability Standard CIP-014-1.

58. While we approve Reliability Standard CIP-014-1 in this final rule, including the Reliability Standard's treatment of control centers, the Commission, for the reasons set forth in the NOPR, finds that NERC should assess whether all "High Impact" control centers should be protected under Reliability Standard CIP-014-1.[55] We recognize that NERC and applicable entities will be in a better position to provide this assessment after implementation of Reliability Standard CIP-014-1 and Reliability Standard CIP-006-5, the latter of which provides some physical protection to "High Impact" control centers. Accordingly, the Commission directs NERC to submit the informational filing two years following the effective date of Reliability Standard CIP-014-1. The Commission, while not directing NERC to submit the informational filing as CEII, recognizes the concerns raised by commenters regarding confidentiality. The Commission expects NERC to prepare the informational filing and submit it in such a way as to protect any critical information from public disclosure.

59. At this time, the Commission will not direct NERC to address in the informational filing whether all "High Impact" and "Medium Impact" BES Cyber Assets should be considered critical for the purposes of Reliability Standard CIP-014, Requirement R1. We are sympathetic to several points raised in ITC's comments, which echo some of the

[55] *See* NOPR, 148 FERC ¶ 61,040 at PP 35-39.

statements in the NOPR. However, as stated in the NOPR, the basis for directing an informational filing regarding control centers is found in the March 7 Order, where the Commission stated that it "expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."[56] While NERC explained why not all "High Impact" control centers may be critical for the purposes of Reliability Standard CIP-014-1, we conclude that this issue requires close attention and should be addressed in the informational filing. The broader concerns raised by ITC regarding the scope of Requirement R1 can be evaluated by NERC and industry as part of the implementation process. As we noted above, the Commission will devote resources to compliance with and enforcement of Reliability Standard CIP-014-1 to ensure that all critical facilities are identified pursuant to Requirement R1. Should the Commission find through these efforts, or through the post-implementation reports and informational filing that NERC will submit, that Requirement R1 as currently written is not capturing all critical facilities, then the Commission will act upon that information.

D. Informational Filing on Resiliency

March 7 Order

60. In the March 7 Order, the Commission stated that the development of physical security Reliability Standards "will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow

[56] NOPR, 148 FERC ¶ 61,040 at P 44 (quoting March 7 Order, 146 FERC ¶ 61,166 at P 6 n.6).

owners or operators to consider resiliency of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management."[57]

NERC Petition

61. Reliability Standard CIP-014-1 mentions resiliency in Requirement R5, stating in Requirement R5.1 that the physical security plans that entities develop shall include, among other attributes: "Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4." The NERC petition describes Requirement R5.1, with regard to resiliency, as referring to "steps an entity may take that, while not specifically targeted as hardening the physical security of the site, help to decrease the potential adverse impact of a physical attack … including modifications to system topology or the construction of a new Transmission station … that would lessen the criticality of the facility."[58]

[57] March 7 Order, 146 FERC ¶ 61,166 at P 7.

[58] NERC Petition at 42.

NOPR

62. The NOPR stated that the NERC petition describes resiliency measures that could be included in the required physical security plans. The NOPR also stated, however, that specific resiliency measures are not required by Reliability Standard CIP-014-1, which is consistent with the March 7 Order. Instead, the NOPR noted that Reliability Standard CIP-014-1 allows the security plans to be flexible in order to meet different threats and protect varying Bulk-Power System configurations.

63. The NOPR stated that resiliency is as, or even more, important than physical security given that physical security cannot protect against all possible attacks. The NOPR also stated that, in the case of the loss of a substation, the Bulk-Power System may depend on resiliency to minimize the impact of the loss of facilities and restore blacked-out portions of the Bulk-Power System as quickly as possible. The NOPR further stated that some entities may implement resiliency measures rather than security measures, such as by adding facilities or operating procedures that reduce or eliminate the importance of existing critical facilities, which could significantly improve reliability and resiliency.

64. The NOPR stated that the NERC petition indicated that the NERC Board of Trustees expects NERC management to monitor and assess the implementation of Reliability Standard CIP-014-1 on an ongoing basis, which would include: the number of assets identified as critical under the Reliability Standard; the defining characteristics of the assets identified as critical; the scope of security plans (i.e., the types of security and resiliency measures contemplated under the various security plans); the timelines included in the security plan for implementing the security and resiliency measures; and

industry progress in implementing the Reliability Standard. The NOPR also stated that NERC explained that this information could be used to provide regular updates to Commission staff.[59] The NOPR proposed to rely on NERC's ongoing assessment of Reliability Standard CIP-014-1's implementation and to require NERC to make such information available to Commission staff upon request.

65. In addition, the NOPR proposed to direct NERC to submit an informational filing that addresses the resiliency of the Bulk-Power System when confronted with the loss of critical facilities. The NOPR stated that the informational filing should explore what steps can be taken, in addition to those required by Reliability Standard CIP-014-1, to maintain the reliable operation of the Bulk-Power System when faced with the loss or degradation of critical facilities. The NOPR proposed to direct NERC to submit the informational filing within one year after the effective date of the final rule in this proceeding.[60]

[59] NOPR, 148 FERC ¶ 61,040 at P 56.

[60] NERC issued a report on severe impact resilience in 2012. *See* NERC, Severe Impact Resilience: Considerations and Recommendations (May 2012), *available at* http://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf. The NOPR stated that the proposed informational filing could draw on the report but should also reflect subsequent work and development on this topic, particularly including supply chain, transporting and other logistical issues for equipment such as large transformers. NOPR, 148 FERC ¶ 61,040 at P 57.

Comments

66. NERC requests that the Commission not direct it to submit an informational filing on resiliency. NERC contends that an informational filing on resiliency would divert resources from NERC's oversight of the implementation of Reliability Standard CIP-014-1 and NERC's efforts to assess the Reliability Standard's effectiveness. NERC states that it will monitor and assess implementation of Reliability Standard CIP-014-1, as described in NERC's petition, and will prepare two initial reports for the NERC Board of Trustees, the first report being submitted three months following implementation of Requirements R1, R2 and R3 and the second report being submitted three months after implementation of Requirements R4, R5 and R6. With respect to the second report, NERC states that "[g]iven the NOPR's discussion of resiliency, this report will pay particular attention to the resiliency measures included in entities' security plans."[61] NERC further states that it commits to provide both reports to Commission staff.

67. Pepco does not support the proposed informational filing because of the burden Pepco contends it would impose on NERC and registered entities, including diverting resources from the implementation of Reliability Standard CIP-014-1. Pepco asserts that resiliency is already addressed in Reliability Standard CIP-014-1.

[61] NERC Comments at 28.

68. SDG&E, MISO and Idaho Power support directing NERC to submit the proposed informational filing on resiliency as a way of determining next steps for enhancing the reliability of the Bulk-Power System.[62]

69. Other commenters, including Associations, while generally agreeing that the issue of resiliency needs to be considered, recommend that the Commission convene a technical conference rather than require NERC to submit an informational filing because, they maintain, a technical conference would be more effective.[63]

Commission Determination

70. The Commission determines not to adopt the NOPR proposal requiring NERC to submit an informational filing concerning resiliency of the Bulk-Power System. While commenters expressed differing views on whether an informational filing is needed, the comments recognized the importance of Bulk-Power System resiliency. In addition, NERC committed to providing the Commission with two reports following implementation of Reliability Standard CIP-014-1, which, NERC indicates, will address the issue of resiliency.

71. Rather than require NERC to submit an informational filing at this time, the Commission will review the NERC reports and will consider ways for industry to best

[62] *See* SDG&E Comments at 5; MISO Comments at 6-7; Idaho Power Comments at 4; *see also* Paschall Comments at 2.

[63] *See* Associations Comments at 17; KCP&L Comments at 6-7; SCE Comments at 4; Trade Associations Comments at 13-14; GridWise Comments at 3.

inform the Commission of its current and future resiliency efforts, which could take the form of reports and/or technical conferences to address specific areas of concern (e.g., spare parts, fuel security, and advanced technologies).

E. Third-Party Verification and Review

March 7 Order

72. In the March 7 Order, the Commission stated that "the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator ... [and] [s]imilarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise."[64]

NERC Petition

73. Requirement R2 of Reliability Standard CIP-014-1 requires transmission owners to have their risk assessments verified by an unaffiliated third party. Requirement R6, likewise, requires each transmission owner and transmission operator to have their vulnerability and threat assessment(s) along with their security plan(s) for any critical facilities reviewed by an unaffiliated third party.

74. Regarding how an applicable entity is supposed to address any recommendations by a third-party verifier, Reliability Standard CIP-014-1, in Requirement R2.3, states that the transmission owner must either (a) "modify its identification … consistent with the

[64] March 7 Order, 146 FERC ¶ 61,166 at P 11.

recommendation" or (b) "document the technical basis for not modifying the identification in accordance with the recommendation." Similarly, Requirement R6.3 sets forth the procedure for considering any recommendations from the reviewing entity as to the threat assessments and security plans: the applicable entity must either (a) "modify its evaluation or security plan(s) consistent with the recommendation" or (b) "document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation."

75. NERC states that "[r]equiring documentation of the technical basis for not modifying the identification in accordance with the recommendation will help ensure that a Transmission Owner meaningfully considers the verifier's recommendations and follows those recommendations unless it can technically justify its reasons for not doing so. To comply with Part 2.3, the technical justification must be sound and based on acceptable approaches to conducting transmission analyses."[65] The NERC petition contains a similar explanation for the third-party review (Requirement R6) of the threat assessments and security plans mandated in Requirements R4 and R5.[66]

NOPR

76. The NOPR proposed to approve the third-party verification and review method proposed by NERC in Requirements R2 and R6. The NOPR stated that failure to provide

[65] NERC Petition at 36.

[66] *Id.* at 50.

a written, technically justifiable reason for rejecting a third-party recommendation would render the applicable entity non-compliant. With that understanding, the NOPR proposed to approve NERC's proposed third-party verification and review in Requirements R2 and R6 of Reliability Standard CIP-014-1 as an equally efficient and effective alternative to the directive in the March 7 Order.

Comments

77. NERC states that it supports the NOPR proposal. NERC states that third-party verification and review will provide another layer of expertise and independence to the identification of critical assets, the evaluation of threats and vulnerabilities, and the development of effective security plans. NERC reiterates that an applicable entity's failure to provide a reasonable, written explanation for declining to follow a third-party recommendation would constitute non-compliance.

78. MISO, Reclamation, KCP&L, ITC, and G&T Cooperatives support the NOPR proposal but each suggest modifications or request clarification of Reliability Standard CIP-014-1.[67]

79. MISO states that entities like itself, that are both reliability coordinators and planning coordinators, may be subject to substantial, simultaneous demands by many transmission owners for concurrent verification of risk assessments. MISO notes that Requirement R2.2 requires applicable entities to have their risk assessment verified

[67] *See also* Paschall Comments at 2; Foundation Comments at 7.

within 90 days of completion of the risk assessment. MISO states that firm adherence to the 90-day deadline could undermine the protections in Reliability Standard CIP-014-1 by requiring verifying entities (e.g., MISO) to conduct hurried or shorter-than-optimal assessments. Accordingly, MISO seeks clarification that NERC has the discretion to extend the implementation deadline, especially with respect to the 90-day verification deadline in Requirement R2.2. Likewise, G&T Cooperatives, NIPSCO and KCP&L state that there should be flexibility regarding the 90-day deadline because of the limited pool of qualified third-party verifiers.

80. Reclamation states that transmission owners should have discretion to make decisions regarding third-party recommendations based on cost and risk analyses. Reclamation also states that Requirement 2.1 should be modified to require that third-party verifications be conducted by a transmission owner's planning coordinator or transmission planner. If the transmission owner is also the planning coordinator and transmission planner, then Reclamation states that the verification should be conducted by the reliability coordinator.

81. KCP&L states that NERC should develop a pre-approved list of qualified third-party contractors or require third parties to register with NERC. KCP&L also seeks clarification that an independent system operator (ISO) or regional transmission operator (RTO) concurrent with its role as reliability coordinator could provide third-party review services. KCP&L states that it does not oppose having an RTO that is also a reliability coordinator or planning coordinator serve as a third-party reviewer but would not support

a mandate requiring a specific third-party reviewer. KCP&L also seeks clarification of the meaning of the phrase "unaffiliated third-party."

82. ITC states that the Commission should "confirm that the verification of a responsible entity's risk assessment, threat assessment, and security plan, as specified in Requirements R2 and R6, constitutes full compliance by that responsible entity with respect to the risk assessment and security plan."[68]

83. NIPSCO, TVA and Idaho Power do not support the NOPR proposal. NIPSCO contends that third-party verification is "inconsistent with the approach to entity self-assessment applied in other Reliability Standards" and notes that the Version 5 CIP Reliability Standards do not include a provision for third-party review.[69] NIPSCO also contends that the use of third parties could raise confidentiality concerns. Idaho Power maintains that the proposal should not be adopted because it does not require third parties to include a written or technical justification with their recommendations. Idaho Power also states that "if a third-party verification and review process is incorporated in to the Standard, it should clearly describe the specific methodology and performance criteria to be applied."[70] TVA states that FPA section 215 does not contemplate the use of third-party verifiers and reviewers acting in an enforcement role. TVA also contends that

[68] ITC Comments at 10.

[69] NIPSCO Comments at 2.

[70] Idaho Power Comments at 3-4.

Reliability Standard CIP-014-1 does not contain any qualification criteria that third-party verifiers and reviewers must meet. TVA further states that using third-party verifiers and reviewers could compromise the confidentiality of critical information.

Commission Determination

84. We adopt the NOPR proposal and approve the third-party verification and review provisions found in Requirements R2 and R6 of Reliability Standard CIP-014-1. These provisions, as stated by NERC, provide an important, independent layer of expertise in the identification, assessment and protection of critical facilities.

85. We disagree with the arguments raised in the comments submitted by NIPSCO, TVA and Idaho Power. The use of third-party verification and review in Reliability Standard CIP-014-1 is not inconsistent with other Commission-approved Reliability Standards merely because third-party review is not used in other Reliability Standards. NIPSCO is correct that the Version 5 CIP Reliability Standards do not include third-party review provisions. However, as NIPSCO acknowledges, the Version 5 CIP Reliability Standards contain bright-line criteria that guide the determinations made by applicable entities in identifying BES Cyber Assets.[71] By contrast, Reliability Standard CIP-014-1 contains no such criteria and instead requires applicable entities to develop their own

[71] We also note that in Order No. 706, the Commission directed NERC to develop an external review procedure for the identification of critical assets by responsible entities. *See Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at PP 322-329, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

analysis. In addition, the threat evaluation in Requirement R4 and security plan in Requirement R6 involve areas of expertise that applicable entities in the electric industry may not possess and thus would strongly benefit from the experience of qualified third parties.

86. Similarly, we disagree with TVA that the use of third-party verifiers and reviewers is inconsistent with FPA section 215. As discussed above, we reject TVA's view that third-party verifiers and reviewers will be acting in an enforcement capacity. These third parties will have no authority to determine whether an applicable entity has violated a requirement of Reliability Standard CIP-014-1, require compliance, or issue penalties. Moreover, as stated in the NOPR, an applicable entity in some cases could be found to be in violation of a requirement even if the applicable entity's actions were verified by a third party.[72] We also determine that the requirements in Reliability Standard CIP-014-1 (i.e., Requirements R2.1 and R6.1) establishing the qualifications for third-party verifiers and reviewers are sufficient. As discussed below, as Reliability Standard CIP-014-1 is implemented, we are satisfied that NERC and Regional Entities will provide additional assistance to applicable entities to identify qualified third-party verifiers and reviewers if the need arises. We are also satisfied that Requirements R2.4 and R6.4 provide adequate protection against the disclosure of sensitive or confidential information.

[72] NOPR, 148 FERC ¶ 61,040 at P 23.

87. In response to Idaho Power's concern, we expect that third-party verifiers and reviewers will articulate a reasonable basis for their recommendations. The absence of such a basis for a recommendation could justify an applicable entity's decision to decline to adopt the recommendation. We also see no reason to include in Reliability Standard CIP-014-1 "specific methodology and performance criteria" for third-party verification and review beyond what is already contained in the requirements and compliance measures recited in the Reliability Standard.

88. With respect to the other comments, there is no evidence in the record to support the conclusion that an insufficient number of qualified third-party verifiers and reviewers exists such that applicable entities will be unable to meet the 90-day deadline in Requirements R2 and R6. To the extent an applicable entity requires additional time to comply, that situation should be addressed on a case-by-case basis.[73] Reclamation has not explained why Requirement R2.1 should be modified to require that a transmission owner use its planning coordinator or transmission planner as a verifier, and thus we reject that proposal. In addition, addressing Reclamation's second point, while risk and cost could be aspects of an applicable entity's technical justification for declining to follow a third-party recommendation, ultimately there must be a sufficient objective basis

[73] For similar reasons, we reject Entergy's suggestion that Reliability Standard CIP-014-1 include language providing for flexibility concerning delays in compliance with deadlines contained in the Reliability Standard due to acts of nature. *See* Entergy Comments at 1.

in the justification document from which to determine that the applicable entity acted reasonably in declining to follow the recommendation.

89. With respect to KCP&L's comments, there may be value in NERC developing a list of qualified third-party verifiers and reviewers or otherwise requiring some form of registration process for third-party verifiers and reviewers. The Commission, however, will not direct NERC to do so at this time. We expect that NERC could, as Reliability Standard CIP-014-1 is implemented, pursue or, if necessary, propose such an effort if warranted. Indeed, Reliability Standard CIP-014-1 appears to contemplate such a role for NERC by indicating in Requirement R6.1 that an entity is qualified to serve as a reviewer if "approved by the ERO." In addition, we see no reason why an ISO or RTO could not serve as a third-party verifier or reviewer provided it satisfies the qualifications stated in Requirements R2.1 and R6.1. We also conclude that the term "unaffiliated third party" is sufficiently clear. As NERC stated in its petition, "the term 'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit."[74] KCP&L does not indicate what, in this explanation, is ambiguous or requires clarification.

[74] NERC Petition at 34-35.

90. With respect to ITC's comment, third-party verification under Requirement R2 adds an important layer of expertise and independence in the identification of critical facilities. However, verification under Requirement R2 is not intended to and, indeed, cannot cure an applicable entity's failure to comply with Requirement R1 if it is determined by the compliance enforcement authority that the applicable entity failed to do so, a situation that ITC concedes could happen.[75] We anticipate that a properly verified critical facility list will normally result in compliance with Requirement R1, but the Commission cannot foreclose the possibility that that may not be the case.[76]

F. Generators

March 7 Order

91. The March 7 Order did not direct NERC to make the physical security Reliability Standards applicable to specific functional entity types. The March 7 Order stated that "some of the requirements imposed by these newly proposed Reliability Standards may

[75] ITC Comments at 9 ("ITC further doesn't disagree that, in extremely dire circumstances, a risk assessment which has been verified by a third-party may nonetheless be so deficient (and the third-party review be similarly inadequate) that it could be considered non-compliant."); *see also* NERC Petition at 37 ("If, in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity, or FERC finds that the entity's transmission analysis was patently deficient and that the Requirement R2 verification process did not cure those deficiencies, they could use their enforcement authority to compel Transmission Owners to re-perform the risk assessment using assumptions designed to identify the appropriate critical facilities.").

[76] *See* Order No. 706, 122 FERC ¶ 61,040 at P 320 (denying "safe harbor" for good faith compliance with CIP Reliability Standards).

best be performed by the owner and other activity may best be performed by the operator," and that NERC should clearly indicate which entity is responsible for each requirement.[77] With regard to the applicable types of facilities, the Commission stated that it "is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards."[78]

NERC Petition

92. In explaining why the Reliability Standard does not include generator owners and generator operators as applicable entities, the standard drafting team found that:

> it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2 … Second, the transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the [March 7] order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities.[79]

[77] March 7 Order, 146 FERC ¶ 61,166 at P 6, n.4.

[78] *Id.* P 6.

[79] NERC Petition, Exhibit A (Proposed Reliability Standard) at 23. The standard drafting team provided the following example: "a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500 kV or greater or if

(continued ...)

93. NERC explains that generator owners and generator operators were not included in the applicability section because, "while the loss of a generator facility due to a physical attack may have local reliability effects, the loss of the facility is unlikely to have the widespread, uncontrollable impact" contemplated for loss of a critical facility in the March 7 Order.[80] NERC maintains that a "generation facility does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility."[81]

NOPR

94. The NOPR proposed to approve the applicability section of the Reliability Standard CIP-014-1 without the inclusion of generator owners and generator operators. The NOPR stated that omitting generator owners and generator operators from the applicability section is consistent with the March 7 Order. The NOPR affirmed the statement in the March 7 Order that the "number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power

---

it is connected at 200 kV – 499 kV to three or more other Transmission stations or Transmission substations and has an 'aggregate weighted value' exceeding 3000 according to the table in Applicability Section 4.1.1.2." *Id.* at 23.

[80] NERC Petition at 22.

[81] *Id.*

System."[82] The NOPR proposed to accept NERC's justification for excluding generator owners and operators because it is in keeping with the March 7 Order's focus on protecting the most critical facilities. The NOPR stated that, according to NERC, a generation facility "does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility."[83] The NOPR also noted that Requirement R1 mandates a transmission analysis that accounts for transmission owner- or transmission operator-owned substations that connect generating stations to the Bulk-Power System with step-up transformers.

95. While proposing to accept the applicability section of the proposed Reliability Standard, the NOPR stated that NERC's proposed omission of generator owners and generator operators could potentially exempt substations owned or operated by generators. The NOPR sought comment on the potential reliability impact of excluding generator owned or operated substations.

Comments

96. NERC states that it supports the NOPR proposal to approve the applicability criteria in Reliability Standard CIP-014-1 without the inclusion of generator owners and

[82] NOPR, 148 FERC ¶ 61,040 at P 44 (quoting March 7 Order, 146 FERC ¶ 61,166 at P 12).

[83] NOPR, 148 FERC ¶ 61,040 at P 45 (quoting NERC Petition at 22).

generator operators. NERC, reiterating the justification in the NERC petition, states that the loss of a generation facility is unlikely to result in critical impacts on the Bulk-Power System.

97. Associations, Trade Associations, Reclamation, G&T Cooperatives, KCP&L, Idaho Power, and APS also support the NOPR proposal.[84] Associations' comments are representative of the comments supportive of the NOPR proposal in that Associations state that generation facilities will be considered in Reliability Standard CIP-014-1, even without generator owners and generator operators included in the applicability criteria, because all generators interconnected to applicable transmission stations or substations will be in included in the transmission analysis under applicability sections 4.1.1.1 and 4.1.1.2.

98. Paschall states, without elaboration, that generation facilities should be included within the scope of Reliability Standard CIP-014-1. Foundation comments that it supports Reliability Standard CIP-014-1, as modified in the NOPR, and also advocates for the inclusion of certain generation facilities in a second stage physical security Reliability Standard (discussed in Section H below).

[84] Associations Comments at 16-17; Trade Associations Comments at 12-13; Reclamation Comments at 1; G&T Cooperatives Comments at 13-14; KCP&L Comments at 5; Idaho Power Comments at 3; APS Comments at 4-5.

Commission Determination

99. We adopt the NOPR proposal and approve the applicability criteria in Reliability Standard CIP-014-1 without the inclusion of generator owners and generator operators. As the Commission stated in the NOPR, we agree with NERC that a generation facility "does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility."

100. Paschall provides a conclusory statement that generation facilities should be included in Reliability Standard CIP-014-1, but does not provide a rationale for this position. Thus, we find Paschall's comments unpersuasive.

G. Confidentiality

March 7 Order

101. The March 7 Order stated that:

> All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.[85]

[85] March 7 Order, 146 FERC ¶ 61,166 at P 10.

NERC Petition

102. Reliability Standard CIP-014-1 includes two requirements addressing the concerns over confidentiality. Requirements R2.2 and R6.4, which are substantially the same, state that "[e]ach Transmission Owner shall implement procedures, such as the use of non- disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party [verifier or reviewer] and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure."

Comments

103. Associations, GridWise, Duke, Seattle, ITC, and Trade Associations state that the Commission should explicitly address the issue of confidentiality in the final rule. Associations state that the Commission should state that any data produced or collected by an RTO in accordance with a requirement of Reliability Standard CIP-014-1 are protected and should not be made available to a market monitor pursuant to a RTO tariff or market monitor agreement. Associations state that, at a minimum, a market monitor should have to make a filing with the Commission explaining the need for such information and indicating how the market monitor would protect such information from disclosure. GridWise and ITC state that they share Associations' concerns regarding confidentiality.

104. Trade Associations and Seattle comment that the final rule should contain an explicit statement that Reliability Standard CIP-014-1 is intended to preempt any state or local public disclosure laws. SWTDUG's reply comments question the Commission's

legal authority to preempt state or local public disclosure laws, as suggested by Trade Associations and Seattle, without further Congressional action.

105. Duke comments that the Commission should take all necessary steps to protect the confidential information related to the activities of applicable entities, the Commission, NERC and Regional Entities in performance of their obligations under Reliability Standard CIP-014-1. Duke states that, pursuant to the Commission's regulations, the "disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise."[86] Duke recommends interpreting this provision to include violations of Reliability Standard CIP-014-1 or to revise the regulation to do so. Duke also maintains that: (1) the risk assessment required under Requirement R1; (2) the third-party verification performed under Requirement R2; (3) the notification provided to transmission operators under Requirement R3; (4) the evaluation of threats and vulnerabilities performed under Requirement R4; (5) the development of physical security plans performed under Requirement R5; and (6) the third-party review performed under Requirement R6 all qualify as CEII. In addition, Duke states that this information is also exempt from the Freedom of Information Act under the (b)(4) exemption for "trade secrets and commercial or financial information obtained from a person and privileged or confidential."

[86] 18 CFR 39.7(b)(4).

Commission Determination

106. In the March 7 Order, the Commission recognized that compliance with the contemplated physical security Reliability Standards would likely require the development or sharing of confidential or sensitive material that, if disclosed to the public, could jeopardize the reliable operation of the Bulk-Power System. As a result, the Commission directed NERC to include adequate procedures in the Reliability Standards to prevent the dissemination of confidential or sensitive information.

107. We find that NERC has included sufficient safeguards in Reliability Standard CIP-014-1 to ensure that confidential or sensitive information produced in compliance with the Reliability Standard will not be publicly disclosed. Reliability Standard CIP-014-1 includes requirements regarding the sharing of information between applicable entities and third-party verifiers and reviewers in Requirements R2.4 and R6.4. Moreover, the "Compliance" section of Reliability Standard CIP-014-1 provides: "Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities."

108. The Commission will take all necessary and appropriate steps, as provided for in our governing statutes and regulations, to preserve an applicable entity's confidential or sensitive information when the public disclosure of such information could jeopardize the reliable operation of the Bulk-Power System. However, we decline to address in this final rule issues of preemption or the specific mechanism for treating confidential or sensitive information. Moreover, we find that it would be inappropriate to address

Associations' request concerning the disclosure of information related to compliance with Reliability Standard CIP-014-1 to market monitors pursuant to a market monitor agreement or RTO tariff. No such agreements or tariffs are before us in this rulemaking proceeding.

H. Other Issues

109. Entergy seeks clarification as to whether the requirement in Reliability Standard CIP-014-1, Requirement R5 that an applicable entity "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) . . . [and] shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s)" means that the actions called for in the security plan must be completed within 120 days. We see no ambiguity in Requirement R5 as the requirement only states that the security plan, not the actions called for in the plan, must be developed within 120 calendar days.

110. Reclamation proposes that the term "risk assessment" in Requirement R1 of Reliability Standard CIP-014-1 be changed to "impact assessment" because the requirement contemplates an assessment on the impact of the loss of facilities on the stability of the bulk electric system rather than a "risk assessment." Reclamation further states that, based on the generally accepted meaning of the term "risk assessment," that term better correlates to Requirement R4. We see no practical reason to require NERC to modify the nomenclature used in Requirement R1. Similarly, we see no reason to require NERC to change "risk assessment" to "threat risk assessment," as suggested by Paschall,

or to require NERC to define "risk assessment" because the term is largely defined in Requirement R1.

111. Foundation recommends that the Commission direct NERC to begin development of a second phase physical security Reliability Standard. Foundation maintains that such a Reliability Standard would address deficiencies in Reliability Standard CIP-014-1, including the exclusion of generation facilities and certain control centers. For example, Foundation maintains that the loss of a single generation facility could cause cascading outages on the Bulk-Power System. However, for the reasons discussed in Sections C and F above, we are not persuaded that there is a sufficient factual basis at this time to direct NERC to develop a second phase physical security Reliability Standard. While we decline to direct NERC to develop a second phase physical security Reliability Standard at this time, the informational filing on "High Impact" control centers required in this final rule, the post-implementation reports that NERC has committed to provide to the Commission, the Commission's compliance and enforcement efforts, and other outreach with NERC, industry and the public, will inform the Commission's views going forward as to what additional steps, if any, might be required to help ensure the reliable operation of the Bulk-Power System in the face of physical security threats.

I. Violation Risk Factors and Violation Severity Levels

112. Each requirement of Reliability Standard CIP-014-1 includes one violation risk factor and has an associated set of at least one violation severity level. The ranges of penalties for violations will be based on the sanctions table and supporting penalty determination process described in the Commission-approved NERC Sanction

Guidelines, according to the NERC petition. The NOPR proposed to approve the violation risk factors and violation severity levels for the requirements in Reliability Standard CIP-014-1 consistent with the Commission's established guidelines.[87] The Commission did not receive any comments regarding this aspect of the NOPR. Accordingly, the Commission approves the violation risk factors and violation severity levels for the requirements in Reliability Standard CIP-014-1.

J. Implementation Plan and Effective Date

NERC Petition

113. The NERC petition proposes that Reliability Standard CIP-014-1 become effective the "first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities" (i.e., the effective date of a final rule in this proceeding approving the proposed Reliability Standard).[88] NERC states that the initial risk assessment required under Requirement R1 must be completed by or

[87] *North American Electric Reliability Corp.*, 135 FERC ¶ 61,166 (2011).

[88] NERC Petition, Exhibit B (Implementation Plan) at 1. Exhibit B also delineates the completion timelines for Requirements R2 through R6. Parts 2.1, 2.2, and 2.4 of Requirement R2 shall be completed within 90 calendar days of the effective date of the Reliability Standard. Part 2.3 of Requirement R2 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2. Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. Parts 6.1, 6.2, and 6.4 of Requirement R6 shall be completed within 90 calendar days of completion of performance under Requirement R5. Part 6.3 of Requirement R6 shall be completed within 60 calendar days of Requirement R6 part 6.2.

before the effective date of the proposed Reliability Standard.[89] As described in the requirements of the Reliability Standard, NERC also identifies when Requirements R2, R3, R4, R5, and R6 must be complied with following the effective date of Reliability Standard CIP-014-1.

NOPR

114. The NOPR proposed to approve NERC's implementation plan and effective date for Reliability Standard CIP-014-1.

Comments

115. KCP&L states that the Commission should make it clear if the effective date of Reliability Standard CIP-014-1 will be earlier than April 2016, which KCP&L states is the effective date of Reliability Standard CIP-002-5. KCP&L states that the "basis for determination of criticality in CIP-014-1 references the same applicability as found in the CIP-002-5 … [and the] potential disconnect in implementation dates may impact registered entities adversely in preparations for Critical Infrastructure Protection standards or in application of physical security improvements given the work required to identify critical assets."[90]

[89] *Id.*

[90] KCP&L Comments at 7.

Commission Determination

116. We approve the implementation plan and effective date proposed by NERC for Reliability Standard CIP-014-1. In response to KCP&L's comment, we understand that, pursuant to the implementation plan and effective date proposed by NERC and approved herein, Reliability Standard CIP-014-1 will become effective before April 2016.

III. Information Collection Statement

117. The Paperwork Reduction Act (PRA)[91] requires each federal agency to seek and obtain Office of Management and Budget (OMB) approval before undertaking a collection of information directed to ten or more persons or contained in a rule of general applicability. OMB regulations require approval of certain information collection requirements imposed by agency rules.[92] 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 an agency 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.

Comments

118. Associations state that developing a security plan will cost more than $19,000 per company and "should include a more realistic estimate of costs to comply with the

[91] 44 U.S.C. 3501-3520.

[92] *See* 5 CFR 1320.10.

proposed standard because of the influence that the Commission's assessment may have on the judgment of state utility commission or other regulatory authorities determining the prudence of costs incurred to comply with the proposed standard."[93] Associations also state "that it understands that one medium-sized investor-owned utility anticipates that third-party contract support will cost approximately $270,000 for conducting transmission studies under R1, third-party verification under R2, analyses of threats under R4, and support for security plan development under R5."[94] Associations further state that the Commission's estimate did not include the cost of implementing the actual security measures included in applicable entity security plan. KCP&L states that it supports Associations' comments.

Commission Determination

119. We adopt the Information Collection Statement estimates contained in the NOPR. As we have previously stated, the estimates provided in an Information Collection Statement are meant to quantify the paperwork burden imposed by a final rule.[95] The

[93] Associations Comments at 19.

[94] *Id.* at 19 n.19.

[95] As defined in the PRA, "the term ''burden'' means time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for— (A) reviewing instructions; (B) acquiring, installing, and utilizing technology and systems; (C) adjusting the existing ways to comply with any previously applicable instructions and requirements; (D) searching data sources; (E) completing and reviewing the collection of information; and (F) transmitting, or otherwise disclosing the information."

Information Collection Statement is not intended to estimate the cost of compliance with the requirements of a Reliability Standard approved in a final rule.[96] Associations has not explained why it believes the Commission's paperwork burden estimate is not "realistic" or what would be a "realistic" figure other than to relate, in a footnote, that it understands that an unidentified medium-sized utility anticipates that compliance with requirements of Reliability Standard CIP-014-1, rather than the paperwork burden imposed by a final rule approving the Reliability Standard, will cost approximately $270,000. Associations' comments do not provide any creditable evidence or analysis to cause us to reevaluate the paperwork burden estimate contained in the NOPR. Accordingly, as set forth below, we adopt the NOPR's Information Collection Statement burden and cost estimates.

120. The Commission based its estimates on the number of respondents on the NERC compliance registry as of May 28, 2014. According to the registry, there are 357 transmission owners (TOs) and 197 transmission operators (TOPs). The NERC compliance registry also shows that there are only 19 transmission operators that are not also registered as a transmission owner.

121. The burden associated with the final rule is included in FERC-725U (Mandatory Reliability Standards: Reliability Standard CIP-014, OMB Control Number 1902-

[96] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160, at P 235 (2013), *order granting clarification in part and denying rehearing*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

.

0274).[97] The following table shows the Commission's burden and cost estimates, broken down by requirement and year:

FERC-725U					
Requirements in Reliability Standard CIP-014-1 over Years 1-3	**Number and Type of Respondents (1)**	**Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden Hours & Cost Per Response[98] (4)**	**Total Burden Hours & Total Cost (3)*(4)**
Year 1					
R1	357 TOs	1	357	20 $1,220	7,140 $435,540
R2	357 TOs	1	357	34 $2,342	12,138 $836,094
R3	2 TOPs	1	2	1 $128	2 $256

[97] The requirement for NERC to make the informational filing is part of the responsibilities related to being the nation-wide Electric Reliability Organization. The burden related to that filing is part of FERC-725 (OMB Control Number 1902-0225).

[98] The estimates for cost per response are derived using the following formula: Average Burden Hours per Response * XX per Hour = Average Cost per Response.

The hourly cost figures are based on data for wages plus benefits from the Bureau of Labor Statistics (as of September 4, 2014) at http://www.bls.gov/oes/current/naics3_221 000.htm and http://www.bls.gov/news.release/ecec.nr0.htm. The figures are rounded for the purposes of calculations in this table and are:

- for electrical engineers: $60.87/hr., rounded to $61/hr.
- for attorneys: $128/hr.
- for administrative staff: $31.86/hr., rounded to $32/hr.

R4	30 TOs 2 TOPs	1	32	80 $4,880	2,560 $156,160
R5	30 TOs 2 TOPs	1	32	320 $19,520	10,240 $624,640
R6	30 TOs 2 TOPs	1	32	304 $18,812	9,728 $601,984
Record Retention	357 TOs 2 TOPs	1	359	2 $64	718 $22,976
Year 2					
Record Retention	357 TOs 2 TOPs	1	359	2 $64	718 $22,976
Year 3					
R1	30 TOs	1	30	20 $1,220	600 $36,600
R2	30 TOs	1	30	34 $2,342	1,029 $70,260
R3	2 TOPs	1	2	1 $128	2 $256
R4	30 TOs 2 TOPs	1	32	80 $4,880	2,560 $156,160
R5	30 TOs 2 TOPs	1	32	80 $4,880	2,560 $156,160
R6	30 TOs 2 TOPs	1	32	134 $8,442	4,288 $270,144
Record Retention	357 TOs 2 TOPs	1	359	2 $64	718 $22,976
Year 1 Total					42,526 $2,677,650
Year 2 Total					718 $22,976
Year 3 Total					11,748 $712,556
TOTAL (for Years 1-3)					**54,992** **$3,413,182**

122. In arriving at the figures in the above table, the Commission made the following assumptions:

a. Requirement R1: We assume that responsible entities will complete the required risk assessment at approximately the same time as they complete

the assessments required under the existing TPL Reliability Standards. Accordingly, the burden for Reliability Standard CIP-014-1 only represents the documentation required in addition to what entities currently prepare. Conservatively, we assume that in the first year all transmission owners and transmission operators will complete the required risk assessment.[99] In the third year, we assume that only 30 transmission operators will be required to do another risk assessment and that the entities with critical facilities after the first risk assessment will still have critical facilities after the second risk assessment.

b. Requirement R5: We assume that developing physical security plans in the first year will be more time consuming than in later years because in later years the plans will likely only need to be updated.

123. Title: FERC-725U, Mandatory Reliability Standards: Reliability Standard CIP-014-1.

Action: Proposed Collection of Information.

OMB Control No: 1902-0274.

Respondents: Business or other for profit, and not for profit institutions.

Frequency of Responses: Ongoing.

[99] While it is likely that only large transmission owners and transmission operators will have critical facilities under Requirement R1, the Commission's estimate includes all transmission owners and operators because reliable data on what percentage of large owners and operators control critical facilities is unavailable.

Necessity of the Information: Reliability Standard CIP-014-1 implements the Congressional mandate of the Energy Policy Act of 2005 to develop mandatory and enforceable Reliability Standards to better ensure the reliability of the nation's Bulk-Power System. Specifically, Reliability Standard CIP-014-1 ensures that applicable entities with critical Bulk-Power System facilities develop and implement physical security plans to address physical security threats and vulnerabilities that could result in widespread instability, uncontrolled separation, or cascading within an Interconnection. Internal review: The Commission has reviewed Reliability Standard CIP-014-1 and has determined that the Reliability Standard is necessary to ensure the reliability and integrity of the nation's Bulk-Power System.

124. 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]. Comments on the requirements of this rule may also be sent to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission]. For security reasons, comments should be sent by e-mail to OMB at oira_submission@omb.eop.gov. Comments submitted to OMB should refer to FERC-725U and OMB Control No. 1902-0274.

IV. Environmental Analysis

125. 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.[100] 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.[101] The actions here fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act

126. The Regulatory Flexibility Act of 1980 (RFA)[102] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

127. The Small Business Administration (SBA) revised its size standard (effective January 22, 2014) for electric utilities from a standard based on megawatt hours to a standard based on the number of employees, including affiliates.[103] Under SBA's new size standards, transmission owners and transmission operators likely come under the

[100] Order No. 486, *Regulations Implementing the National Environmental Policy Act of 1969*, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Regulations Preambles 1986-1990 ¶ 30,783 (1987).

[101] 18 CFR 380.4(a)(2)(ii).

[102] 5 U.S.C. 601-612.

[103] SBA Final Rule on "Small Business Size Standards: Utilities," 78 FR 77,343 (Dec. 23, 2013).

following category and associated size threshold: Electric bulk power transmission and control, at 500 employees.[104]

128. The NOPR stated that, based on U.S. economic census data, the approximate percentage of small firms in this category is 57 percent.[105] The NOPR also stated that the Commission did not have information concerning how the economic census data compares with entities registered with NERC and is unable to estimate the number of small transmission owners and transmission operators using the new SBA definition. However, the NOPR stated that Reliability Standard CIP-014-1 only applies to transmission owners and transmission operators that own and/or operate certain critical Bulk-Power System facilities. In the NOPR, the Commission stated that it believes that Reliability Standard CIP-014-1 will be applicable to a relatively small group of large entities. No comments were received addressing the Commission's proposed certification.[106]

---

[104] 13 CFR 121.201, Sector 22, Utilities.

[105] NOPR, 148 FERC ¶ 61,040 at P 70. Data and further information are available on the SBA website. *See* SBA Firm Size Data, *available at* http://www.sba.gov/advocacy/849/12162. Since issuance of the NOPR, the Commission has obtained data that enables us to estimate more closely the number of small entities affected by this final rule. We now estimate that 28 percent (or 103 out of the 359 entities) are small entities.

[106] To the extent that Associations' comments, which we addressed above in the Information Collection Statement section, were also directed to the Commission's proposed certification regarding the Regulatory Flexibility Act, Associations' comments do not dispute any of the assumptions underlying the proposed certification or contest the proposed certification itself.

129. Accordingly, the Commission certifies that Reliability Standard CIP-014-1 will not have a significant impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

VI. Document Availability

130. 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 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington DC 20426.

131. 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.

132. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at 202-502-6652 (toll free at 1-866-208-3676) or email 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.

VII. Effective Date and Congressional Notification

133. This final rule is effective **[INSERT DATE 60 days after publication in the**

FEDERAL REGISTER]. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.[107] This final rule is being submitted to the Senate, House, and Government Accountability Office.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[107] 5 U.S.C. 804(2).

Note: The Appendix will not appear in the *Code of Federal Regulations*.

Appendix

Initial Commenters

Abbreviation	Commenter
APS	Arizona Public Service Company
Associations	Edison Electric Institute, Electric Power Supply Association, Electricity Consumers Resource Council
BPA	Bonneville Power Administration
CEA	Canadian Electricity Association
Duke	Duke Energy Corporation
Entergy	Entergy
Foundation	Foundation for Resilient Societies
GridWise	GridWise Alliance
G&T Cooperatives	Associated Electric Cooperative, Inc., Basin Electric Power Cooperative, and Tri-State Generation and Transmission Association, Inc.
Idaho Power	Idaho Power Company
ITC	International Transmission Company
KCP&L	Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company
MISO	Midcontinent Independent System Operator, Inc.
NARUC	National Association of Regulatory Utility Commissioners
NEMA	National Electrical Manufactures Association
NERC	North American Electric Reliability Corporation
NU Utilities	Northeast Utilities System
NYPSC	New York Public Service Commission
Ohio PUC	Public Utilities Commission of Ohio
Oncor	Oncor Electric Delivery Company LLC
Pa PUC	Pennsylvania Public Utility Commission
Paschall	Roger Paschall
Pepco	Pepco Holdings, Inc.
Reclamation	U.S. Department of Interior, Bureau of Reclamation
Seattle	City of Seattle
SCE	Southern California Edison
SDG&E	San Diego Gas & Electric
SIA	Security Industry Association
Southern	Southern Company Services, Inc.
TAPS	Transmission Access Policy Study Group
TVA	Tennessee Valley Authority

Trade Associations	American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association
Xcel	Xcel Energy Services Inc.

Reply Commenters

Foundation	Foundation for Resilient Societies
ITC	International Transmission Company
NIPSCO	Northern Indiana Public Service Company
SmartSenseCom	SmartSenseCom, Inc.
SWTDUG	Southwest Transmission Dependent Utility Group
Tallahassee	City of Tallahassee

149 FERC ¶ 61,139
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM14-10-000]

Real Power Balancing Control Performance Reliability Standard

(Issued November 20, 2014)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Federal Energy Regulatory Commission proposes to approve Reliability Standard BAL-001-2 (Real Power Balancing Control Performance) and proposed new definitions submitted by the North American Electric Reliability Corporation (NERC). The proposed Reliability Standard is designed to ensure that applicable entities maintain system frequency within narrow bounds around a scheduled value. In addition, the Commission proposes that NERC submit an informational filing that would address the impact of the proposed Reliability Standard on inadvertent interchange and unscheduled power flows.

DATES: Comments are due [INSERT DATE 60 days after publication in the **FEDERAL REGISTER**].

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:

Enakpodia Agbedia (Technical Information)
Office of Electric Reliability, Division of Reliability Standards
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-6750
Enakpodia.Agbedia@ferc.gov

Mark Bennett (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-8524
Mark.Bennett@ferc.gov

SUPPLEMENTARY INFORMATION:

149 FERC ¶ 61,139
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Real Power Balancing Control Performance Reliability Standard — Docket No. RM14-10-000

NOTICE OF PROPOSED RULEMAKING

(Issued November 20, 2014)

1. Under section 215 of the Federal Power Act (FPA),[1] the Commission proposes to approve Reliability Standard BAL-001-2 (Real Power Balancing Control Performance) that the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted for approval. The proposed Reliability Standard applies to balancing authorities and regulation reserve sharing groups, and is designed to maintain Interconnection frequency within predefined frequency limits. The Commission also proposes to approve the retirement of currently-effective Reliability Standard BAL-001-1 immediately prior to the effective date of BAL-001-2.

2. Further, the Commission proposes to approve NERC's four proposed definitions, associated violation risk factors and violation severity levels, implementation plan, and effective dates. The Commission also proposes that NERC submit an informational

[1] 16 U.S.C. 824(o) (2012).

filing that would address the impact of the proposed Reliability Standard on inadvertent interchange[2] and unscheduled power flows.[3]

I. Background

A. Mandatory Reliability Standards and Order No. 693 Directive

3. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards that are subject to Commission review and approval. Specifically, the Commission may approve, by rule or order, a proposed Reliability Standard or modification to a Reliability Standard if it determines that the Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest.[4] Once approved, the Reliability Standards may be enforced by NERC, subject to Commission oversight, or by the Commission independently.[5]

[2] NERC defines "Inadvertent Interchange" in the NERC Glossary of Terms Used in Reliability Standards (Glossary) as "[t]he difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. ($I_A - I_S$)"

[3] "Unscheduled power flows" generally refers to the power flows that result from the law of physics that causes power from a given source to flow over all possible paths to its destination.

[4] 16 U.S.C. 824o(d)(2).

[5] 16 U.S.C. 824o(e).

4. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[6] and subsequently certified NERC.[7] On March 16, 2007, the Commission issued Order No. 693, approving 83 of the 107 Reliability Standards filed by NERC, including BAL-001-0 and a companion standard BAL-002-0.[8] When approving BAL-002-0, the Commission directed NERC "to modify this Reliability Standard to define a significant deviation and a reportable event, taking into account all events that have an impact on frequency, e.g., loss of supply, loss of load and significant scheduling problems, which can cause frequency disturbances and to address how balancing authorities should respond."[9]

B. Proposed Reliability Standard BAL-001-2

5. On April 2, 2014, NERC filed a petition (Petition) seeking approval of proposed Reliability Standard BAL-001-2, four new definitions to be added to the Glossary of Terms used in NERC Reliability Standards (NERC Glossary of Terms) and the

[6] *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).

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

[8] *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). The Commission approved Reliability Standard BAL-001-1 in an unpublished letter order, October 16, 2013 in Docket No. RD13-11-000.

[9] *Id.* P 355.

associated violation risk factors and violation severity levels, effective dates, and implementation plan.[10] NERC states that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest because it satisfies the factors set forth in Order No. 672, which the Commission applies when reviewing a proposed Reliability Standard.[11] Also, NERC asserts that proposed Reliability Standard BAL-001-2 addresses the Commission's Order No. 693 directive pertaining to BAL-002-0.

6. NERC proposes to revise Reliability Standard BAL-001-2 by replacing the Control Performance Standard 2 (CPS2) in currently-effective Requirement R2 with a new term, "Balancing Authority ACE Limit (BAAL)."[12] The Balancing Authority ACE Limit, unique for each balancing authority, contains dynamic limits as a function of Interconnection frequency and provides the basis for a balancing authority's obligation to balance its resources and demand in real-time so that its clock-minute average ACE does

[10] Proposed Reliability Standard BAL-001-2 is available on the Commission's eLibrary document retrieval system in Docket No. RM14-10-000 and on the NERC website, www.nerc.com.

[11] NERC Petition at 6 and Exhibit C (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 323-335, 444).

[12] Area Control Error (ACE) is the instantaneous difference between a Balancing Authority's Net Actual and Scheduled Interchange, taking into accounts the effects of Frequency Bias, correction for meter error, and Automatic Time Error Correction, if operating in that mode.

not exceed its Balancing Authority ACE Limit for more than 30 consecutive clock-minutes.[13]

7. Proposed Reliability Standard BAL-001-2 has two requirements and two attachments containing the mathematical equations for calculating the Control Performance Standard 1 (CPS1) in Requirement R1,[14] the Balancing Authority ACE Limit in Requirement R2, and associated measures. NERC states that the only proposed change to Requirement R1 is to move the equation and explanation of the individual components of CPS1 to Attachment 1. NERC explains that the proposed revisions to Requirement R1 "are administratively efficient and clarify the intent of the Requirement."[15] NERC states that the "underlying performance aspect" of Requirement R1 remains the same: "to measure how well a Balancing Authority is able to control its generation and load management programs, as measured by its ACE, to support its Interconnection's frequency over a rolling one-year period."[16]

8. Proposed Requirement R2 is new and replaces the existing Control Performance Standard 2 requirement. The current Reliability Standard BAL-001-1 Requirement R2 requires each balancing authority to operate such that for at least 90 percent of the ten-

[13] NERC Petition at 12.

[14] The "Responsible Entity" designated in proposed Reliability Standard BAL-001-2 Requirement R1 is the balancing authority and/or regulation reserve sharing groups.

[15] NERC Petition at 11.

[16] *Id.*

minute periods in a calendar month (using six non-overlapping periods per hour), the average area control error (ACE) must be within a specific limit, referred to as L_{10}.[17]

9. Requirement R2 of the proposed Reliability Standard BAL-001-2 states:

> Balancing Authority shall operate such that its clock-minute average of Reporting ACE does not exceed its clock-minute Balancing Authority ACE Limit (BAAL) for more than 30 consecutive clock-minutes, calculated in accordance with Attachment 2, for the applicable Interconnection in which the Balancing Authority operates.

10. NERC explains that the Balancing Authority ACE Limits are unique for each balancing authority and provide dynamic limits for the balancing authority's ACE value as a function of its Interconnection frequency.[18] NERC states that the proposed Reliability Standard is intended to enhance the reliability of each Interconnection by maintaining frequency within predefined limits under all conditions. Furthermore, NERC states that proposed Reliability Standard BAL-001-2 and accompanying definitions include the benefits of the Automatic Time Error Correction (ATEC) equation in the WECC-specific regional variance in Reliability Standard BAL-001-1.[19]

11. NERC also proposes violation risk factors and violation severity levels for each requirement of the proposed Reliability Standard and an implementation plan and

---

[17] Reliability Standard BAL-001-1 *available at*: http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-001-1.pdf.

[18] NERC Supplemental Filing at 1.

[19] NERC Petition at 2.

effective dates. NERC states that these proposals were developed and reviewed for consistency with NERC and Commission guidelines.

12. NERC proposes an effective date for the proposed Reliability Standard that is the first day of the first calendar quarter that is twelve months after the date of Commission approval. NERC states that its proposed implementation date will allow entities to make any software adjustment that may be required to perform the Balancing Authority ACE Limit calculations.[20]

13. On May 9, 2014, NERC submitted a supplemental filing (Supplemental Filing) to address the status of the Commission directive in Order No. 693 pertaining to Reliability Standard BAL-002-0 and update the Commission regarding the status of a field trial undertaken for proposed Reliability Standard BAL-001-2.[21] In its Supplemental Filing, NERC reiterates the importance of the proposed revision establishing dynamic limits for a balancing authority's ACE as a function of the Interconnection frequency, stating that "[o]ne of the reliability benefits of the proposed Reliability Standard is that it allows Balancing Authorities to calculate their position within these boundaries on a real-time basis and take action to support reliability."[22] Further, NERC states that proposed Reliability Standard BAL-001-2 addresses the Commission's directive related to

[20] NERC Petition at 3.

[21] NERC Supplemental Filing at 1.

[22] *Id.* at 2.

BAL-002-0 "in an equally efficient and effective manner"[23] NERC adds that revisions to Reliability Standard BAL-002-1 are currently being developed and will complement proposed Reliability Standard BAL-001-2 that is the subject of the immediate proceeding.[24] Regarding the ongoing field trial, NERC stated that "the widespread participation of Balancing Authorities has provided insight into how the changes in proposed Reliability Standard BAL-001-2 will impact reliability."[25]

14. On July 31, 2014, NERC submitted an informational filing (Informational Filing) of its Preliminary Field Trial Report (Field Trial Report) evaluating the effects of proposed Reliability Standard BAL-001-2. NERC states that the Field Trial Report results to date demonstrate that the correlation between Requirements R1 and R2 of proposed Reliability Standard BAL-001-2 drive corrective actions to support Interconnection frequency and reliability.[26] NERC also states that the Balancing

[23] *Id.* at 3.

[24] The Commission notes that the currently-effective Reliability Standard BAL-002-1 requires balancing authorities to return its ACE to zero within 15 minutes following a reportable disturbance. However, the Field Trial Report does not provide any information whether compliance with Reliability Standard BAL-002-1 had any impact on the proposed Balancing Authority ACE Limits in Reliability Standard BAL-001-2. Any future modifications to BAL-002 should take this into consideration.

[25] NERC Supplemental Filing at 6, noting that 47 balancing authorities participated in the Field Trial Report: 16 in the Eastern Interconnection, 29 in the Western Interconnection, ERCOT and Quebec.

[26] NERC Field Trial Report at 1.

Authority ACE Limit, in conjunction with currently-effective Reliability Standard BAL-003-1 (Frequency Response and Frequency Bias Setting), satisfies the directive.[27]

II. Discussion

15. Pursuant to FPA section 215(d)(2), we propose to approve Reliability Standard BAL-001-2 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We propose to approve NERC's four proposed definitions, violation risk factor and violation severity level assignments, and the retirement of currently-effective BAL-001-1.[28] Likewise, we propose to approve NERC's implementation plan, in which NERC proposes an effective date of the first day of the first calendar quarter, twelve months after the date of Commission approval.[29]

16. The purpose of proposed Reliability Standard BAL-001-2 is to control Interconnection frequency within defined limits. Proposed Reliability Standard BAL-001-2 includes both long and short term performance measures for Interconnection frequency control by providing dynamic (i.e., real-time) limits that are specific for each balancing authority and Interconnection. By basing Balancing Authority ACE Limits on

[27] *Id.* at 14.

[28] NERC proposes four definitions for inclusion in the Glossary of Terms Used in NERC Reliability Standards: Regulation Reserve Sharing Group, Reserve Sharing Group Reporting ACE, Reporting ACE, and Interconnection. As stated in Exhibit G, Consideration of Comments at 13, "Regulation Reserve Sharing Group" would be added to the NERC Compliance Registry prior to implementation of the proposed standard.

[29] NERC Petition Exhibit B at 4.

pre-defined frequency trigger limits for each Interconnection, we believe the real-time measurements established in proposed Reliability Standard BAL-001-2 will help ensure the Interconnection frequency returns to a reliable state should a balancing authority's ACE, or the Interconnection's frequency, exceed acceptable bounds.

17. We agree with NERC's assertion that the Balancing Authority ACE Limit is a real-time measure of a balancing authority's required performance and encourages operation in support of the Interconnection frequency and drives corrective action back within predefined ACE limits when helpful for adjusting Interconnection frequency.[30]

18. Further, we believe that the NERC proposal satisfies the directive set forth in Order No. 693 that NERC modify Reliability Standard BAL-002 "…to define a significant deviation and a reportable event, taking account all events that have an impact on frequency, e.g., loss of supply, loss of load and significant scheduling problems…."[31] In particular, we believe that NERC's statement that the Balancing Authority ACE Limit, in conjunction with currently-effective Reliability Standard BAL-003-1, satisfies the directive.[32] We also believe that Reliability Standard BAL-003-1 addresses the Commission's Order No. 693 directive with regard to events that have an impact on frequency due to the loss of supply and proposed Reliability Standard BAL-001-2

[30] NERC Field Trial Report at 23**.**

[31] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 355.

[32] NERC Field Trial Report at 4.

addresses aspects of the same directive with regard to loss of load. Further, we accept NERC's explanation that proposed Reliability Standard BAL-001-2 addresses the Commission's Order No. 693 directive with regard to the need to more broadly define reportable events and that the proposed standard sets a variable joint megawatt limit (i.e., real-time) that is dependent on concurrent Interconnection frequency. With regard to the aspect of the Order No. 693 directive requiring that reportable events account for loss of load, we agree with NERC's statement that loss of load can cause a mismatch in supply and demand that results in a positive change in frequency.[33] We accept NERC's explanation that the Balancing Authority ACE Limit has been shown to be effective in limiting the duration that the Interconnection frequency is impacted by loss of supply, loss of load or any other conditions causing a balancing authority to exceed its Balancing Authority ACE Limit.[34]

19. In sum, we believe the statements in NERC's Petition, Supplemental Filing, and Informational Filing provide sufficient technical support that NERC has addressed the Commission's Order No. 693 directive in an equally and effective manner.[35] While we propose to approve Reliability Standard BAL-001-2, we also propose that NERC submit an informational filing - discussed immediately below - regarding the potential of

[33] *Id*. at 7.

[34] *Id.* at 27.

[35] NERC Supplemental Filing at 3.

proposed Reliability Standard BAL-001-2 to contribute to unscheduled power flows and inadvertent interchange.

Potential for Proposed Reliability Standard BAL-001-2 to Contribute to Unscheduled Power Flows and Inadvertent Interchange

20. NERC states that, as a proof of concept for the Balancing Authority ACE Limit requirement, a field trial was endorsed by the NERC Operating committee and subsequently approved by the NERC Standards Committee in June 2005.[36] During the development of the proposed Reliability Standard, some stakeholders that participated in the field trial commented to the NERC standard drafting team that the proposed Balancing Authority ACE Limit established in Requirement R2 of BAL-001-2 has caused increased system operating limit violations, particularly in the Western Interconnection. For example, one large transmission operator commented that the proposed Balancing Authority ACE Limit could increase the number of system operating limit violations, and could possibly cause large unscheduled power flows resulting in an increased ACE.[37] Another NERC stakeholder commented that the proposed Reliability Standard could provide opportunities for entities to create unscheduled power flows within the standard's boundaries, without regard to the impacts and which could lead to system operating limit violations due to large ACEs.[38] The same stakeholder commented

[36] *Id*. at 3.

[37] NERC Petition, Exhibit G, Consideration of Comments April 2013, at 43.

[38] *Id.* at 77.

that the Western Electricity Coordinating Council has decided to apply a limit of four times a balancing authority's L_{10} to limit ACE deviations from balancing authority flows that negatively impact the transmission system.

21. In addition, in the Field Trial Report, NERC asserts that there is no relationship between the Balancing Authority ACE Limit field trial and accumulated inadvertent interchange in either the Eastern or Western Interconnections.[39] However, due to a large allowance in ACE deviations in real-time while still complying with the proposed Balancing Authority ACE Limit, an increase in the amount of inadvertent interchange on the bulk electric system of all Interconnections may result.[40] In other words, proposed BAL-001-2 could allow balancing authorities to have a very large deviation from an ACE of zero and still be compliant with the dynamic values of the Balancing Authority ACE Limits in the proposed Reliability Standard.

22. The Commission is concerned that the Balancing Authority ACE Limit in proposed Reliability Standard BAL-001-2 may have an unintended consequence of (i) allowing significant amounts of unscheduled power flows, creating an undue burden for transmission operators and reliability coordinators to address power flows approaching or exceeding system operating limits or interconnection reliability operating

[39] NERC Field Trial Report at 20.

[40] A comparison between the existing Control Performance Standard 1 curves and the Balancing Authority ACE Limit curves shown in NERC's Field Trial Report indicates that there are large ACE deviations at the boundaries of 60 +/- 0.02 Hz. *Id.* Figure 5 at 24.

limits, and (ii) the significant increase in inadvertent interchange could result in an adverse reliability impact between real-time operations and day and/or hour-ahead analysis performed by reliability coordinators and transmission operators.

23. Based on the concerns discussed above, the Commission proposes to direct that NERC submit an informational filing following implementation of the proposed Reliability Standard to monitor unscheduled power flows and inadvertent interchange in the Western and Eastern Interconnections. Specifically, for the two-year period following implementation (i.e., the effective date) of the standard, the Commission proposes to direct NERC to provide the number of SOL/IROL violations, the date and time, location, the duration and magnitude, due to unscheduled power flows and inadvertent interchange within Western and the Eastern Interconnections. This information will provide NERC, the Commission, and other interested entities with the material to evaluate the effect of Reliability Standard BAL-001-2 on unscheduled power flows and inadvertent interchange and the resulting consequences on the Bulk-Power System. Accordingly, the Commission proposes to direct that NERC provide data on unscheduled power flows and inadvertent interchange for a two-year period following implementation of the proposed Reliability Standard.

24. The Commission proposes to direct NERC to submit the informational filing 90 days after the end of the two-year period following implementation. Should the data indicate reliability issues due to increases in unscheduled power flows and inadvertent interchange under the new Balancing Authority ACE Limit at any time during the two-year period of study, the Commission expects that NERC will immediately propose and

implement adequate remedies. The Commission seeks comments from NERC, and other interested entities on the proposed informational filing. The Commission also seeks comment whether any additional data would support the analysis and, thus, should be provided with the informational filing. Furthermore, the Commission also seeks comment on whether a regional variance would be necessary for those regions that experienced adverse impacts during the field trial due to inadvertent interchange.[41]

III. Information Collection Statement

25. The Office of Management and Budget (OMB) regulations require that OMB approve certain reporting and recordkeeping (collections of information) imposed by an agency.[42] 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.

26. The Commission is submitting these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of the PRA. Comments are solicited on the Commission's need for this information, whether the information will have practical utility, the accuracy of the provided burden estimate, ways to enhance the

[41] The Western Interconnection applies a limit of four times a balancing authority's L_{10} to limit ACE deviations from balancing authority flows that negatively impact the transmission system. *Id.* at 14.

[42] 5 C.F.R. 1320.11.

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.

27. This Notice of Proposed Rulemaking proposes to approve revisions to Reliability Standard BAL-001-2. NERC states in its petition that the proposed Reliability Standard defines a new concept: Balancing Authority ACE Limit, which is unique for each balancing authority and provides dynamic limits for a balancing authority's ACE value as a function of the Interconnection frequency.[43] NERC states that the proposed Reliability Standard improves reliability by adding a frequency component to the measurement of a balancing authority's ACE, and allows for the formation of "Regulation Reserve Sharing Groups." NERC's proposed Reliability Standard requires a balancing authority to balance its resources and demand in real-time so that the clock-minute average of its ACE does not exceed its Balancing Authority ACE Limit for more than 30 consecutive clock-minutes. Furthermore, NERC states that proposed Reliability Standard BAL-001-2 and accompanying definitions include the benefits of the Automatic Time Error Correction equation in the WECC-specific regional variance in Reliability Standard BAL-001-1.[44] The proposed Reliability Standard and related reporting requirements are applicable to balancing authorities and regulation reserve sharing groups.

[43] NERC Petition at 12.

[44] *Id.* at 2.

28. Public Reporting Burden: Our estimate below regarding the number of respondents is based on the NERC Compliance Registry as of October17, 2014. According to the NERC Compliance Registry, there are 71 balancing authorities in the Eastern Interconnection, 34 balancing authorities in the Western Interconnection and one balancing authority in the Electric Reliability Council of Texas (ERCOT). The Commission bases individual burden estimates on the time needed for balancing authorities to develop tools needed to facilitate reporting that are required in the Reliability Standard. These burden estimates are consistent with estimates for similar tasks in other Commission-approved Reliability Standards. The following estimates relate to the requirements for this Notice of Proposed Rulemaking in Docket No. RM14-10-000.

RM14-10-000 Final Rule (BAL-001-2: Real Power Balancing Control Performance) [45]						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response (4)**	**Total Annual Burden Hours & Total Annual Cost [46] (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**
BA/RRSG:[47] Update and Maintain Energy Management Systems	106	1	106	8 hours per response $1030 (8 x $128.76)	848 (106*8) $109,180 (1030*106)	$1030
BA: Record Retention [48]	106	1	106	4 $112	424 $11,872	$112
TOTAL			**212**		**1,272** **$121,052**	**$1,142**

Title: Mandatory Reliability Standards for BAL-001-2.

Action: Proposed Collection FERC-725R.

OMB Control No.: 1902-0268.

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: On Occasion.

[45] Proposed Reliability Standard BAL-001-2 applies to balancing authorities and regulation reserve sharing groups. However, the burden associated with the BA complying with Requirement R1 is not included within this table because the Commission accounted for it under Commission-approved Reliability Standards BAL-001-1.

[46] The estimated hourly costs (salary plus benefits) are based on Bureau of Labor Statistics (BLS) information (*available at* http://www.bls.gov/oes/current/naics2_22.htm) for an electrical engineer ($60.87/hour) and a lawyer ($128.76).

[47] BA=Balancing Authority; RRSG=Regulation Reserve Sharing Group.

[48] $28/hour, based on a Commission staff study of record retention burden cost.

Necessity of the Information: This proposed rule proposes to approve the Reliability Standard pertaining to requiring balancing authorities to operate such that its clock-minute average reporting ACE does not exceed its clock-minute Balancing Authority ACE Limits for more than 30 consecutive clock-minutes. The proposed Reliability Standard Requirement R2 provides each balancing authority a dynamic ACE limit that is a function of Interconnection frequency. The proposed Reliability Standard will provide dynamic limits that are balancing authority and Interconnection specific. In addition, these ACE limits are based on identified Interconnection frequency limits to ensure the Interconnection returns to a reliable state when an individual balancing authority's ACE or Interconnection frequency deviation contributes undue risk to the Interconnection.

Internal Review: The Commission reviewed the proposed Reliability Standard 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 generation and demand balance throughout the Eastern and Western Interconnections as well as within the ERCOT Region.

29. 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].

30. 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 FERC-725R and Docket Number RM14-10-000.

IV. Environmental Analysis

31. 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] 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.[50] The actions proposed here fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Certification

32. The Regulatory Flexibility Act of 1980 (RFA)[51] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities. As shown in the information collection section, the proposed

[49] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs., Regulations Preambles 1986-1990 ¶ 30,783 (1987).

[50] 18 C.F.R. 380.4(a)(2)(ii).

[51] 5 U.S.C. 601-612.

Reliability Standard applies to 106 entities. Comparison of the applicable entities with the Commission's small business data indicates that approximately 23[52] are small business entities. Of these, the Commission estimates that approximately five percent, or one of these small entities, will be affected by the new requirements of the proposed Reliability Standard.

33. The Commission estimates that the small entities that will be affected by proposed Reliability Standard BAL-001-2 will incur one-time compliance cost up to $109,180 (i.e. the cost of updating and maintaining energy management systems), resulting in cost of approximately $1,030 per balancing authority and/or regulation reserve sharing groups. These costs represent an estimate of the costs a small entity could incur if the entity is identified as an applicable entity. The Commission does not consider the estimated cost per small entity to have a significant economic impact on a substantial number of small entities. Accordingly, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities.

VI. Comment Procedures

34. 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 [INSERT DATE 60 days after publication in the **FEDERAL REGISTER**]. Comments must refer to

[52] 21.4 percent of the total number of affected entities.

Docket No. RM14-10-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

35. 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.

36. 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.

37. 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.

VII. Document Availability

38. 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 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

39. 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.

40. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email 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.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

149 FERC ¶ 61,141
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Chairman;
Philip D. Moeller, Tony Clark,
and Norman C. Bay.

North American Electric Reliability Corporation Docket No. RR14-5-000

ORDER ON THE ELECTRIC RELIABILITY ORGANIZATION'S FIVE-YEAR PERFORMANCE ASSESSMENT

(Issued November 20, 2014)

1. On July 21, 2014, North American Electric Reliability Corporation (NERC) filed its Five-Year Electric Reliability Organization Performance Assessment Report (Performance Assessment) in accordance with the requirements of the Commission's regulations.[1] The Performance Assessment is the second such assessment filed by NERC as the Commission-certified Electric Reliability Organization (ERO). The Performance Assessment discusses whether and how NERC satisfies the criteria for ERO certification under 18 C.F.R. § 39.3(b), evaluates the effectiveness of each Regional Entity in carrying out its delegated functions, and addresses stakeholder comments on NERC's performance as the ERO. NERC highlights activities and accomplishments demonstrating how the ERO is improving the performance of, and mitigating risks to, the Bulk-Power System as related to avoidable outages, and how NERC's compliance monitoring and enforcement efforts have matured to provide industry with greater certainty on actions, outcomes, and reliability consequences.

2. In this order, we accept NERC's Performance Assessment, find that NERC continues to satisfy the statutory and regulatory criteria for certification as the ERO, and find that the Regional Entities continue to satisfy applicable statutory and regulatory criteria. In addition, we find that NERC should take several actions to continue improving its performance as the ERO. Specifically, we direct NERC to submit an informational filing addressing specific matters and direct or encourage NERC to take certain additional actions as discussed in this order. These action items provide practical

[1] 18 C.F.R. § 39.3(c) (2014).

steps to improve the effectiveness of the ERO and Regional Entity functions and programs, and to improve the quality of NERC's Performance Assessment process going forward. These action items address important concerns, such as continued development of performance and reliability metrics for the ERO and Regional Entities; improvement in the development and periodic review of Reliability Standards; and improvement in efforts to ensure appropriate consistency across and coordination among all regions.

I. Background

A. Section 215 of the Federal Power Act

3. Section 215 of the Federal Power Act (FPA) requires the Commission to issue regulations that, among other things, provide for certification of an entity as the ERO if it meets certain criteria.[2] Specifically, FPA section 215(c) establishes that an ERO candidate must have the ability to develop and enforce mandatory Reliability Standards that provide for an adequate level of reliability of the Bulk-Power System.[3] The statute also requires that an ERO candidate have established 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; (4) provide reasonable notice and opportunity for public comment, due process, and balance in developing Reliability Standards and otherwise exercising its duties; and (5) provide appropriate steps to gain recognition in Canada and Mexico.

4. Additionally, FPA section 215(e)(4) provides that the ERO may delegate authority to a Regional Entity for the purpose of proposing regional Reliability Standards and enforcing Reliability Standards. Regional Entities must meet the same statutory criteria as those required for Commission certification of an ERO, except that more flexibility is allowed in the composition of a Regional Entity board of directors. The Commission must approve a delegation agreement between the ERO and a Regional Entity, and the Commission is authorized to modify such delegation.

[2] 16 U.S.C. § 824o (2012).

[3] *Id.* § 824o(c).

B. Order No. 672

5. On February 3, 2006, the Commission issued Order No. 672, which, among other things, amended the Commission's regulations to implement the requirements of FPA section 215.[4] Order No. 672 sets forth the process for certifying a single independent ERO to oversee the reliability of the United States' portion of the interconnected North American Bulk-Power System, subject to Commission oversight. Further, in Order No. 672, the Commission mandated that the ERO submit periodic assessments of its performance that require the ERO to "affirmatively demonstrate to the Commission that it satisfies the statutory and regulatory criteria for an ERO and is not only maintaining but improving the quality of its activities and those of the Regional Entities to which it has delegated such activities."[5]

6. In Order No. 672, the Commission also stated that the performance assessments should employ regular and systematic measurement and reporting of the ERO's performance, including information regarding: (1) the ERO's ability to develop and enforce Reliability Standards providing for an adequate level of reliability of the Bulk-Power System; (2) how the ERO effectively enforced Reliability Standards, including statistical information on its investigations, findings, and assessments of penalties, on a regional and continent-wide basis; and (3) how the ERO provided for fair and impartial procedures for enforcement of Reliability Standards and provided for openness, due process, and balance of interests in developing Reliability Standards.[6]

7. The specific requirements for the performance assessments are set out in the Commission's regulations at 18 C.F.R. § 39.3(c), and provide that the ERO file an assessment of its performance three years from the date of initial certification, and every five years thereafter. Each performance assessment filing is required to include the following: (1) an explanation of how the ERO satisfies the requirements of § 39.3(b); (2) recommendations by Regional Entities, users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the ERO operations, activities, oversight and procedures, and the ERO's response to such recommendations; and (3) the ERO's evaluation of the effectiveness of each Regional Entity, recommendations by the

---

[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] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 186.

[6] *Id.* P 189.

Electric Reliability Organization, users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the Regional Entity's performance of delegated functions, and the Regional Entity's response to such evaluation and recommendations.[7]

8. The specific requirements in section 39.3(c)(2) of the Commission's regulations explain that the Commission will review the periodic performance assessments and may require follow-up actions by the ERO to comply or improve compliance with the statutory and regulatory qualifications for the ERO, if the Commission determines that the ERO has not satisfied specific criteria. Moreover, that subsection requires the Commission to assess the performance of each Regional Entity and issue an order addressing Regional Entity compliance.[8]

C. Certification of NERC as the ERO

9. On July 20, 2006, the Commission certified NERC as the ERO for the continental United States under FPA section 215(c).[9] The Commission found that NERC satisfied the criteria to be the ERO responsible for developing and enforcing mandatory Reliability Standards for the United States.

10. In April 2007, in accordance with FPA section 215(e)(4) and the Commission's regulations at 18 C.F.R. § 39.8, NERC entered into a separate delegation agreement with each of the eight Regional Entities[10] by which NERC delegated certain authority to the

[7] 18 C.F.R. § 39.3(c) (2014).

[8] *Id.* § 39.3(c)(2); *see also* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 33, 187.

[9] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062 (ERO Certification Order), *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *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).

[10] The eight Regional Entities currently are: Florida Reliability Coordinating Council, Inc. (FRCC); Midwest Reliability Organization (MRO); Northeast Power Coordinating Council, Inc. (NPCC); Reliability*First* Corporation (RFC); SERC Reliability Corporation (SERC); Southwest Power Pool, Inc. (SPP); Texas Reliability Entity (TRE); and Western Electricity Coordinating Council (WECC).

Regional Entities.[11] Specifically, NERC delegated authority to the Regional Entities to audit, investigate, and otherwise ensure that users, owners, and operators of the Bulk-Power System comply with NERC's mandatory Reliability Standards, subject to ERO oversight.[12] In addition, the delegation agreements address such matters as: (1) regional Reliability Standards development; (2) registration of entities that must comply with Reliability Standards; and (3) other services supporting NERC's statutory reliability functions, including reliability assessments, event analysis, and training and education.

D. NERC Initial Performance Assessment

11. On July 20, 2009, NERC filed its Initial Performance Assessment in accordance with the Commission's regulations.[13] On September 16, 2010, the Commission accepted NERC's Initial Performance Assessment and found that NERC continued to satisfy the statutory and regulatory criteria for ERO certification, and that each of the Regional Entities met the relevant statutory and regulatory criteria.[14] The Commission also directed NERC to submit an informational filing to address specific concerns discussed in the 2010 Performance Assessment Order.[15]

12. The Commission also explained, among other things, that according to Order No. 672, the purpose of the ERO's performance assessments is not only to determine whether the ERO is satisfying the statutory criteria for certification, but also to identify areas in which the ERO can improve performance. The Commission also noted that it sees the performance assessments as an opportunity not only to demonstrate that the ERO has maintained, but also is improving, the quality of its activities and those of the Regional Entities.[16] In that vein, NERC identified in its Initial Performance Assessment filing

---

[11] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,060 (2007), *order on reh'g,* 120 FERC ¶ 61,260 (2007).

[12] *See* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 654.

[13] North American Electric Reliability Corp., Filing, Docket No. RR09-7-000 (filed July 20, 2009) (Initial Performance Assessment).

[14] *North American Electric Reliability Corp.*, 132 FERC ¶ 61,217, at P 35 (2010) (2010 Performance Assessment Order).

[15] *Id.* P 1 and Appendix A.

[16] 2010 Performance Assessment Order, 132 FERC ¶ 61,217 at P 5 (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 186-188).

specific "action items" to address "opportunities for improvement" in the various NERC programs. The Commission stated that "generally, the action items are reasonable and provide practical steps to improve the effectiveness of the ERO and Regional Entity functions and programs," addressing important concerns such as accelerating and prioritizing the Reliability Standards development process, enhancing stakeholder communications, improving registration consistency across regions, eliminating the backlog of audit reports and compliance violations, promoting self-reporting of non-compliance, and providing compliance guidance to registered entities.[17]

II. NERC Five-Year Performance Assessment

13. On July 21, 2014, NERC submitted its Performance Assessment as required by the Commission's regulations. NERC states that the Performance Assessment describes NERC's efforts to maintain and improve the quality of its activities as the ERO since its Initial Performance Assessment. Specifically, NERC explains how it continues to meet the criteria for ERO certification under 18 C.F.R. § 39.3(b), evaluates the effectiveness of each Regional Entity in carrying out its delegated functions, and addresses stakeholder comments on NERC's performance as the ERO.

14. NERC explains that, unlike its Initial Performance Assessment, NERC is not presenting a program area-by-program area discussion of its activities; rather, NERC highlights activities and accomplishments in support of its strategic plan initiatives for the Performance Assessment period, which include reforming the Reliability Standards program, developing the Reliability Assurance Initiative, and revising the "bulk electric system" definition. NERC also states that the Performance Assessment demonstrates how the ERO is improving the performance of, and mitigating the risks to, the Bulk-Power System as related to avoidable outages, and how NERC's compliance monitoring and enforcement efforts have matured to provide industry with greater certainty on actions, outcomes, and reliability consequences.

15. NERC's Performance Assessment includes attachments that provide additional information on the following matters: how NERC meets the ERO certification criteria (Attachment 1); joint Regional Entity self-assessments (Attachment 2); NERC's assessment of Regional Entity delegated functions (Attachment 3); NERC's

[17] *Id.* P 4.

consideration of industry feedback (Attachment 4); status of areas for improvement identified in the 2010 Performance Assessment Order (Attachment 5); and NERC's plans and initiatives for improving coordinated operations across the ERO Enterprise (Attachment 6).[18]

III. Notice and Responsive Pleadings

16. Notice of NERC's filing was published in the *Federal Register*, with comments due on or before August 20, 2014.[19] On August 18, 2014, Eric S. Morris filed a motion to intervene and request for extension of time, identifying a number of issues raised by NERC's filing and requesting additional time to more fully respond to those issues. On August 19, 2014, the Commission granted Mr. Morris's request, extending the comment deadline for all interested parties to August 29, 2014.

17. Timely motions to intervene were filed by the National Rural Electric Cooperative Association, American Public Power Association, Eric S. Morris, and, jointly, the eight Regional Entities.

18. Mr. Morris, who identifies himself as a ratepayer, was the only party to submit comments on NERC's Performance Assessment, both in his motion to intervene filed on August 18, 2014, and in subsequent comments filed on August 26, 2014. On August 27, 2014, NERC filed Reply Comments to Mr. Morris's August 18, 2014 Comments.

IV. Procedural Matters

19. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, the timely, unopposed motions to intervene serve to make the entities that filed the motions parties to this proceeding.[20] Rule 213(a)(2) of the Commission's Rules of Practice and Procedure prohibits an answer to an answer or protest unless otherwise ordered by the decisional authority.[21] We will accept NERC's Reply Comments because they have provided information that assisted us in our decision-making process.

---

[18] NERC states that the term "ERO Enterprise" encompasses both NERC and the eight Regional Entities.

[19] 79 Fed. Reg. 44,761 (Aug. 1, 2014).

[20] 18 C.F.R. § 385.214 (2014).

[21] *Id.* § 385.214(a)(2).

V. Discussion

A. NERC's Satisfaction of the Criteria for Certification as the ERO and Evaluation of the Regional Entities

20. Under section 215(c) of the FPA and section 39.3(b)(1) of the Commission's regulations, the ERO must demonstrate that it has the ability to develop and enforce Reliability Standards that provide for an adequate level of Bulk-Power System reliability.[22] In addition, the ERO must show that it has established 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; (4) provide reasonable notice and opportunity for public comment, due process, and balance in developing Reliability Standards and otherwise exercising its duties; and (5) provide appropriate steps to gain recognition in Canada and Mexico.[23]

21. In addition, the ERO is required under section 39.3(c)(1)(ii) of the Commission's regulations to provide a response to recommendations by the Regional Entities and users, owners, and operators of the Bulk-Power System for improvement in the ERO's operations. In addition, under section 39.3(c)(1)(iii), the ERO is required to evaluate each Regional Entity's effectiveness, including how the Regional Entity responded to recommendations for improvement as suggested by the ERO and by users, owners, and operators of the Bulk-Power System.

NERC Performance Assessment

22. NERC provides a detailed narrative describing how it satisfies the statutory and regulatory requirements for certification on an ongoing basis.[24] NERC explains that, as the ERO, it has undertaken initiatives during the Performance Assessment period to "enhance the reliability of the [Bulk-Power System] and to increase the effectiveness and efficiency of the operations of the ERO Enterprise."[25] NERC states that these initiatives have included, among other things: (1) development of clear, reasonable, and technically sound Reliability Standards; (2) registration of entities with functional responsibilities for

[22] *Id.* § 39.3(b)(1).

[23] *Id.* § 39.3(b)(2).

[24] *See* Performance Assessment at 82-89.

[25] *Id.* at 7.

Bulk-Power System reliability; (3) monitoring and enforcing compliance with Reliability Standards; (4) identification and prioritization of, and communicating information on, risks to Bulk-Power System reliability; and (5) collecting and sharing information on threats to the cyber and physical security of the Bulk-Power System. According to NERC, it started several initiatives during the Performance Assessment period to further improve the Reliability Standards, including: (1) the results-based Reliability Standards initiative; (2) the removal of duplicative or otherwise unnecessary provisions from Reliability Standards, referred to as the "Paragraph 81" project; (3) internal reorganization of NERC's Reliability Standards department; and (4) establishment of the Independent Experts Review Panel. In addition, NERC states that during this Performance Assessment period, it addressed 128 directives by year-end 2013, reducing the number of open directives involving Reliability Standards to 107. NERC also states that it anticipates that 90 percent of Commission directives issued to date will be resolved during the first half of 2015.[26]

23. NERC provides a detailed evaluation of the Regional Entities' effectiveness at performing their delegated functions and of NERC's response to recommendations for improvement, as required by the Commission's regulations.[27] In addition, NERC provides a joint evaluation conducted by the Regional Entities, which includes self-evaluations and suggestions for improvements.[28] NERC also includes suggestions for improvement from users, owners, and operators of the Bulk-Power System, and other interested parties, as well as NERC's and the Regional Entities' responses to these suggestions.[29]

1. Development and Enforcement of Reliability Standards under Section 39.3(b)(1)

24. Section 39.3(b)(1) of the Commission's regulations requires that the ERO have the ability to develop and enforce Reliability Standards that provide for an adequate level of Bulk-Power System reliability. In the Performance Assessment, NERC states that it "continues to have the ability to develop and enforce, subject to 18 C.F.R. § 39.7, Reliability Standards that provide for an adequate level of reliability of the [Bulk-Power

[26] *Id.* at 7-12.

[27] *See* Performance Assessment, Att. 3.

[28] *See* Performance Assessment, Att. 2.

[29] *See* Performance Assessment, Att. 4.

System].”[30] NERC notes that as of December 1, 2013, NERC developed and submitted to the Commission a total of 293 continent-wide Reliability Standards that have been approved by the Commission, a number which have been retired or superseded by revised Reliability Standards. In addition, NERC approved and submitted to the Commission a total of 23 regional Reliability Standards that have been approved by the Commission.[31] These Reliability Standards encompass a broad range of subjects relating to Bulk-Power System reliability. NERC states that it made improvements to the Commission-approved, American National Standards Institute-accredited Standard Processes Manual during the Performance Assessment period and that the “Reliability Standards development process contains the essential attributes of the standards development process as set forth in prior Commission orders.”[32] NERC indicates that it systematically manages the development and revision of Reliability Standards in the areas of highest need and importance through the rolling three-year Reliability Standards Development Plan.

25. NERC states that monitoring and enforcing compliance with the mandatory Reliability Standards is conducted through the Compliance Monitoring and Enforcement Program (CMEP). NERC explains that section 6(a) of the Regional Delegation Agreements between NERC and each of the eight Regional Entities requires each Regional Entity to enforce mandatory Reliability Standards within its specific geographic boundaries. NERC states that, to further that effort, NERC and the Regional Entities have increased the number of budgeted compliance program staff approximately 191.72 percent from 2009 to 2014, and increased the budgeted compliance program direct expenses by 175.84 percent over the same period.[33] In addition, NERC explains that it conducts an audit at least once every five years to evaluate each Regional Entity’s implementation of the NERC CMEP, in addition to spot checks, as required by section 402.1.1.3 of the NERC Rules of Procedure.[34]

[30] Performance Assessment at 83.

[31] Performance Assessment, Att. 1 at 7.

[32] Performance Assessment at 83.

[33] Performance Assessment, Att. 1 at 16.

[34] *See id.* at 9-17.

2. Certification Criteria under Section 39.3(b)(2)

a. Independence and Fair Stakeholder Representation

26. NERC states that it "continues to have in place rules that assure its independence from users, owners, and operators of the [Bulk-Power System] while assuring fair stakeholder representation in the selection of its directors and balanced decision making in any ERO committee or subordinate organizational structure."[35] Specifically, NERC states that its Bylaws provide that NERC's business and affairs are managed by a Board of Trustees consisting of ten independent trustees plus the President of NERC. NERC explains that, pursuant to the Bylaws, a NERC trustee cannot be an officer, director, or employee of any entity "that would be perceived as having a direct financial interest in the outcome of board decisions, and may not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a trustee."[36] Candidates for a trustee role are selected by a nominating committee, which is established annually, composed of the independent trustees whose terms will not expire during the current year, and at least three members of the NERC Member Representatives Committee. In addition, the NERC *Conflict of Interest and Business Ethics Policy for Trustees, Officers and Employees* provides that NERC representatives shall refrain from participation in situations where there is an actual conflict of interest or where there is the appearance of a conflict of interest.[37]

b. Equitable Allocation of Reasonable Dues, Fees, and Other Charges

27. NERC explains that, under its Bylaws and Rules of Procedure, the annual funding requirements for the statutory activities of NERC and the Regional Entities are allocated based on net energy for load.[38] In instances where a direct assignment of costs to a specific interconnection, Regional Entity, or group of entities is appropriate, NERC states

[35] Performance Assessment at 85.

[36] Performance Assessment, Att. 1 at 18.

[37] *See generally* Performance Assessment, Att. 1 at 17-23.

[38] NERC defines net energy for load as "[n]et 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." Performance Assessment, Att. 1 at 24 (citing NERC Rules of Procedure, App. 2).

that such costs are assigned to the appropriate entities based on net energy for load. NERC explains further that the allocation of the annual assessments based on net energy for load is submitted to the Commission for approval in NERC's annual business plan and budget filing.[39]

c. Rules that Provide Fair and Impartial Procedures for Enforcing Reliability Standards Through Imposition of Penalties

28. NERC states that it has established rules that provide fair and impartial procedures for monitoring and enforcing compliance with Reliability Standards, set forth in section 400 of the NERC Rules of Procedure, NERC's CMEP, and the individual CMEP of each Regional Entity. NERC explains that the CMEP includes provisions allowing registered entities to participate in settlement discussions with NERC or the Regional Entity related to notices of alleged violations, proposed penalties or sanctions, and mitigation plans. [40]

29. NERC states that the CMEP includes rules regarding the determination and imposition of financial penalties on registered entities that have violated Reliability Standards. NERC explains that penalties are to be commensurate to the reliability impact of the violation and to those levied for similar violations, but still reflect any unique facts and circumstances related to the registered entity or specific violation. NERC states that it "evaluates the facts and circumstances of every violation that is part of a settlement to ensure that the penalty for that violation, and for the group of violations in the settlement, is within a range of reasonableness that displays consistency."[41]

30. With regard to the penalty determination, NERC explains that the Commission-approved Sanction Guidelines establish a base penalty amount established by the associated Violation Risk Factor (VRF) and Violation Severity Level (VSL) tables. The base penalty amount can be adjusted up or down based on factors such as a registered entity's compliance history, the violation time horizon, entity size, the operating condition of the Bulk-Power System at the time of the violation, and any mitigating factors. NERC explains that a penalty may be mitigated based on factors such as the quality of the registered entity's internal compliance program, amount of cooperation in resolving the violation, and whether the registered entity self-reported the violation.

---

[39] *See* Performance Assessment at 86; and Att. 1 at 23-24.

[40] Performance Assessment, Att. 1 at 24-25.

[41] *Id.* at 27.

31. NERC also describes the hearing procedures included in the uniform CMEP that apply when a registered entity requests a hearing concerning a disputed notice of alleged violation, disputed proposed penalty or sanction, disputed mitigation plan provisions, or disputed remedial action directive. NERC also explains that it adopted guidelines in 2013 to provide practical guidance to the Regional Entity hearing body members regarding the hearing process. NERC states that the guidelines outline the duties of the hearing officer and hearing body, and discuss the appropriate standard of review to be used throughout the hearing process.[42]

d. Rules that Provide Notice and Opportunity for Public Comment, Due Process, and Balance in Developing Reliability Standards and Otherwise Exercising Duties

32. NERC states that it has established rules, reflected in its Bylaws, Rules of Procedure, and Standard Processes Manual, that provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards and exercising its other duties, such as compliance monitoring and enforcement. NERC explains that participation in the development of Reliability Standards is open to all persons who are directly and materially affected by the reliability of the North American Bulk-Power System. NERC states that the ballot body established for voting on a proposed Reliability Standard is organized in ten segments to reflect a balance of interests.[43]

33. NERC provides a detailed description of the Reliability Standards development process, which is overseen by a Standards Committee. NERC explains that the Standards Committee, which represents the interests of the industry as a whole, was established to ensure stakeholder interests are fairly represented in the Reliability Standards development process. NERC further explains that the Standard Processes Manual details the steps for developing a new or modified Reliability Standard. NERC states that once a draft Reliability Standard has been developed, NERC posts the proposed new or revised Reliability Standard for public comment, and the Reliability Standard drafting team must address any comments received. After the comment period is complete, the ballot pool for that Reliability Standard votes on the final proposed new or revised Reliability Standard. Approval of a proposed new or revised Reliability Standard requires both a

[42] *Id.* at 25.

[43] *Id.* at 28-30.

quorum, consisting of 75 percent of the ballot pool membership submitting a vote, and an affirmative vote by a two-thirds majority of the weighted-segment votes.[44]

34. NERC states that other rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in other areas of NERC's duties. NERC explains that these rules apply to, among other things, the election of trustees, revisions to the NERC Rules of Procedure, meetings of the Board of Trustees and associated committees, development of NERC's annual business plan and budget, and compliance monitoring and enforcement process.[45]

e. Appropriate Steps to Gain Recognition in Canada and Mexico

35. NERC states that it continues to engage in significant efforts to gain and maintain recognition as the ERO in Canada and Mexico. With respect to Canada, NERC explains that, depending on the particular circumstances of each Canadian province, it gained recognition as the ERO through statutes or other provisions of provincial law, or through a memorandum of understanding with the appropriate provincial entities. In addition, NERC explains that it also signed a memorandum of understanding with the Canadian National Energy Board, which has jurisdiction over international transmission lines within Canada. As for Mexico, NERC states that the Comisión Federal de Electricidad, which is responsible for reliable operation of the electric system in Mexico, and the Area de Control Baja California have entered into a membership and operating agreement with WECC with respect to the portion of the grid in Baja California Norte that is part of the Western Interconnection. NERC explains that WECC monitors compliance with the ten approved Mexico Reliability Standards, but does not have enforcement or registration authority within Mexico. NERC explains further that as to Mexico, WECC "provides compliance monitoring, reviews proposed and completed mitigation plans, and provides assessment recommendations with respect to alleged violations."[46]

Commission Determination

36. We find that NERC's Performance Assessment demonstrates that NERC continues to satisfy the statutory and regulatory requirements set forth in section 215(c) of the FPA and section 39.3(b) of our regulations. As discussed above, NERC provides a

[44] *Id.* at 30-32.

[45] *Id.* at 33-34.

[46] Performance Assessment at 88-89.

detailed description of how it meets the statutory and regulatory requirements established for the Commission-approved ERO. We conclude that NERC demonstrated that it has the ability to develop and enforce Reliability Standards. In addition, the Performance Assessment reflects improvements made to NERC's processes and procedures since our issuance of the 2010 Performance Assessment Order, such as revisions to the Standard Processes Manual to streamline the Reliability Standards development process and the adoption of standardized hearing procedures.

37. We also find that each of the Regional Entities continues to meet the relevant statutory and regulatory criteria. As directed in the 2010 Performance Assessment Order, NERC addressed each Regional Entity's performance in light of the relevant statutory and regulatory criteria.[47] We particularly note the increase in budgeted compliance program staff across NERC and the eight Regional Entities, demonstrating the increased commitment to monitoring and enforcement as the entities mature to a "steady state."[48]

38. While we acknowledge the improvements that NERC and the Regional Entities have made with regard to their compliance and enforcement responsibilities over the Performance Assessment period, we believe that there are still opportunities for additional improvement. With regard to compliance enforcement processing, NERC and the Regional Entities have made significant efforts to prioritize and reduce their outstanding pre-2012 caseload. According to NERC's Performance Assessment, as of December, 2013, only 65 violations older than 24 months remain to be processed.[49] However, the average violation age has only marginally improved, from 11.86 months in 2012 to 11.2 months in 2013.[50] In light of increased enforcement staffing and improved enforcement processes at NERC and the Regional Entities, we expect that violation processing times and the average violation age will continue to decline. In addition, to ensure that the ERO Enterprise and the Commission are both able to effectively perform their duties under section 215 of the FPA, we expect NERC to continue to cooperate with and share all appropriate data and information with Commission staff.

---

[47] *See North American Electric Reliability Corp.*, 132 FERC ¶ 61,217, at P 36 (2010).

[48] NERC and the Regional Entities' approved business plans and budgets for 2009 provided for approximately 158 full-time staff in compliance, monitoring, and enforcement programs. For 2014, the number of full-time staff devoted to compliance, monitoring, and enforcement programs increased to 303.

[49] Performance Assessment at 49, Att. 3 at 63.

[50] *Id.*

39. Additionally, it is unclear from NERC's Performance Assessment whether the compliance and enforcement program is effectively reducing repeat violations in a meaningful way. Monitoring recidivism among registered entities can provide a key indicator of whether NERC's CMEP is effective in deterring and mitigating violations. Therefore, we direct NERC to include an analysis of repeat violations in its next Performance Assessment that will allow NERC, the Regional Entities, and the Commission to evaluate whether NERC's compliance and enforcement efforts have been effective in improving registered entities' compliance and overall reliability.

40. With regard to the equitable allocation of reasonable dues, fees and other charges, we continue to agree with NERC that its allocation based on net energy for load is a reasonable and equitable allocation method.[51] The Commission found application of the net energy for load allocation methodology in Order No. 672 to be fair and reasonable,[52] and approved NERC's specific net energy for load proposal in the ERO Certification Order.[53] Thus, we believe that NERC's continued use of the net energy for load methodology is well justified, and we note its equitable benefits (including the elimination of double counting), and its relatively simple application compared to other apportionment methods. Further, we believe that NERC's budget development process and the Commission's approval of the ERO and Regional Entity annual business plans and budgets support the reasonableness of the charges.

41. Likewise, the Commission generally is satisfied with other features of NERC's Rules of Procedure, including rules that provide fair and impartial procedures for enforcing Reliability Standards and rules that provide for broad participation, notice, and opportunities for comment in developing Reliability Standards. Pursuant to FPA section 215(f), the Commission approved the initial submission of the NERC Rules of Procedure, as well as each subsequent revision. Thus, along with the individual findings that the NERC Rules of Procedure are just, reasonable, not unduly discriminatory or preferential, and in the public interest, we conclude here that the NERC Rules of Procedure are fair

[51] *See, e.g.*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 213; ERO Certification Order, 116 FERC ¶ 61,062, at P 167; *North American Electric Reliability Corp.*, 128 FERC ¶ 61,025, at P 38 (2009); *North American Electric Reliability Corp.*, 132 FERC ¶ 61,217, at P 56 (2010).

[52] *See* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 35, 213.

[53] ERO Certification Order, 116 FERC ¶ 61,062 at P 167. The net energy for load allocation method was upheld on appellate review. *See Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

and impartial and generally support the varied functions and programs of the ERO. Further, we recognize NERC's efforts to gain and maintain recognition as the ERO in Canada and Mexico, and urge NERC to continue its efforts to support the reliability of the North American Bulk-Power System through work with our international partners.

42. We also find that NERC and the Regional Entities responded to suggestions for improvement from users, owners, and operators of the Bulk-Power System and other interested parties as required by section 39.3(c) of our regulations. However, we believe that having access to the original comments from stakeholders in addition to the comment summaries provided by NERC will aid the Commission in its evaluation of the ERO and Regional Entities.[54] Therefore, we will direct NERC to include the original comments from interested stakeholders in its future performance assessment filings, beginning in 2019.

B. Assessment of NERC's Performance and Areas for Improvement

1. Commenter Concerns

Comments

43. Mr. Morris, the sole commenter, identified three areas of concern in his August 18, 2014 comments. First, Mr. Morris raises questions about NERC's protection of confidential information, and asks questions concerning one specific instance in which an Unidentified Registered Entity's identity was revealed in a separate penalty proceeding.[55] Second, Mr. Morris questions the consistency of penalties as imposed across the regions, and as compared to NERC's VRF and VSL tables and other penalty guidelines.[56] To address these concerns, he asks that NERC provide (1) an analysis of the penalties imposed on a per dollar per day basis as compared to the VRF and VSL tables; (2) an analysis to show that NERC is treating multiple violations appropriately and consistently

[54] *See* Performance Assessment, Att. 4 (which, in table format, includes a "Summary of Key Stakeholder Comments").

[55] Mr. Morris cites Docket No. NP12-27-000, which he believes inadvertently revealed the identity of the Unidentified Registered Entity sanctioned for violations of the Critical Infrastructure Protection (CIP) Reliability Standards in Docket No. NP12-16-000.

[56] Morris August 18, 2014 Comments at 2 ("I am really seeking data that [NERC's] penalty guidelines are being followed, and whether they are being applied consistently across the regions.").

across regions; and (3) tables providing information on a regional basis similar to that provided in NERC's "Violations for all Regional Entities 2009-2013 by Year Reported to NERC U.S. Violations Only" and "Data on Regional Entity Compliance Resources" reports. Third, Mr. Morris questions whether the entire regional model is appropriate, given "its inherent administrative cost," and asks that NERC provide a cost-benefit analysis of the Regional Entity model as compared to a single unified ERO.[57]

44. In his August 26, 2014 Comments, Mr. Morris requests that NERC use net energy for load in developing its comparison of penalty amounts among the regions. In addition, he reiterates his request for a cost-benefit analysis of the regional model versus a single ERO model, pointing to NERC's statements about the difficulty of developing and analyzing Regional Entity compliance program data as evidence that "managing these entities in an oversight capacity is probably more trouble than it is worth."[58] In addition, he supports the need for such a cost-benefit analysis based on NERC's own statements regarding the need for consistency in the ERO Enterprise's compliance, enforcement, and event analysis program. Finally, he suggests that "a significant portion" of the current levels of compensation for senior leadership of the Regional Entities would not be necessary under a unified ERO.[59]

45. On August 27, 2014, NERC filed Reply Comments to Mr. Morris's August 18, 2014 Comments. NERC responds to Mr. Morris's request for a cost-benefit analysis of the Regional Entity model by noting that FPA section 215 and Commission regulations implementing that section contemplate the delegation of certain authority from the ERO to a Regional Entity.[60] In addition, NERC states that its Performance Assessment meets the requirements of FPA section 215(e)(4) and its implementing regulations, none of which require submission of a cost-benefit analysis. NERC responds to Mr. Morris's questions about NERC's protection of confidential information by stating that it improved its internal procedures on redaction guidelines since the 2012 incident referenced by Mr. Morris, and notes that its procedures for protecting confidentiality are

[57] Morris August 18, 2014 Comments at 2.

[58] Morris August 26, 2014 Comments at 1.

[59] *Id.*

[60] NERC states that Mr. Morris's August 26 Comments reiterated his concern with the regional model and that Mr. Morris cited a single Internal Revenue Service Form 990 for Reliability*First* Corporation to suggest that the regional model is unnecessarily wasteful. *See* NERC Comments at fn.5.

reviewed at least once per year.[61] Finally, NERC maintains that the comparison of actual penalties imposed by the Regional Entities, versus NERC's VRF and VSL tables, would not be meaningful in assessing the fairness of NERC's and the Regional Entities' enforcement methods. NERC asserts that the tables provide base penalty amounts only, while NERC's Sanction Guidelines contemplate that NERC and the Regional Entities consider a number of other factors in setting penalty amounts. In addition, NERC states that it encourages the Regional Entities to consider the imposition of non-monetary sanctions or acceptance of certain activities "above and beyond those required to ensure compliance . . . in lieu of full monetary penalties permitted by the NERC *Sanction Guidelines* (where it is appropriate)."[62]

46. On August 28, 2014, Mr. Morris submitted additional comments responding to NERC's Reply Comments. First, Mr. Morris requests that NERC withdraw its comment that he stated that "the benefits of managing the Regional Entities are grossly outweighed by the costs," and "the [R]egional [E]ntity model is inherently wasteful." Rather, Mr. Morris states that he made no arguments regarding the outcome of a cost-benefit analysis, and merely believes that it should be done.[63] Second, responding to NERC's statement that Mr. Morris provided limited data to support the need for a cost-benefit analysis, Mr. Morris provides additional information on key leader compensation of the Midwest Reliability Organization.[64]

Commission Determination

47. With respect to concerns and questions raised regarding NERC's protection of information deemed to be confidential, particularly as related to cybersecurity incidents or CIP violations, we believe that NERC currently has adequate rules and procedures in place to protect against improper disclosure of sensitive information, and note that NERC

[61] NERC acknowledges it has an obligation to ensure that the disposition of each violation or alleged violation that relates to a cybersecurity incident will remain nonpublic. NERC also states that the Rules of Procedure provide that NERC will not disclose any confidential information, including cybersecurity incidents, and will redact such information in any public filings unless disclosure is otherwise permitted by the Rules of Procedure.

[62] NERC Comments at 1 (footnotes omitted).

[63] Morris August 28, 2014 (citing NERC Comments at 2).

[64] *Id.*

improved its redaction procedures since the dockets referenced by Mr. Morris were filed with the Commission.[65]

48. Regarding Mr. Morris's requests for a comparison of penalty amounts imposed across regions as compared to NERC's VRF and VSL tables, we agree with NERC that such a comparison would have limited utility, as it fails to reflect the many other penalty factors that NERC and the Regional Entities must consider under NERC's Sanction Guidelines. These factors include, among other things, the violator's compliance history, degree of cooperation during the enforcement process, quality of the entity's overall compliance program, and whether the violation was self-reported. We have repeatedly endorsed this approach to the imposition of penalties,[66] and find that, as long as NERC continues to oversee the Regional Entities' application of the Sanction Guidelines to promote consistency as and when appropriate, NERC is satisfying its obligations with respect to enforcement.[67]

49. With respect to concerns about the value of the Regional Entity model, we decline to grant Mr. Morris's request for NERC to perform a cost-benefit analysis. As an initial matter, we do not find that such an analysis is required under FPA section 215 or our implementing regulations as part of NERC's performance assessment obligations. Also, FPA section 215 explicitly contemplates the delegation of certain enforcement and other authorities by the ERO to Regional Entities.[68] Mr. Morris provides no evidence to support his request other than implying that the costs of a unified ERO could be lower than the current Regional Entity model due to fewer salaries, and a suggestion that the Regional Entity model is more costly due to "its inherent administrative cost."

---

[65] NERC notes that the dockets referenced in Mr. Morris's August 18, 2014 comments were filed in 2012, and that NERC "improved its internal procedures when it documented its redaction guidelines in early 2013 and incorporated them by reference into its internal Compliance Enforcement Manual." NERC Reply Comments at 5.

[66] *See, e.g., North American Electric Reliability Corp*., 132 FERC ¶ 61,182 (2010) (providing guidance on the application of one of the aggravating factors identified in NERC's Sanction Guidelines); *see also North American Electric Reliability Corp.*, 141 FERC ¶ 61,241, at P 71 (2012) (accepting revised Sanction Guidelines, and their nine adjustment factors for use in determining penalties).

[67] We continue to encourage NERC to develop performance metrics that will be meaningful in evaluating the consistency of the various Regional Entities' approaches to enforcement and imposition of penalties, as further discussed below.

[68] *See* 16 U.S.C. § 824o(e)(4).

Accordingly, we conclude that the comments are not persuasive and do not provide adequate support to direct NERC to take further action on the matter.

2. ERO Enterprise Performance Metrics

NERC Performance Assessment

50. NERC states that it made substantial progress in structuring the ERO Enterprise and improving the reliability of the Bulk-Power System during this Performance Assessment period. NERC explains that, "despite the achievements to date, the … ERO Enterprise … is not without certain challenges and risks. Going forward, NERC needs and intends to focus attention on actions necessary to reach an end-state of a fully-integrated ERO Enterprise that can exercise effective and well-coordinated reliability oversight that mitigates reliability risks to the BPS."[69] NERC states that in order to achieve this end-state, it must increase clarity about the allocation of roles and responsibilities between NERC and the Regional Entities, improve coordination of goals, and establish more uniform work processes, tools, and performance.[70]

51. NERC states that "coordinated strategic planning" is one of five areas that NERC needs to focus on to achieve excellence in the oversight and execution of its statutory functions. NERC explains that its Board of Trustees recently approved ERO Enterprise Performance Metrics that will be used to assess the overall effectiveness of the ERO Enterprise in achieving the goals and objectives outlined in the ERO Enterprise Strategic Plan for 2014-2017, which include addressing risk to the Bulk-Power System, achieving reliability results, assuring Reliability Standards and compliance effectiveness, and improving risk mitigation and program execution.[71] NERC explains that the ERO Enterprise Performance Metrics include four overarching metrics that focus on the overall effectiveness in addressing Bulk-Power System risks and improving reliability, and a number of supporting measures that focus on the effectiveness of key operational elements of the ERO Enterprise.[72] NERC states that its intent is to report the results of

[69] Performance Assessment at 96.

[70] *Id.*

[71] Performance Assessment at 98 (citing ERO Enterprise Performance Metrics, approved by the NERC Board May 2014, *available at* http://www.nerc.com/gov/bot/FINANCE/Hidden%20Documents/ERO%20Enterprise%20Performance%20Metrics%20-%20Board%20Approved%2005%2007%202014.pdf).

[72] *Id. See also* Performance Assessment, Attachment 4 at 24-25, 33.

these metrics on an ERO Enterprise-wide basis, and distinguish results for NERC and individual Regional Entities.[73]

Commission Determination

52. The Commission supports NERC's goal of improving coordinated operations across the ERO and Regional Entities by, among other things, developing a set of common performance measures focused on Bulk-Power System reliability outcomes and effectiveness of statutory programs. The Commission explained in Order No. 672 that the ERO should "affirmatively demonstrate to the Commission that it satisfies the statutory and regulatory criteria for an ERO and is not only maintaining but improving the quality of its activities and those of the Regional Entities to which it has delegated such activities" and continued that it "expects the performance assessment to include regular and systemic measurements and reporting of the ERO's performance."[74] NERC's Performance Assessment has demonstrated that it is improving the quality of its activities. However, we believe that NERC's future Performance Assessments could be improved by including regular and systematic measurements of its performance, including setting performance targets. Accordingly, as discussed further below, we will direct NERC to include its performance measures in future assessment filings.

53. The Board of Trustees' recent adoption of ERO Enterprise Performance Metrics, which will be used to compare performance with future targets and objectives as set forth in the ERO Strategic Plan, and NERC's intent to regularly report the results, should help NERC improve coordinated operations across the ERO and Regional Entities. Additionally, we believe that a common set of performance metrics that will serve as indicators of the overall effectiveness of the ERO in achieving its mission and goals will help both NERC and the Commission assess ERO performance and identify any areas for improvement. Therefore, we encourage NERC to continue tracking, measuring, and reporting its performance using the ERO Enterprise Performance Metrics as adopted by the Board of Trustees. Further, we will direct NERC to incorporate the ERO Enterprise Performance Metrics, and any associated performance measures into its future

[73] Performance Assessment at 98, 102.

[74] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 187.

performance assessment filings, beginning in 2019. More immediately, we expect NERC will continue to post these ERO Enterprise Performance Metrics as the metrics are further developed, and associated metrics, measures, and targets on at least an annual basis.[75]

3. Reliability Metrics

54. In addition to the ERO Enterprise Performance Metrics discussed above, NERC uses certain reliability metrics to assess the performance of the Bulk-Power System. NERC's State of Reliability 2014 Report discusses two primary types of metrics: (1) event-driven metrics that measure the cumulative stress on the grid from events resulting in transmission loss, generation loss, and load loss; and (2) condition-driven metrics that quantify deviations from the adequate level of reliability established by NERC. Along with these two groups of metrics, NERC is also creating a new metric to quantify the impact of violations of Reliability Standards that are considered to have serious risk to the Bulk-Power System. NERC states that, in addition to reliability metrics, NERC's State of Reliability 2014 Report assesses grid reliability based on performance trends identified through data and analysis of system disturbances.[76]

55. The Commission supports NERC's efforts to develop reliability performance metrics and recognizes the benefit of such metrics, as NERC analyzes the emerging risks facing the Bulk-Power System, such as a rapidly changing fuel mix, unit retirements, continued advancement of variable resources, and a growing dependence on demand side management programs. Beyond assessing the overall reliability of the Bulk-Power System and identifying trends that could affect the industry's risk profile, reliability metrics that measure grid performance can also assist in evaluating the effectiveness of Reliability Standards. Therefore, we encourage NERC to continue developing its reliability metrics as described in its Performance Assessment and State of Reliability 2014 Report, and tie the results of grid performance-related metrics to ongoing Reliability Standards development efforts. Creating this feedback loop to the Reliability Standards development process will further support NERC's goal of developing results-based Reliability Standards.

---

[75] *See* Performance Assessment at 98 ("[t]he intent is to report the results of these metrics on an ERO Enterprise-wide basis, and also as applicable, distinguish results for NERC and individual Regional Entities").

[76] *See* Performance Assessment at 69-71 (citing NERC's State of Reliability 2014 Report, *available at* http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf).

56. We also encourage NERC to continue its effort to develop metrics to address other areas, such as situational awareness measures. Situational awareness was identified as a significant contributing factor in major events and as such, continued improvement in this area will further improve reliability.[77] In addition, we encourage NERC to refine its current reliability metrics to more effectively analyze risks to the Bulk-Power System. For example, NERC could refine its current metrics to incorporate additional data, such as an analysis of cause codes from the event analysis program, transmission availability data system, generating availability data system, protection system misoperations reporting, and progress of resolution of any gaps found in Reliability Standards. In addition, NERC could consider developing performance targets (i.e., normal or acceptable levels of performance) and tying such targets to the reliability metrics in order to enhance understanding of the state of reliability across the Bulk-Power System. Finally, as NERC continues its efforts to refine these reliability metrics, the Commission encourages NERC to collaborate with Commission staff in this area.

4. Reliability Standards Development

Performance Assessment

57. In its Performance Assessment, NERC addresses how it satisfies the requirements of section 39.3(b) of the Commission's regulations regarding NERC's ability to develop Reliability Standards that provide for an adequate level of reliability.[78] NERC also describes at length the improvements in its Reliability Standards development program since filing its Initial Performance Assessment.[79] Specifically, NERC highlights its efforts to transform Reliability Standards to a steady-state (i.e., a "stable set of clear, concise, high-quality, and technically sound Reliability Standards"),[80] including efforts to complete revisions to Reliability Standards in response to Commission directives and a comprehensive review of all Reliability Standards by the Independent Experts Review Panel. NERC adds that, "to set the foundation for a steady-state body of Reliability Standards, NERC established the [Independent Experts Review Panel] to evaluate the existing families of Reliability Standards and Requirements."[81] NERC explains that five

[77] *See, e.g.,* FERC and NERC Joint Staff Report, *Arizona-Southern California Outages on September 8, 2011* at 85 (2012).

[78] Performance Assessment, Att. 1 at 1-9.

[79] Performance Assessment at 22-32.

[80] *Id.* at 7.

[81] *Id.* at 14.

independent consultants with an array of electric industry experience presented a report to the NERC Board of Trustees in August 2013 that outlined a vision for transforming the NERC Reliability Standards to a steady-state, including short-term and long-term recommendations, recommending retirement of certain provisions, identification of "gaps" not currently addressed by Reliability Standards, and recommendation of a new construct to consolidate Reliability Standards and required actions.

58. NERC describes the Paragraph 81 project, a Commission-initiated project to identify and remove requirements from existing Reliability Standards that either: (1) provide little protection for Bulk-Power System reliability or (2) are redundant with other aspects of the Reliability Standards. NERC highlights other improvements to the Reliability Standards development process, including revisions to NERC's Standard Processes Manual to provide for a more efficient development process, formation of the Reliability Issues Steering Committee, and realignment of NERC's resources to "focus[] resources on the production of Reliability Standards rather than on executing and monitoring the development process."[82]

Commission Determination

59. The development of Reliability Standards is a fundamental responsibility of the ERO and a function that must be addressed as part of NERC's periodic performance assessment filings.[83] We recognize NERC's efforts to improve both the efficiency of its Reliability Standards development process as well as the quality of the Reliability Standards developed. While it appears that many of the initiatives described in NERC's Performance Assessment improved (or will improve) NERC's Reliability Standards development process, we believe NERC must continue to improve its programs as it moves forward into the next performance assessment period, as further discussed below.

60. We believe that NERC's formation of the Independent Experts Review Panel was particularly valuable. NERC tasked the Independent Experts Review Panel with evaluating the entire existing set of Reliability Standards, making recommendations on how to transition to a steady state, and identifying high-level gaps in reliability not currently addressed by existing Reliability Standards. As NERC states, the Independent Experts Review Panel's recommendations have been "pivotal" in NERC's evaluations of Reliability Standards by the Reliability Standard drafting teams. We are encouraged that the Independent Experts Review Panel's recommendations are, according to NERC,

[82] *Id.* at 30; *see generally id.* at 7-24.

[83] *See, e.g.*, 2010 Performance Assessment Order, 132 FERC ¶ 61,217 at P 67; Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 189.

either assigned to active drafting projects or to teams that conduct periodic reviews of Reliability Standards for future consideration.[84]

61. We also commend NERC on the improvements in the efficiency of its Reliability Standards development process, as reflected in the reduction of average time to revise or develop a new Reliability Standard. Specifically, NERC states that the average time for revising an existing Reliability Standard and development of a new Reliability Standard fell from a historical baseline of 27 and 40 months, respectively, to a period of 6 and 10 months, respectively, for projects completed since approval of NERC's revised Standard Processes Manual in 2013.[85]

62. Despite these apparent improvements to NERC's Reliability Standards processing times, the process for developing interpretations of Reliability Standards does not appear to be experiencing similar improvements in total processing time. Rather, over the Performance Assessment period, the average time for NERC to process a request for interpretation (i.e., time between the initial interpretation request and subsequent filing of the interpretation with the Commission) is approximately 21 months,[86] with processing times ranging from approximately 6 months to 50 months.

63. We understand that the processing time for interpretations may be affected by other considerations, including a possible preference for addressing ambiguities through the Reliability Standards development process. However, with NERC's stated goal of bringing the Reliability Standards program to a "steady state" (i.e., with fewer Reliability Standards under development or modification), the ability to efficiently resolve possible ambiguities through the interpretation process may take on added importance. Accordingly, we encourage NERC to explore ways to reduce the time needed to process a request for interpretation.

64. In addition, we believe that additional granularity in the measurement of Reliability Standards development would be beneficial. First, we note that the six and ten month average development time reported for recent projects includes projects for which

---

[84] *See* Performance Assessment at 16-17.

[85] *Id.* at 25.

[86] These statistics are derived from data filed in each petition for Commission approval during the Performance Assessment period. *See also* Quarterly Reports on Standards Development submitted in compliance with the 2010 Performance Assessment Order (Docket No. RR09-7-001).

the Commission imposed a specific deadline.[87] While we recognize the significant effort put in by NERC and stakeholders in meeting those deadlines, it is not clear whether these projects are representative of the improvements to the Reliability Standards process more generally. Instead, as we noted in the 2010 Performance Assessment Order, information regarding average total processing times for the development of Reliability Standards is of limited use where it reflects both "urgent" and "non-urgent" projects.[88] We continue to believe that total time for development as reported may need to reflect the overall complexity of the project and be compared to the initial expected time for completion. Thus, we will direct NERC to track, on a going-forward basis, actual project completion times as compared to estimated time for completion at the outset of a given project. We will also direct NERC to incorporate these more granular measures into its future performance assessment filings, beginning in 2019, and post them as developed prior to 2019.

65. Finally, we recognize that NERC made significant improvements in its Reliability Standards development process through redeployment of its and stakeholders' resources and other adjustments to the Reliability Standards development process. Among other things, NERC revised the composition of Reliability Standard drafting teams to include legal and compliance experts, and incorporated quality review and compliance assessment tool development in parallel or in conjunction with the Reliability Standards development process.[89] In addition to the technical expertise provided by industry volunteers, we believe NERC technical staff has an important role to play in providing feedback on proposed Reliability Standards throughout the development process.[90]

---

[87] *See, e.g., Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (requiring NERC to develop and submit within 90 days a proposed Reliability Standard addressing threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System).

[88] *See* 2010 Performance Assessment Order, 132 FERC ¶ 61,217 at PP 81, 85.

[89] Performance Assessment at 23. NERC staff is responsible for conducting a quality review of a Reliability Standard under development, prior to posting for formal comment and ballot to assess whether the documents are within the scope of the associated Standard Authorization Request, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval. NERC Standards Process Manual, Section 4.3.

[90] For example, NERC staff submitted useful comments on several draft Reliability Standards during the Performance Assessment period. *See, e.g.,*

(continued…)

Among other things, we believe NERC staff has unique expertise based on its compliance and enforcement experience, and unique insight into emerging reliability issues gained through NERC's administration of the events analysis program. Therefore, we encourage NERC's technical staff to provide feedback to the Reliability Standard drafting teams as early as possible in the drafting process so the drafting team can consider NERC staff's unique insights, particularly prior to comment or ballot periods.

5. Regional Entity Performance and Coordination

Performance Assessment

66. In its Performance Assessment, NERC explains its ongoing efforts to increase consistency and promote coordination throughout the ERO Enterprise. NERC states that the ERO Enterprise has been effective in mitigating important risks to the Bulk-Power System since its inception in 2006. NERC highlights the ability of the Regional Entities to identify trends and leading indicators of potential reliability problems to be addressed. NERC notes efforts to address protection system misoperations and transmission right-of-way clearances as examples of situations where the ERO Enterprise was able to use information from the Regional Entities to develop strategies to address potential risks.[91]

67. NERC states that the compliance monitoring and enforcement program implemented by NERC and the Regional Entities "has been effective in ensuring that compliance violations are identified and mitigated, thereby reducing reliability risk."[92] NERC states that the ERO Enterprise has uniform procedures for compliance and enforcement, including standardized penalty guidelines. For example, NERC states that all Regional Entities utilize the Find, Fix, Track and Report (FFT) process to resolve a high number of minimal risk issues and that NERC, through its monthly reviews and annual spot checks, verifies that the parameters for identifying minimal risk issues are consistently applied throughout the ERO Enterprise.

68. NERC also states the Reliability Assurance Initiative will help NERC foster greater consistency and efficiency in its compliance monitoring and enforcement process, providing a greater level of predictability for registered entities to understand how the

---

Docket Nos. RM14-13-000 (COM-001-2 and COM-002-4), RM13-15-000 (CIP Version 5), and RM12-16-000 (Generator Requirements at the Transmission Interface).

[91] Performance Assessment, Att. 6 at 5.

[92] *Id.* at 6.

Reliability Standards are applied and enforced.[93] Moreover, NERC explains that it and the Regional Entities no longer create nine separate CMEP implementation plans, but rather have consolidated these documents into a single, integrated CMEP implementation plan for the ERO Enterprise, which eliminates redundant information, improves transparency of CMEP activities, and promotes consistency among Regional Entities.[94]

69. NERC states that, in order to achieve excellence in the oversight and execution of its statutory functions, it must improve coordinated operations across the ERO Enterprise by focusing on six areas relating to the relationships and allocations of responsibilities between and among NERC and the Regional Entities. These areas include (1) clarifying roles and responsibilities, (2) coordinating strategic planning, (3) coordinating operational decision-making, (4) achieving consistency, (5) sharing tools and infrastructure for delegated functions, and (6) coordinating communications.[95] NERC identifies 11 action items aimed at achieving these goals. NERC also states that, to improve the delegation process, NERC and the Regional Entities should work together to update and refine the regional delegation agreements, which are due for renewal in May 2015, to provide a clearer division of responsibilities.[96] In the development of the Performance Assessment, numerous stakeholder comments focused on the need for consistency and coordination across the ERO Enterprise.[97]

Commission Determination

70. The Commission recognizes and supports NERC's efforts to increase consistency and promote coordination across the ERO Enterprise. A key element of consistency is the transparency of the ERO Enterprise's processes and its outcomes. Improved consistency and coordination helps to clarify the roles and responsibilities of NERC and the Regional Entities and should lead to more efficient and uniform work practices. Specifically, we believe that a focus on achieving consistent compliance and enforcement outcomes (e.g., monetary penalties, registration decisions, and consistent understanding of Reliability Standard requirements) while not equating consistency with a "lowest common denominator" approach would provide the greatest benefit to registered entities.

---

[93] *Id.*

[94] Performance Assessment at 55.

[95] Performance Assessment, Att. 6 at 7-8.

[96] *See id.*, at 7-16.

[97] *See* Performance Assessment, Att. 4 at 13-15, 21, 29, and 32.

Accordingly, we are pleased to see NERC's efforts in this area such as the adoption of a single, integrated CMEP implementation plan for the ERO Enterprise. We believe that actions such as the integrated CMEP are a step toward addressing the concerns raised by stakeholders regarding potential inconsistencies across the Regional Entities.[98]

71. However, to better understand NERC's ongoing efforts, we direct NERC to submit an informational filing within 12 months of the date of this order that describes NERC's progress in increasing consistency and promoting coordination across the ERO Enterprise. Specifically, NERC should address how it is improving coordinated operations and describe any efforts it has made to improve such operations, including, but not limited to the 11 action items described in Attachment 6 of the Performance Assessment.

72. In addition, NERC should continue to promote transparency in its enforcement programs, particularly as it moves forward with its Reliability Assurance Initiative, given the value of transparency in encouraging full and adequate mitigation practices and in providing assurance to the Commission, registered entities, and the public that the program is being fairly and consistently implemented across all regions. We note that the FFT program created efficiencies in the ERO Enterprise's enforcement process, without the need to sacrifice any degree of transparency in the form of current public disclosure regarding FFT-processed violations. Therefore, we expect NERC to continue making information publicly available concerning possible non-compliance (other than those involving physical security or cybersecurity concerns) resolved through any and all processing methods.

73. We also support NERC's efforts to develop metrics to measure the overall effectiveness of the ERO Enterprise. While we recognize that enforcement metrics developed to date aid in promoting consistency and measuring the performance of NERC and the individual Regional Entities,[99] they represent only one aspect of consistency across the ERO Enterprise. Therefore, we will direct NERC to continue developing performance metrics that measure consistency, coordination, and efficiency between and among NERC and the Regional Entities in order to achieve predictable, timely, and consistent results across the ERO Enterprise and incorporate these metrics into its future performance assessment filing, beginning in 2019. In developing such metrics, we

[98] We note that the Commission also supported such efforts in the 2010 Performance Assessment Order. *See* 2010 Performance Assessment Order, 132 FERC ¶ 61,217 at P 138.

[99] *See* Performance Assessment, Att. 5 at 24-26.

encourage NERC to focus on achieving consistent outcomes on issues such as assessing monetary penalties, assessing non-monetary penalties, registering entities, and exhibiting a consistent understanding of requirements in the auditing process.

The Commission orders:

(A) The Commission hereby accepts NERC's Performance Assessment and finds that NERC continues to meet the statutory and regulatory requirements for ERO certification set forth in section 215(c) of the FPA and section 39.3(b) of our regulations, as discussed in the body of this order.

(B) The Commission hereby finds that the Regional Entities continue to meet the statutory and regulatory requirements set forth in section 215(e) of the FPA and section 39.3(c) of our regulations, as discussed in the body of this order.

(C) NERC is hereby directed to submit an informational filing within 12 months of the date of this order, as discussed in the body of this order.

(D) NERC is hereby directed to include additional information in its future performance assessment filings, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

SUNSHINE ACT MEETING NOTICE

November 13, 2014

The following notice of meeting is published pursuant to section 3(a) of the government in the Sunshine Act (Pub. L. No. 94-409), 5 U.S.C. 552b:

AGENCY HOLDING MEETING:	FEDERAL ENERGY REGULATORY COMMISSION
DATE AND TIME:	November 20, 2014 10:00 A.M.
PLACE:	Room 2C 888 First Street, N.E. Washington, D.C. 20426
STATUS:	OPEN
MATTERS TO BE CONSIDERED:	Agenda * NOTE - Items listed on the agenda may be deleted without further notice.
CONTACT PERSON FOR MORE INFORMATION:	Kimberly D. Bose Secretary Telephone (202) 502-8400 For a recorded message listing items struck from or added to the meeting, call (202) 502-8627.

This is a list of matters to be considered by the Commission. It does not include a listing of all documents relevant to the items on the agenda. All public documents, however, may be viewed on line at the Commission's website at http://www.ferc.gov using the eLibrary link, or may be examined in the Commission's Public Reference Room.

1010TH - MEETING

REGULAR MEETING

November 20, 2014

10:00 AM

Item No	Docket No.	Company
		ADMINISTRATIVE
A-1	AD02-1-000	Agency Business Matters
A-2	AD02-7-000	Customer Matters, Reliability, Security and Market Operations
A-3	AD07-13-008	2014 Report on Enforcement
		ELECTRIC
E-1	EC14-96-000	Exelon Corporation and Pepco Holdings, Inc.
E-2	AD13-7-000	Centralized Capacity Markets in Regional Transmission Organizations and Independent System Operators
	AD14-8-000	Winter 2013-2014 Operations and Market Performance In Regional Transmission Organizations and Independent System Operators
E-3	AD14-16-000	Kansas City Board of Public Utilities
E-4	RM14-15-000	Physical Security Reliability Standard
E-5	OMITTED	
E-6	RM14-10-000	Real Power Balancing Control Performance Reliability Standard
E-7	ER14-2936-000	Sunbury Generation LP
E-8	ER14-2963-000	California Independent System Operator Corporation
E-9	OA14-3-000	FPL Energy Oklahoma Wind, LLC
E-10	RR14-5-000	North American Electric Reliability Corporation
E-11	EL15-15-000	PJM Interconnection, L.L.C.

GAS

G-1	PL15-1-000	Cost Recovery Mechanisms for Modernization of Natural Gas Facilities
G-2	RM14-21-000	Natural Gas Act Pipeline Maps
G-3	RP12-318-003 RP12-318-005	Texas Eastern Transmission, LP
G-4	RP13-431-003	Dominion Transmission, Inc.
G-5	OR14-6-000 OR14-6-001	BP Pipelines (Alaska) Inc., ConocoPhillips Transportation Alaska, Inc. and ExxonMobil Pipeline Company

HYDRO

H-1	P-12588-010	Hydraco Power, Inc. and Warren David Long
H-2	P-12690-007 P-12690-009 EL14-47-001	Public Utility District No. 1 of Snohomish County, Washington
H-3	P-13997-002	Richard A. Glover, Jr.
H-4	P-2210-248	Appalachian Power Company

CERTIFICATES

C-1	RM12-11-002	Revisions to Auxiliary Installations, Replacement Facilities, and Siting and Maintenance Regulations

Kimberly D. Bose,
Secretary.

A free webcast of this event is available through www.ferc.gov. Anyone with Internet access who desires to view this event can do so by navigating to www.ferc.gov's Calendar of Events and locating this event in the Calendar. The event will contain a link to its webcast. The Capitol Connection provides technical support for the free webcasts. It also offers access to this event via television in the DC area and via phone bridge for a fee. If you have any questions, visit www.CapitolConnection.org or contact Danelle Springer or David Reininger at 703-993-3100.

Immediately following the conclusion of the Commission Meeting, a press briefing will be held in the Commission Meeting Room. Members of the public

may view this briefing in the designated overflow room. This statement is intended to notify the public that the press briefings that follow Commission meetings may now be viewed remotely at Commission headquarters, but will not be telecast through the Capitol Connection service.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 21, 2014

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
Five-Year Electric Reliability Organization Performance Assessment Report
Submitted in Accordance with 18 C.F.R. § 39.3(c)

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) respectfully submits its Five-Year Electric Reliability Organization (ERO) Performance Assessment Report in accordance with the requirements of the Commission's regulations at 18 C.F.R. § 39.3(c).

The filing consists of this transmittal letter and the following documents:

- **Overview of NERC Activities and Accomplishments in the Five-Year Period**
- **Attachment 1:** Discussion of How NERC Meets the ERO Certification Criteria of 18 C.F.R. §39.3(b)
- **Attachment 2:** Joint Regional Entity Self-Assessment
- **Attachment 3:** NERC Assessment of Regional Entity Delegated Functions
- **Attachment 4:** NERC Consideration of Industry Feedback
- **Attachment 5:** Status of Areas for Improvement Identified in the Order on the Three-Year ERO Performance Assessment
- **Attachment 6:** NERC's Plan and Initiatives for Improving Coordinated Operations Across the ERO Enterprise

These documents are transmitted in two PDF files.

Please place the following persons on the Commission's official service list on behalf of NERC with respect to this submittal and the proceeding that we understand the Commission will open pursuant to 18 C.F.R. § 39.3(c) to consider this report:

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Nina H. Jenkins-Johnston
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
nina.johnston@nerc.net

Lauren A. Perotti
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Nina H. Jenkins-Johnston
Nina H. Jenkins-Johnston

Attorney for the North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RR14-__-000**

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

SUBMITTED IN ACCORDANCE WITH 18 C.F.R. §39.3(c)

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

Charles A. Berardesco
Senior Vice President and General Counsel
Willie L. Phillips
Assistant General Counsel
Nina H. Jenkins-Johnston
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
willie.phillips@nerc.net
nina.johnston@nerc.net

Counsel for North American Electric Reliability Corporation

July 21, 2014

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

OVERVIEW OF NERC ACTIVITIES AND ACCOMPLISHMENTS IN THE FIVE-YEAR PERIOD

SUBMITTED IN ACCORDANCE WITH 18 C.F.R. §39.3(c)

JULY 21, 2014

TABLE OF CONTENTS

I. INTRODUCTION 1

A. Contents of Five-Year ERO Performance Assessment 1

B. Industry Engagement 4

II. NERC ACTIVITIES AND ACCOMPLISHMENTS 7

A. The ERO Is Transitioning NERC Reliability Standards to a Steady-State 7

1. Completing Commission Directives 12

2. The Standards Independent Experts Review Panel 14

3. Implementation of the Paragraph 81 Project 17

4. Development of Compliance Assessment Tools Concurrently with Reliability Standards Development 19

5. Review of Regional Reliability Standards 21

6. Improvements in the Reliability Standards Development Process 22

a. Revisions to the *Standard Processes Manual* and Related Improvements 22

b. Formation and Work of the Reliability Issues Steering Committee 28

c. Realignment of Resources in the Reliability Standards Program 30

d. Developing and Implementing Procedures for the Cost-Effective Analysis Process 32

7. Improved Stakeholder Access to Reliability Standards Information 33

8. Specific Reliability Standards Projects 34

a. Critical Infrastructure Protection Version 5 Reliability Standards 34

b. Transmission Vegetation Management 36

c. Protection System Maintenance and Testing 37

d. Geomagnetic Disturbances 40

e. Physical Security Reliability Standard 42

B. The ERO Is Implementing Processes to Register Entities Commensurate with Risk to the Bulk Power System 44

1. Improved Registration Processes, Information Systems, and Methods Across Regional Entities 44

2. BES Definition 45

C. The ERO Monitors and Enforces Compliance with Reliability Standards in an Efficient and Transparent Manner Using Enforcement Processes that Match the Risk and Importance of Possible Violations to BPS Reliability 49

1. Compliance Enforcement Initiative and Find, Fix, Track and Report 50

2. Reliability Assurance Initiative 51

a. RAI Improvements to Compliance Monitoring Processes 52

b. RAI Improvements to Compliance Enforcement Processes 53

3. Development of a Consolidated CMEP Implementation Plan 55

4. Improvements in Processing of Compliance and Enforcement Items by NERC and the Regional Entities 56

a. NERC and the Regional Entities Have Improved the Speed and Efficiency of Processing Enforcement Items 56

b. Oversight of Regional Entity Processes and Actions 59

c. Developing Common Compliance Auditor Qualifications Across the ERO Enterprise 59

d. Enhancing the Training Program for Auditors so that Processes and Procedures Developed in the RAI are Implemented Consistently Across the ERO Enterprise 60

D. Identification, Prioritization, and Dissemination of Information on Risks to the BPS 61

1. Establishing a Structured Reliability Risk Management Process 63

2. ERO Top Priority Reliability Risks for 2014-2017 64

3. NERC Event Analysis Process and How it is Used to Identify Risks to the BPS and Disseminate Lessons Learned 66

4. Reports on Reliability 69

5. Bulk Power System Awareness Department 71

E. The ERO Facilitates Information Sharing on Cybersecurity and Cyber and Physical Threats to the BPS among Industry, Regional Entities, and Government 73

1. Critical Infrastructure Department Activities 75

a. Critical Infrastructure Protection Committee 75

b. Security Readiness Program 76

c. Grid Security Conferences 77

d. Grid Security Exercises 78

e. Electricity Sub-sector Coordinating Council 78

2. ES-ISAC Tools and Activities 79

a. ES-ISAC Portal 79

b. Analytics 80

c. Industry and Government Coordination 81

d. Cyber Risk Preparedness Assessments 81

III. NERC CONTINUES TO MEET THE §39.3(b) CRITERIA 82

IV. REGIONAL ENTITY PERFORMANCE AND EFFECTIVENESS CONTINUES TO IMPROVE 89

V. NERC HAS SURVEYED STAKEHOLDERS FOR COMMENTS AND SUGGESTIONS FOR IMPROVEMENTS 92

VI. NERC HAS MADE SUBSTANTIAL PROGRESS IN COMPLETING ACTIONS ON ITEMS IN THE COMMISSION'S ORDER ON THE *THREE-YEAR ERO PERFORMANCE ASSESSMENT REPORT* 95

VII. NERC HAS A VISION AND A PLAN FOR IMPROVING COORDINATED OPERATONS ACROSS THE ERO ENTERPRISE TO REACH THE END STATE OF A HIGHLY EFFECTIVE AND EFFICIENT ERO ENTERPRISE 96

VIII. CONCLUSION 103

ATTACHMENTS:

Attachment 1: Discussion of How NERC Meets the ERO Certification Criteria of 18 C.F.R. §39.3(b)

Attachment 2: Joint Regional Entity Self-Assessment

Attachment 3: NERC Assessment of Regional Entity Delegated Functions

Attachment 4: NERC Consideration of Industry Feedback

Attachment 5: Status of Areas for Improvement Identified in the Order on the Three-Year ERO Performance Assessment

Attachment 6: NERC's Plan and Initiatives for Improving Coordinated Operations Across the ERO Enterprise

I. INTRODUCTION

A. Contents of Five-Year ERO Performance Assessment

The North American Electric Reliability Corporation (NERC) is submitting this *Five-Year Electric Reliability Organization (ERO) Performance Assessment Report* in accordance with the Commission's regulations at 18 C.F.R. §39.3(c). NERC was certified by the Commission as the ERO, pursuant to §215(c) of the Federal Power Act (FPA), by Commission order issued July 20, 2006.[1] The Commission's regulations at 18 C.F.R. Part 39 require the ERO to submit an assessment of its performance three years from the date of certification and every five years thereafter.[2] On July 20, 2009, NERC filed its initial, Three-Year ERO Performance Assessment Report with the Commission. On September 16, 2010, the Commission issued an order accepting the three-year performance assessment of NERC and the Regional Entities and found that they continue to satisfy the statutory and regulatory criteria for certification.[3] NERC now submits this *Five-Year ERO Performance Assessment Report* in accordance with the Commission's regulations.

In this *Five-Year ERO Performance Assessment Report*, NERC describes its activities and accomplishments during the assessment period[4] in carrying out its statutory and regulatory responsibilities as the ERO, with a particular focus on the latter part of the assessment period and on NERC's current and planned initiatives. As required by 18 C.F.R. §39.3(c)(1), this report: (i) describes how NERC continues to meet the certification criteria of 18 C.F.R. §39.3(b); (ii)

[1] *Order Certifying the North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

[2] 18 C.F.R. §39.3(c).

[3] *Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010).

[4] NERC defines the assessment period as January 1, 2009 through May 31, 2014.

evaluates of the effectiveness of each Regional Entity in carrying out its delegated functions;[5] and (iii) addresses stakeholder comments on NERC's performance that were collected in the preparation of this report. As noted, this report identifies actions that NERC and the Regional Entities are currently taking and plan to take to continue to improve their operations to enhance the reliable operation of the bulk power system (BPS). Unlike the three-year performance assessment report, NERC has not presented a program area-by-program area discussion of activities because NERC's annual business plan and budgets (and those of the Regional Entities) provide the Commission with an annual, detailed look at NERC's and each Regional Entity's current and planned activities by program area. Instead, this *Five-Year ERO Performance Assessment Report* highlights activities and accomplishments in support of the ERO Enterprise[6] Strategic Plan (Strategic Plan) initiatives applicable to this assessment period. These initiatives include: (i) Reliability Standards reform (both as to the number and content of Reliability Standards and the processes for developing them); (ii) the Reliability Assurance Initiative (RAI) which involves identifying risks to reliability and reformulating the compliance monitoring and enforcement processes to have a risk-based focus; and (iii) the revision of the bulk electric system (BES) definition.

In this *Five-Year ERO Performance Assessment Report*, NERC also demonstrates how the ERO is improving the performance of, and mitigating risks to, the BPS as related to avoidable outages. As detailed in NERC's *State of Reliability 2014* report, the number of BPS transmission-related events resulting in loss of firm load, other than events caused by factors

[5] The eight Regional Entities are: (i) Florida Reliability Coordinating Council, Inc.; (ii) Midwest Reliability Organization; (iii) Northeast Power Coordinating Council, Inc.; (iv) ReliabilityFirst Corporation; (v) SERC Reliability Corporation; (vi) Southwest Power Pool Regional Entity; (vii) Texas Reliability Entity, Inc.; and (viii) Western Electricity Coordinating Council (WECC).

[6] NERC uses the term "ERO Enterprise" to encompass both NERC and the eight Regional Entities.

external to the transmission system's actual performance (i.e., weather-initiated events), decreased from an average of ten per year over a ten year period (2002 through 2011) to seven in 2013. The daily severity risk index value (SRI), a metric created by NERC that measures risk impact or "stress" from events resulting in the loss of transmission, generation, and load, has been stable from 2008 to 2013. Including weather-initiated events, 2013 had no high-stress days, which is within the range of zero to seven days experienced during 2008 through 2013. The availability of the bulk transmission system, as measured by the SRI and other metrics, continues to remain high with no statistically significant change from 2008 to 2013.[7]

Despite the progress made to date in improving the reliability of the BPS and reducing the risks to reliability, opportunities remain for enhancements to ensure that the BPS remains reliable. NERC describes these opportunities, and its initiatives designed to pursue them, in this *Five-Year ERO Performance Assessment Report*. Additionally, in this assessment report, NERC evaluates the effectiveness of each Regional Entity in performing its delegated functions, drawing from NERC's ongoing oversight activities, the Regional Entities' self-assessments, and feedback solicited from industry through an industry survey and posting the Regional Entity self-assessments for stakeholder comment.

Finally, NERC describes how its compliance monitoring and enforcement efforts have matured into a robust program providing industry with greater certainty on actions, outcomes, and reliability consequences. The actions taken by the ERO to identify, correct, and prevent violations of NERC's Reliability Standards have promoted the reliability of the BPS. For example, the adoption, modification, and rigorous enforcement of NERC's transmission vegetation management Reliability Standard (FAC-003), which became mandatory and

[7] NERC's *State of Reliability 2014* report is available at: http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf.

enforceable in 2007, has dramatically reduced the number of outages caused by vegetation growing into high voltage lines. From 2004 through 2008, there were 58 reported outages. By contrast, from 2009 through 2013, only six instances were reported.[8]

B. Industry Engagement

The electric industry has made tremendous strides towards improving reliability since the August 2003 Northeast blackout, which left 50 million customers without power. Enactment of §215 of the FPA, NERC's certification as the ERO, and the adoption of mandatory and enforceable Reliability Standards renewed the industry's focus on reliability. This focus, which includes proactive steps by the ERO to identify and address risks and avoid preventable events, has had a demonstrable and positive impact on reliability.

In passing the Energy Policy Act of 2005, which included the enactment of §215, Congress recognized the importance of an international ERO across North America to ensure the reliability of the BPS. As the ERO, NERC plays a unique role in facilitating industry engagement to create effective approaches for reliability initiatives. For example, industry participation in Reliability Standards development from start to finish is critical. Industry stakeholders participate in Reliability Standards development with increasing frequency since changes to the *Standard Processes Manual* (SPM) became effective June 26, 2013.[9] Stakeholders participate directly by joining standard drafting teams or participating as observers; attending and discussing Reliability Standards at webinars, committee meetings or technical conferences with standard drafting team members and NERC staff; communicating technical opinions directly to standard drafting teams or NERC staff; and commenting and voting on

[8] NERC's quarterly *Vegetation-Related Transmission Outage Reports* are available at: http://www.nerc.com/pa/comp/CE/Pages/vegetation-management-reports.aspx.

[9] The SPM is Appendix 3A to the NERC Rules of Procedure (NERC ROP) and is available at: http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.

proposed Reliability Standards. As of May 2014, 858 stakeholder representatives had registered their eligibility to vote on proposed Reliability Standards as members of the Registered Ballot Body, and in 2013 alone NERC hosted 43 Reliability Standard industry webinars attended by an average of 360 participants. During the last six months of 2013, standard drafting teams and five-year review teams made up of 195 industry volunteers participated in 60 team meetings to advance standard development activities.[10]

Industry engagement is also a critical component of NERC's strategic initiatives, such as RAI. Through RAI, NERC and the Regional Entities are adopting a risk-based approach to compliance monitoring and enforcement activities.[11] NERC and the Regional Entities are spearheading RAI, with substantial input from industry representatives on important RAI projects. For example, the ERO Enterprise is examining information flow requirements for registered entity self-reporting and is developing criteria to evaluate the various approaches to reliability risk assessments and internal controls review and testing. Similarly, industry played an important role in the development and implementation of NERC's Find, Fix, Track and Report (FFT) process, an enforcement mechanism that differentiates and processes noncompliance occurrences according to their significance to the reliability of the BPS.

Preparation of this *Five-Year ERO Performance Assessment Report* has benefited from considerable input from industry. On October 31, 2013, NERC distributed a 36-question online survey soliciting numerical ratings and free-form responses from registered entities regarding the performance of NERC and the Regional Entities in carrying out their responsibilities. On March 3, 2014, NERC posted a draft statement of its activities and accomplishments, as well as drafts of

[10] As described later in this *Overview of NERC Activities and Accomplishments in the Five-Year Period*, five-year review teams are engaged in the five-year reviews of those Reliability Standards that have been adopted by the American National Standards Institute (ANSI) as national standards, in accordance with §13.0 of the SPM.

[11] NERC expects to submit an informational filing in 2014 fully describing RAI.

the Regional Entities' self-assessments, on NERC's website for industry comment. On June 17, 2014, NERC posted a complete draft of the *Five-Year ERO Performance Assessment Report* on its website for stakeholder comment. A compilation of the responses to the survey questions and of the comments received on the March 3, 2014 and June 17, 2014 postings, are included as **Attachment 4** to this report.[12]

This *Five-Year ERO Performance Assessment Report* includes the following attachments:

Attachment 1: Discussion of How NERC Meets the ERO Certification Criteria of 18 C.F.R. §39.3(b)

Attachment 2: Joint Regional Entity Self-Assessment[13]

Attachment 3: NERC Assessment of the Regional Entities' Delegated Functions

Attachment 4: NERC Consideration of Industry Feedback

Attachment 5: Status of Areas for Improvement Identified in the Order on the Three-Year ERO Performance Assessment

Attachment 6: NERC's Plan and Initiatives for Improving Coordinated Operations Across the ERO Enterprise

NERC requests that the Commission accept this filing as satisfying NERC's obligation under 18 C.F.R. §39.3(c) to file a performance assessment every five years after the three-year anniversary of its certification as the ERO. Pursuant to 18 C.F.R. §39.3(c), the Commission will initiate a proceeding, with opportunity for public comment, on NERC's *Five-Year ERO Performance Assessment Report*. At the conclusion of the proceeding, the Commission will either issue an order finding that NERC and the Regional Entities meet the statutory and regulatory criteria, or direct them to come into or improve their compliance with

[12] Issues raised by stakeholders, and the responses of NERC and the Regional Entities, are addressed in this report. Industry responses to the survey were discussed at the February 28, 2014 NERC Member Representatives Committee (MRC) meeting, and industry responses to the survey and comments received on the March 3, 2014 posting were discussed at the May 6, 2014 NERC Board of Trustees (NERC Board) meeting.

[13] **Attachment 2** contains both an overall self-assessment of the Regional Entities' collective performance during the assessment period, and individual discussions of how each Regional Entity satisfied the applicable statutory and regulatory criteria including those specified in the Commission's regulations at 18 C.F.R. §39.8.

the requirements of Part 39. Because considerable opportunity has been provided for stakeholder input through the industry survey and the posting of drafts of this report, NERC suggests that the Commission initiate its proceeding by setting a comment period of no more than 45 days on the filed report. Conducting the Commission's proceeding pursuant to §39.3(c) in an expeditious manner will allow NERC and the Regional Entities both to receive timely feedback from commenters and the Commission and to move forward and devote time and resources to the various initiatives outlined in the report. NERC will use the contents of this *Five-Year ERO Performance Assessment Report* and the results of the proceeding to guide the continuing implementation and evolution of its programs in the years ahead.

II. NERC ACTIVITIES AND ACCOMPLISHMENTS

This section describes activities and initiatives that NERC has completed during the assessment period, has in progress, or plans to commence in the near future, to enhance the reliability of the BPS and to increase the effectiveness and efficiency of the operations of the ERO Enterprise. NERC focuses this discussion on the following five areas: (i) development of clear, reasonable and technically sound Reliability Standards; (ii) registration of entities with functional responsibilities for the reliability of the BPS; (iii) monitoring and enforcing compliance with Reliability Standards; (iv) identification, prioritization and dissemination of information on risks to the reliability of the BPS; and (v) collecting and sharing information on cybersecurity and threats to the cyber and physical security of the BPS.

A. The ERO Is Transitioning NERC Reliability Standards to a Steady-State

Since the three-year performance assessment, NERC has made great strides in transforming Reliability Standards to a steady-state, which NERC defines as a stable set of clear, concise, high-quality, and technically sound Reliability Standards. Steady-state Reliability Standards are results-based and include requirements that promote reliability. They are

sustainable (stable), necessary for accountability, and sufficient to maintain the reliability of the BPS. After a set of steady-state Reliability Standards is fully developed, it is expected that Reliability Standards will only need to be amended in response to changes in risks, technology, practices, and similar changes. In support of this objective, during the assessment period, NERC focused on addressing FERC directives and conducting periodic reviews of Reliability Standards. NERC expects to complete the development of a set of steady-state Reliability Standards in 2015.

NERC's efforts to arrive at steady-state Reliability Standards would not have been possible without strong participation from industry stakeholders, FERC staff, the NERC Standards Committee (SC), and other NERC committees and working groups, including the Reliability Issues Steering Committee (RISC) and the Standards Process Improvement Group (SPIG), the NERC Board, and the NERC MRC. Arriving at a set of steady-state Reliability Standards required changes in NERC's Reliability Standards development process. The SPIG identified needed changes to the process. These changes were implemented through amendments to the SPM that became effective on June 26, 2013, upon Commission approval.[14]

The currently effective *Reliability Standards Development Plan 2014-2016* (RSDP), approved by the NERC Board in November 2013, endorses the objective of arriving at steady-state Reliability Standards.[15] It specifically defines "steady-state" as a stable set of clear, concise, high quality, and technically sound Reliability Standards that are results-based and that exclude requirements that do little to promote reliability. The 2014-2016 RSDP prioritizes future Reliability Standards projects as high, medium, low or pending technical committee input based

[14] *Order Approving Revisions to Electric Reliability Organization's Standard Processes Manual*, 143 FERC ¶ 61,273 (2013).

[15] *Reliability Standards Development Plan 2014-2016* is available at: http://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsDevelopmentPlan.aspx.

on a series of inputs, which include the Standards Independent Expert Review Panel's (IERP or Panel) content and quality assessments (discussed later in this document). Prioritization considerations were influenced by: (i) RISC category rankings (also described later in this document); (ii) outstanding regulatory directives; (iii) regulatory deadlines; (iv) Paragraph 81 retirement candidates (also described below); (v) content and quality assessments by the IERP (also described below); and (vi) additional considerations such as fill-in-the-blank status and five-year review assessment commitments.

During the assessment period, NERC launched several initiatives to improve Reliability Standards, including: (i) the results-based Reliability Standards initiative; (ii) the Paragraph 81 project; (iii) the reorganization of the Reliability Standards department; and (iv) the establishment of the IERP. Each of these initiatives built upon the prior initiative, resulting in a comprehensive set of criteria by which to evaluate whether a Reliability Standard has reached its steady-state.

Since the three-year performance assessment, NERC initiated the results-based concept for developing the content of Reliability Standards. Each requirement of a results-based Reliability Standard identifies a measurable outcome such as: (i) a stated level of reliability performance; (ii) a reduction in a specified reliability risk (prevention); or (iii) a necessary competency. In 2011, NERC began training standard drafting teams to write results-based Reliability Standards. In 2013, the Commission approved the first Reliability Standard that resulted from that effort, FAC-003-2 – Transmission Vegetation Management.[16] NERC is in the process of converting major families of Reliability Standards into results-based Reliability

[16] *Revisions to Reliability Standard for Transmission Vegetation Management*, 142 FERC ¶ 61,208 (2013).

Standards.[17] These Reliability Standards include those dealing with long-term planning, reliability coordination, and real-time operations.[18]

In 2012, in response to FERC's invitation to NERC in a March 15, 2012 Order, NERC and industry conducted the Paragraph 81 project, which identified and retired requirements from Reliability Standards that did little to support reliability.[19] The criteria developed to scrutinize existing requirements in Reliability Standards in response to the Commission's Paragraph 81 invitation continue to be used by standard drafting teams to evaluate the need for proposed requirements in new Reliability Standards development projects.[20]

In further support of the development of steady-state Reliability Standards, NERC reorganized its Standards department in 2013 to focus resources on addressing FERC directives, conducting periodic reviews of Reliability Standards, and completing ongoing Reliability Standards development projects. NERC also conducted a parallel effort to identify future work necessary to transform the Reliability Standards to steady-state, by establishing the IERP to evaluate the content and quality of every requirement in the NERC Reliability Standards. The Panel established its own criteria, which included those developed in the Paragraph 81 project, to

[17] The terms "families of standards" refers to groupings of Reliability Standards that address a common subject matter area, e.g., Emergency Preparedness and Operations (EOP), Personnel Performance, Training and Qualifications (PER), and Protection and Controls (PRC).

[18] NERC revised the Transmission Planning (TPL) Reliability Standards and a single consolidated Reliability Standard approved by FERC; revisions to the Transmission Operations (TOP), Interconnection Reliability Operations and Coordination (IRO), Modeling (MOD), and Voltage and Reactive (VAR) standards are pending FERC approval.

[19] "Paragraph 81" refers to P 81 of the Commission's March 15, 2012 Order on NERC's FFT process, in which the Commission invited NERC (as well as the Regional Entities and other stakeholders) to identify specific standards requirements that could be revised or removed because they provide little protection for BPS reliability or are redundant. *Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing*, 138 FERC ¶ 61,193 (2012) (March 2012 FFT Order), at P 81. *See* §II.A.3 below for a more detailed description of the Paragraph 81 initiative.

[20] The Paragraph 81 criteria are outlined in the Phase I *Paragraph 81 Project Technical White Paper* available at: http://www.nerc.com/pa/Stand/Project%20201302%20Paragraph%2081%20RF/P81_Phase_I_technical_white_paper_FINAL.pdf.

determine whether a requirement was steady-state or needed further revisions. The Panel's recommendations set the course for arriving at high quality, results-based Reliability Standards with sustainable requirements. NERC is preparing training materials for standard drafting teams to highlight the use of the Panel's methods for content and quality assessments of Reliability Standards.

NERC has also been diligent in assessing the need for Reliability Standards that address reliability gaps. Sections II.A.8.a through e below discuss five important areas of Reliability Standards development focusing on reliability risk: (i) the Critical Infrastructure Protection (CIP) Version 5 Reliability Standards; (ii) vegetation management (formerly a top ten cause of outage events); (iii) protection system maintenance and testing; (iv) geomagnetic disturbances (GMD) (a high-impact, low-frequency risk to the BPS which does not readily manifest in reliability performance data, but nonetheless represents a significant risk to the BPS); and (v) the physical security Reliability Standard.

A more recent initiative to assist with the achievement of steady-state Reliability Standards is the development of a template for enhanced periodic reviews of Reliability Standards that have not yet been revised through other Reliability Standards development projects. NERC is working with industry stakeholders to develop the necessary criteria for determining which Reliability Standards will be subject to these enhanced periodic reviews as well as whether the Reliability Standards have reached their steady-state. NERC expects the criteria to include those from the results-based Reliability Standards initiative, the Paragraph 81 project and the IERP. Upon reaching a consensus with industry on the criteria for evaluating whether a requirement is steady-state, and after completing the projects identified in the ERO's 2014-2016 RSDP and the ERO's 2015-2017 RSDP, NERC will apply the criteria to the

Reliability Standards through enhanced periodic reviews beginning in 2015.[21]

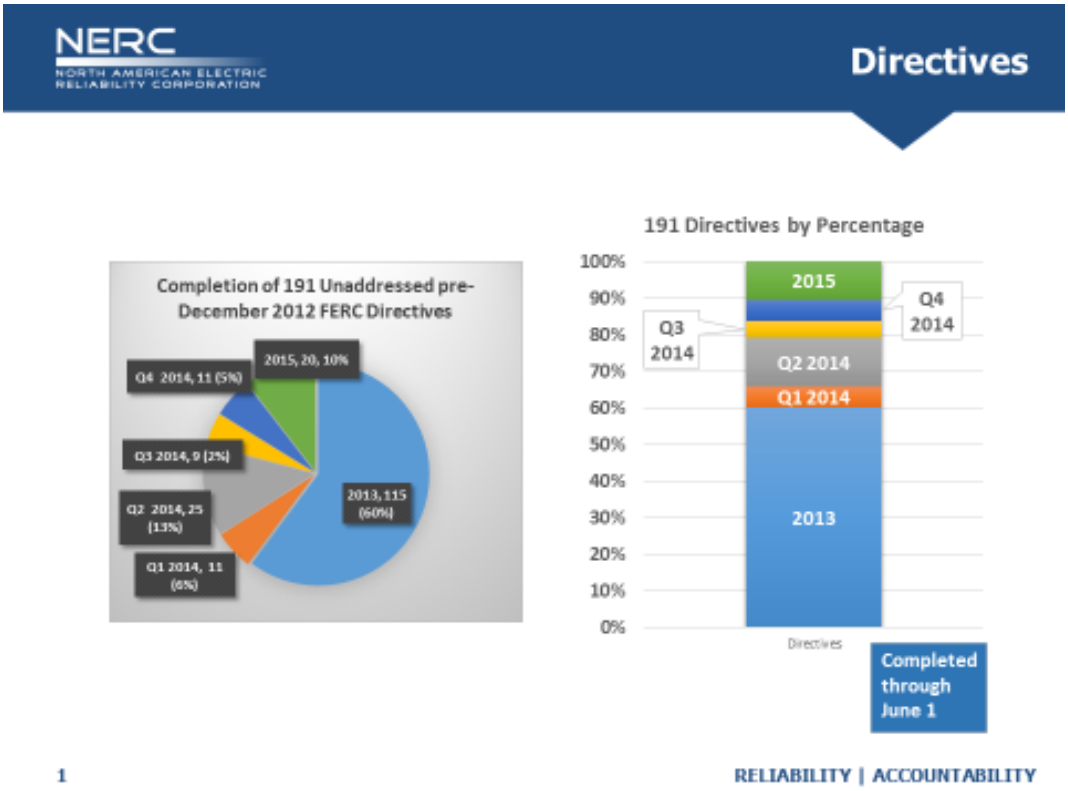
1. Completing Commission Directives

During this assessment period, NERC made significant progress in reducing the number of Commission directives involving Reliability Standards. Addressing these directives is a priority to facilitate the transformation to steady-state.[22] The status of NERC's efforts in addressing Reliability Standards-related directives is reported on a quarterly basis to the NERC Standards Oversight and Technology Committee (SOTC). At the February 2014 SOTC meeting, NERC reported that 128 directives had been addressed by year-end 2013, with 107 directives remaining to be addressed. NERC continues to report the status of completion at every SOTC meeting and anticipates that 90% of FERC directives issued to date will be resolved during the first half of 2015.

[21] The 2014-2016 RSDP identified 18 Reliability Standard development projects completed in 2013 or scheduled to be completed by the first quarter of 2014. It also identified 13 projects that were to be completed thereafter.

On June 20, 2014, the draft 2015-2017 RSDP was posted for industry comment. Currently, it identifies 27 projects that have been completed or are in progress, many of which were newly introduced in 2014. Eight of these 27 projects have been approved by the Registered Ballot Body, approved by the NERC Board, and filed with FERC for approval, and 12 are anticipated to be completed in 2014. The draft 2015-2017 RSDP identifies the remaining seven projects that will extend into 2015, with completion anticipated in the first half of the year. Additionally, four new projects for 2015 are identified. Completion of these projects will position NERC to begin enhanced periodic reviews in late 2015.

[22] Directives may be addressed by: (i) completing the directive as assigned; (ii) addressing the reliability concern of the directive in an equally effective and efficient manner; or (iii) providing persuasive reasoning as to why the directive is no longer necessary.



FERC has been instrumental in reducing the number of outstanding directives, as well. On November 21, 2013, in its order addressing the Paragraph 81 project, the Commission withdrew 41 directives, 24 of which were related to Reliability Standards, effective January 21, 2014.[23] The Commission identified Reliability Standards-related directives for withdrawal based on the following three guidelines:

(1) Whether the reliability concern underlying the outstanding directive has been addressed in some manner, rendering the directive stale;

(2) Whether the outstanding directive provides general guidance for Reliability Standards development rather than a specific directive; and

(3) Whether the outstanding directive is redundant with another directive.

[23] *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, 145 FERC ¶ 61,147 (2013).

FERC staff participation on standard drafting teams has also been instrumental in addressing Reliability Standards directives. Increased participation by FERC staff allows their concerns to be raised early in the Reliability Standard development process and for issues to be vetted with industry. This open dialogue translates into fewer directives in FERC orders.

2. The Standards Independent Experts Review Panel

To set the foundation for a steady-state body of Reliability Standards, NERC established the IERP to evaluate the existing families of Reliability Standards and requirements. The Panel consisted of five independent industry experts and a sixth participant from FERC staff. Their areas of experience and competence included power systems engineering, relaying, transmission system planning, transmission and power system operations (including control center operations and dispatching, generation operations, transmission operations, and maintenance). The independent consultants brought executive leadership, experience from all three U.S. interconnections, experience with investor-owned utilities and public power as well as with vertically integrated and regional transmission organizations/independent system operator (RTO/ISO) market environments and small entities. The Panel also had experience working with Canadian provinces and Mexico. The Commission participant offered thorough knowledge of previous FERC orders and an understanding of the contributions of the requirements of various Reliability Standards to BPS reliability.

Due to the ongoing evolution of NERC's Reliability Standards, the Panel addressed requirements from two groups of Reliability Standards: (i) Reliability Standards that were, or would become, enforceable in 2013 (Enforceable in 2013 Standards); and (ii) Reliability Standards that will be enforceable in the future (Future Enforceable Standards). The Future Enforceable Standards and requirements included both Enforceable in 2013 Reliability Standards and those that, at the time of the Panel's report, had been approved by the NERC Board or by the

FERC and were currently pending enforceability.[24] Requirements pending replacement by approved Reliability Standards were not included in this group.

The Panel issued its report in June 2013 and presented the report to the NERC Board in August 2013. In the report, the Panel outlined a vision for how to transform the NERC Reliability Standards to steady-state. The Panel made seven short-term recommendations, three longer-term recommendations and seven additional recommendations.[25] The Panel's main recommendation was to retire 147 existing requirements of Reliability Standards, address seven areas (high-level gaps) not currently addressed by the Reliability Standards, and complete Reliability Standards development projects to address gaps within individual requirements. The Panel also made recommendations regarding compliance monitoring, prioritization for addressing the identified gaps, using risk to determine whether a future Reliability Standard is needed, and use of the Panel's identified criteria to determine quality and content as future Reliability Standards are developed. Finally, the Panel recommended a new construct to further consolidate Reliability Standards and required actions.

In evaluating whether a requirement should be retired, the Panel assessed whether each requirement: (i) did not support a reliability principle; (ii) met the Paragraph 81 criteria for retirement; or (iii) was better suited as a guideline rather than as a part of a Reliability Standard. For the requirements that the Panel did not recommend for retirement, the Panel applied content and quality criteria to examine whether they were steady-state or needed additional work. Specifically, the Panel examined the following content criteria: (i) whether the content of the

[24] The June 2013 report, *Standards Independent Experts Review Project – An Independent Review by Industry Experts*, is available at: http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Standards_Independent_Experts_Review_Project_Report.pdf.

[25] *Id*., p. 16-17.

requirement is technically correct, including identifying who does what and when; (ii) whether the requirement identifies the correct functional entities; and (iii) whether there are appropriate actions for which there should be accountability included or there is a gap. Additionally, the Panel examined the following quality criteria:

(1) Whether the requirement should stand alone or be consolidated with other Reliability Standards;

(2) Whether the requirement was drafted as a results-based standard;

(3) Whether a requirement is technologically neutral;

(4) Whether the requirement aligns with the purpose of the Reliability Standard;

(5) Whether the requirement is a higher solution than the lowest common denominator;

(6) Whether the requirement is measureable;

(7) Whether the requirement has a technical basis in engineering and operations;

(8) Whether the requirement is complete and self-contained;

(9) Whether the language is clear and does not contain ambiguous or outdated terms;

(10) Whether the requirement can be practically implemented; and

(11) Whether the requirement uses consistent terminology.

The Panel evaluated whether these remaining requirements addressed a risk to reliability by examining: (i) the ranking developed by the NERC RISC; (ii) the violation risk factor (VRF) for each requirement; and (iii) the Panel members' professional judgment.

These recommendations have been pivotal in NERC's evaluations of the Reliability Standards by standard drafting team subject matter experts (SME). Furthermore, the Panel's recommendations have been used to inform standard drafting teams and NERC's annual RSDPs, including the current, 2014-2016 RSDP. The potential reliability gaps identified by the IERP have been evaluated by the RISC and are assigned in some cases to active drafting projects. The

IERP recommendations that apply to Reliability Standards that are not part of active drafting projects are assigned to teams that conduct periodic reviews of Reliability Standards in the future for consideration.[26]

3. Implementation of the Paragraph 81 Project

The Paragraph 81 project was a separate project, carried out during the assessment period, in which requirements were recommended for retirement. This project stemmed from paragraph 81 of the Commission's March 15, 2012 FFT Order, in which the Commission invited NERC (and other interested entities) to propose specific Reliability Standards or requirements for revision or retirement if they did not provide meaningful benefit to BPS reliability. In response, NERC began the Paragraph 81 project to identify and retire Reliability Standards requirements that have little or no effect on reliability. As discussed above, the project established a set of criteria for evaluating whether a requirement should be considered for retirement.[27]

This initiative is reducing and simplifying the set of Reliability Standards with which registered entities must comply and which the ERO must monitor and enforce. This reduction in the body of requirements enables both the ERO and registered entities to redirect resources to matters posing greater risks to the reliability of the BPS and to ensure that the costs of reliability are proportionate to the benefits.

[26] These future periodic reviews are required by §13 of the SPM.

[27] For a detailed discussion of criteria used to determine if a Reliability Standard requirement should be retired, *see Paragraph 81 Project Technical White Paper* (December 20, 2012), available at: http://www.nerc.com/pa/Stand/Project%20201302%20Paragraph%2081%20RF/P81_Phase_I_technical_white_paper_FINAL.pdf.

In February 2013, NERC filed a petition with FERC to retire 34 requirements or sub-requirements within 19 Reliability Standards.[28] In its June 20, 2013 notice of proposed rulemaking (NOPR), the Commission indicated agreement that the requirements proposed for retirement either: (i) provided little protection for BPS reliability; or (ii) were redundant with other aspects of Reliability Standards. In addition, in the NOPR, the Commission proposed to withdraw several outstanding Commission directives relating to Reliability Standards.[29] On November 21, 2013, the Commission issued an order approving, as proposed in the NOPR, the retirement of 34 requirements and sub-requirements within 19 Reliability Standards, and withdrawing the identified directives effective January 21, 2014 (the Retirement Effective Date).[30] As noted above, the retirement of these requirements is enabling both the ERO and registered entities to redirect resources to matters posing greater risks to the reliability of the BPS and to ensure that the costs of reliability are proportionate to the benefits.

In the period leading up to the Retirement Effective Date, Regional Entities did not actively monitor compliance with the 34 retired requirements, nor did they process any new or existing possible violations of these retired requirements. Regional Entities also documented removal of any of the 34 retired requirements from Compliance Audit scopes in the final Compliance Audit reports for those audits. Within 30 days of the Retirement Effective Date, Regional Entities dismissed existing possible violations of the requirements being retired and issued dismissal letters to the registered entities.

[28] *Petition of the North American Electric Reliability Corporation for Approval of Retirement of Requirements in Reliability Standards*, Docket No. RM13-8-000 (Feb. 28, 2013).

[29] *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, Notice of Proposed Rulemaking, 143 FERC ¶ 61,251 (2013).

[30] *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, 145 FERC ¶ 61,147 (2013).

In addition to the 34 requirements that the Commission approved for retirement, stakeholders submitted an additional 217 requirements for consideration for retirement. NERC is examining whether to retire these requirements through individual Reliability Standards development projects. Progress on this retirement effort is reported to the SOTC on a quarterly basis. As of the February 2014 SOTC meeting, 179 out of 281 recommendations had been addressed, 79 were under consideration in either a current project or in a periodic review, and 23 had not yet been assigned to a project.

4. Development of Compliance Assessment Tools Concurrently with Reliability Standards Development

Over time, one of the key improvement opportunities identified for NERC Reliability Standards has been to strengthen the connection between standard drafting teams and the compliance program, in order to clarify the expectations of Reliability Standard requirements. Two efforts at clarifying Reliability Standard requirements, but which ultimately illustrated the need for greater involvement of the Compliance department in the Reliability Standards development process, were the Compliance Application Notice (CAN) initiative and the Reliability Standard Audit Worksheets (RSAWs). CANs were notices drafted to respond to questions regarding how to assess compliance with specific Reliability Standards. CANs were posted on the NERC website to provide transparency to industry; however, since they were drafted well after the Reliability Standard was developed, the compliance assessment positions articulated in the CANs often varied from industry's perspective of the intent of the Reliability Standard or requirement. Similarly, prior to 2013, NERC developed RSAWs after regulatory approval of a Reliability Standard.

The CAN process demonstrated the need for concurrent development and dialogue between standard drafting teams and NERC Compliance Operations staff. As a result, in 2013,

NERC began incorporating the development of compliance assessment information into the Reliability Standards development process. After June 2013, informal development project teams began posting documents during standards development titled "compliance input." These documents provided questions from industry and answers developed by Compliance staff regarding how to assess compliance for specific requirements, or phrases in the requirements. This basic tool opened the door for conversation between the standard drafting teams and Compliance staff. It also allowed for conversation regarding the wording of requirements and the effect of that wording on how compliance would be assessed.

NERC then created an inter-departmental team to examine the development of RSAWs, which resulted in an internal policy on the development of RSAWs concurrent with Reliability Standards development projects. The policy included the following provisions:

(1) Coordinating input between standard drafting teams and NERC Compliance staff;

(2) Posting a draft RSAW during the formal comment period and prior to the ballot period for a Reliability Standard, allowing stakeholders to provide comments or to raise concerns at that time;[31] and

(3) Continuing to involve Regional Entity Compliance staffs in drafting RSAWs to strengthen compliance consensus throughout the ERO and capture additional subject matter expertise.

Today, RSAWs are written concurrently with new Reliability Standard development projects. They provide information regarding compliance assessment and testing. Reliability Standards staff leads coordination between the Standards and Compliance departments. Each Reliability Standards project is assigned dedicated staff support led by Compliance staff. Additionally, NERC Compliance staff are coordinating with Regional Entity Compliance staffs. This increased and ongoing coordination will help ensure that standard drafting teams, NERC

[31] The RSAWs themselves are not subject to the ballot.

and Regional Entity Compliance staffs and RSAWs are aligned as to the intent of Reliability Standards. By creating a uniform understanding of compliance expectations for each Reliability Standard early in the development process, the need for interpretations or other forms of subsequent compliance guidance should be reduced.

NERC Compliance staff will continue to supply standard drafting teams with compliance and enforcement information, statistics, and perspectives to help develop Reliability Standards that provide an increased reliability benefit and clarify compliance risks. Compliance staff will continue collaborating with industry and Reliability Standards staff early in the Reliability Standards development process in order to understand the intent of Reliability Standards under development and provide feedback on the proposed language of Reliability Standards. Finally, as described in greater detail in §II.C.2 and 4 below, NERC is working to provide training to auditors and industry on how to assess compliance with a new or revised Reliability Standard. This training is provided following FERC approval of a Reliability Standard, but well before its effective date.

5. Review of Regional Reliability Standards

A Regional Entity can propose adoption of a regional Reliability Standard to implement requirements that are more stringent than the continent-wide requirement, and/or to address a reliability concern that is unique to that Regional Entity and not addressed in a continent-wide Reliability Standard.[32] Today, a regional Reliability Standard requirement may be developed as a separate regional Reliability Standard or as an addendum to a continent-wide Reliability Standard. NERC is considering, based on the recommendations from the Panel, commissioning a team to evaluate regional Reliability Standards to identify candidates for retirement,

[32] **Attachment 3**, NERC Assessment of the Regional Entities' Delegated Functions, contains a discussion of each Regional Entity's regional Reliability Standards development activity during the assessment period.

consolidation with continent-wide Reliability Standards, or incorporation as variances within continent-wide Reliability Standards. The regional Reliability Standards that are not identified as candidates for retirement or consolidation should align with continent-wide Reliability Standards.

6. Improvements in the Reliability Standards Development Process

Transforming NERC Reliability Standards to a steady-state required changes to how NERC identified and resolved issues through the Reliability Standards development process. Implementing these changes was possible due to strong participation from industry stakeholders, the NERC SC and other NERC committees and workgroups, specifically the RISC, the SPIG, and the NERC technical committees, as well as FERC staff. The NERC Board and the NERC MRC also provided strong support to implement the changes.

a. Revisions to the *Standard Processes Manual* and Related Improvements

NERC's Reliability Standards development process is defined in the SPM, Appendix 3A to the NERC ROP. The SPM governs all NERC activities related to the development, approval, revision, reaffirmation, and withdrawal of Reliability Standards, interpretations, VRFs, violation severity levels (VSLs), definitions, variances, and reference documents developed to support Reliability Standards. It also addresses the respective roles of the NERC SC, standard drafting teams, and Registered Ballot Body members in the stakeholder process. Upon FERC's approval of revisions to the SPM in June 2013, NERC, the NERC SC, and stakeholders began implementing the approved changes into the Reliability Standards development process.

The revisions to the SPM were initiated in February 2012, when the NERC Board, in consultation with the NERC MRC, formed the SPIG.[33] The NERC Board tasked the SPIG with achieving the following objectives: (i) provide clarity on the reliability objectives, technical parameters, scope and relative priority of Reliability Standards; (ii) review the Reliability Standard drafting process to ensure that Reliability Standards contain specific technical content; and (iii) assess Reliability Standards project management.

After gathering input from stakeholders, the SPIG made five recommendations to modify the way NERC develops Reliability Standards.[34] Based on these recommendations, NERC worked with stakeholders to develop revisions to the SPM. In these revisions, NERC:

(1) Revised the composition of standard drafting teams to ensure that they are appropriately equipped to meet reliability objectives, namely by adding legal and compliance experts;

(2) Incorporated references to compliance assessment tool development, such as RSAWs, cooperatively and in parallel with Reliability Standard drafting;

(3) Streamlined commenting and balloting provisions as follows:

  (a) Allowing summary responses to comments;

  (b) Eliminating the obligation to respond in writing at every stage of the comment process; and

  (c) Eliminating negative votes without comments in the calculation of consensus.

(4) Incorporated the following provisions:

  (a) Quality review conducted in parallel with Reliability Standards development;

  (b) Guidance for the appropriate role and scope of interpretations, to be consistent with guidance from the NERC Board; and

[33] The SPIG is composed of the MRC chair and vice chair, other MRC members, two members of the NERC Board, the NERC chief executive officer (CEO), and the NERC SC chair.

[34] The SPIG's *Recommendations to Improve the NERC Standards Development Process* report is available on the NERC website at: http://www.nerc.com/pa/Stand/Standards%20Processes%20Manual%20revisions%20SPIG%20Recommen/Standards_Process_Input_Group_04.24.12_ver_8_FINAL.pdf.

(c) A waiver provision to allow for modifications to the Reliability Standards development process for good cause, with five days' notice and reporting of the exercise of a waiver to the NERC SOTC.

(5) Reduced the requirement for periodic reviews to be consistent with ANSI minimum requirements.

These improvements provide a balanced flexibility to the process, enabling NERC and industry to address pressing reliability issues on accelerated timeframes if necessary. Further, with the changes, the Reliability Standards development process continues to meet ANSI requirements. The Commission approved the proposed revisions on June 26, 2013, agreeing that these changes enable greater flexibility and efficiency.[35] Reliability Standards development projects initiated and completed after FERC's approval of the SPM changes have shown both significant increases in efficiency and improvements in the quality of the product.

In addition to the revisions to the SPM, NERC has implemented additional enhancements to the Reliability Standards development process. In conjunction with implementing changes to the SPM, in 2013, NERC spearheaded an "informal development" effort, which uses informal groups composed of industry subject matter experts to conduct early outreach to industry stakeholders prior to initiating formal development of new or revised Reliability Standards. This early outreach encourages stakeholder conversations to obtain inputs on the proposed Reliability Standards development project. This approach is positively affecting how standard drafting teams are conducting their work. The periodic reviews conducted in 2013 followed this same approach, acting as a tool for gathering stakeholder input. Recommendations from each periodic review team are then implemented through subsequently-formed standard drafting teams.

The most significant improvement from the changes to the Reliability Standards development process has been in the amount of time required to develop a quality Reliability

[35] *Order Approving Revisions to Electric Reliability Organization's Standard Processes Manual*, 143 FERC ¶ 61,273 (2013), at P 18.

Standard. As reported in the *Analysis of NERC Standards Process Results, Fourth Quarter 2013* filing,[36] the baselines for the amounts of time to revise an existing Reliability Standard and to develop a new Reliability Standard were approximately 27 months and 40 months, respectively. The amount of time to produce each of the Reliability Standard development projects that began formal development under the revised SPM was dramatically reduced.[37] Approximately six projects completed formal development, from posting the standard authorization request to being adopted by the NERC Board, in less than seven months.[38] Two other projects completed formal development in ten months.[39]

The changes to the standard development process have provided benefits in terms of standard drafting team management and staffing. The reduced time needed to develop a Reliability Standard combined with the fact that standard drafting team meetings are held closer together in time provide registered entities and other participants with increased flexibility in staffing standard drafting teams. As a result, standard drafting team members are able to stay more focused on the Reliability Standard development project.

The speed and efficiency of the process, particularly at the standard drafting team stage, have also benefited from the following process improvements:

- Smaller standard drafting teams with appropriate expertise have increased the ability to conduct activities and respond to stakeholders in a more-timely and effective manner;

---

[36] Available at: http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Analysis_of_NERC_Standards_Process_Results_Q4_FINAL.pdf.

[37] The projects were: (i) 2010-01 – Training (PER); (ii) 2010-03 – Modeling Data (MOD B); (iii) 2010-04 – Demand Data (MOD C); (iv) 2012-05 – ATC Revisions (MOD A); and (v) 2013-04 – Voltage and Reactive Control (VAR).

[38] The six projects were: (i) GMD Phase 1; (ii) INT; (iii) Physical Security (CIP-014); (iv) MOD A; (v) MOD B; and (vi) PER projects; one of the two Reliability Standards in the VAR project (VAR-001) also met this benchmark.

[39] The two other projects were: (i) the remaining Reliability Standard in the VAR project (VAR-002); and (ii) the MOD C project.

- Open communication and concurrent development of compliance assessment tools have addressed compliance questions and allowed for clarification of compliance intentions during Reliability Standards development;

- Summary responses to comments has allowed standard drafting teams to consider stakeholder inputs, modify the draft Reliability Standard in response to those inputs, and repost it for industry review more quickly (as short as 1.5 weeks); summary responses are more concise while still addressing the issues, and provide visibility into the concerns in an easily digestible format;

- Not considering negative votes without comments in the calculation of consensus encourages entities to provide constructive comments, providing better insight into the issues for the standard drafting teams;

- Coordinating quality review in parallel with standard development has eliminated an additional step (that previously could require 4 to 6 weeks) from the process and improved focus on quality at an earlier stage; and

- Granting the NERC SC authority to waive provisions in the SPM for good cause gives the SC the ability to respond to urgent reliability issues. A recent example, discussed in §II.A.8.e below, is the development of Reliability Standard CIP-014-1 – Physical Security, in less than 90 days.

Another improvement resulting from the SPM revisions, which is also associated with increased outreach and communication, is the partnership created between NERC staff, standard drafting teams, and the NERC SC. Additionally, FERC staff has been providing early input regarding their perspectives during the standards development process, thereby giving standard drafting teams the opportunity to weigh those inputs early in the process. Based on experience to date, NERC anticipates that this open dialogue will result in FERC orders with either no directives or a significantly reduced number of directives.

The NERC SC, under the NERC Board's direction, also developed a strategic plan and work plan, as well as a revised charter, all of which were approved by the NERC Board on February 6, 2014.[40] These actions were designed to increase the NERC SC's effectiveness, efficiency, and ability to deliver high quality Reliability Standards. The *Standards Committee*

[40] The *Standards Committee Strategic Work Plan 2014-2016*, *Standards Committee Strategic Plan*, and amended *Standards Committee Charter* are available at: http://www.nerc.com/comm/SC/Pages/default.aspx.

Strategic Plan is a five-year plan that sets the vision and mission for the NERC SC, describes the guiding principles for the NERC SC, and sets the foundation for refocusing the activities of the NERC SC. The *Standards Committee Strategic Work Plan* is the tactical implementation of the *Standards Committee Strategic Plan*. The revised *Standards Committee Charter* clarifies the NERC SC's role in the development of steady-state Reliability Standards that provide for the reliability of the BPS, and ensures that the NERC SC develops a multi-year strategic vision that describes the goals and direction for the development of Reliability Standards consistent with the strategic and business plans of NERC.

Additionally, the NERC SC created a new subcommittee, the Process Management and Oversight Subcommittee (PMOS), that acts as an industry and standard drafting team partner. This subcommittee assigns a representative to each standard drafting team for the purpose of oversight. The oversight includes such actions as assisting the standard drafting team in understanding any stakeholder concerns, reaching out to stakeholders if they do not understand the actions being taken by the standard drafting team, being partners in reviewing the Reliability Standards for quality, and assisting with advice on a range of topics from direction to posting schedules. The PMOS has assisted standard drafting teams in avoiding or overcoming hurdles during the process.

The revisions made to the SPM and other changes made to the Reliability Standards development process, including strengthened partnerships among standard drafting teams, the NERC SC, and NERC staff, are showing great promise as improvements to the process, in terms of improving efficiency, speed and quality. These improvements have allowed the ERO to make significant progress towards achieving a body of steady-state Reliability Standards. The 2015-2107 RSDP will reflect that most, if not all, FERC directives and recommendations for

retirement (both from the Paragraph 81 project and the IERP review) will be addressed in 2015, and it will provide an opportunity for a strategic review of the Reliability Standards.

b. Formation and Work of the Reliability Issues Steering Committee

In response to the SPIG's recommendations, the NERC Board formed the NERC RISC in August 2012 to establish a collaborative effort at the industry leadership level to set priorities on issues of importance to the BPS. The RISC is composed of industry executives and thought leaders, including representatives from the NERC Operating, Planning, Standards, Critical Infrastructure Protection, and Compliance and Certification Committees. The RISC is an advisory committee that reports directly to the NERC Board, focusing on triaging and providing front-end, high-level leadership and accountability for issues of strategic importance to BPS reliability. The RISC assists the NERC Board, NERC technical committees, NERC staff, regulators, Regional Entities, and industry stakeholders in establishing a common understanding of the scope, priority, and goals for the development of solutions to address these issues. In doing so, the RISC provides a framework for steering, developing, formalizing, and organizing recommendations to help NERC and the industry effectively focus their resources on the critical means to improve the reliability of the BPS. In some cases, that includes recommending reliability solutions other than the development of new or revised Reliability Standards and offering high-level stakeholder leadership engagement and input on issues that enter the Reliability Standards process. In other cases, the development of a new Reliability Standard or modification of an existing Reliability Standard may be the best way to address a particular issue.

The NERC SC works closely with the RISC and the NERC technical committees, creating an alignment of focus on specific issues. The chairs of the technical committees and NERC SC are members of the RISC, which strengthens the needed coordination.

The RISC is developing a triage process to address other reliability issues that are brought to the NERC SC, whether through a standards authorization request or another mechanism. This process will include a review by the RISC to determine whether the issue is a risk to the reliability of the BPS and, if so, the priority of investing ERO and stakeholder resources to resolve the issue. This review will aid in focusing resources on the resolution of the most important issues.

The RISC also provides input into prioritizing Reliability Standards development activities by providing input to the RSDP in two ways: first, by considering whether the projects identified in the RSDP address areas of risk for the BPS; and second, by developing a priority rank for each of the projects.

In considering whether each of the projects addresses an area of risk for the BPS, the NERC RISC considers whether there are outstanding FERC directives or any recommendations for retirement, either from the Paragraph 81 project or the IERP, that could be addressed by the project.

In reviewing the priority of each project, the RISC provides a mechanism for addressing any scheduling conflicts between projects through the development process.[41] In its initial analysis, the RISC identified four high-priority focus areas for Reliability Standards: (i) cyber attacks; (ii) workforce capability and human error; (iii) protection systems; and (iv) monitoring and situational awareness. The RISC presented these priorities to the NERC Board in February 2013. In response, the NERC Board directed the RISC to conduct further analysis of the issues identified as high and medium priority. The NERC Board also directed that the RISC's input be integrated into the overall ERO planning process. NERC staff is implementing process steps to

[41] RISC reviewed and provided input on the use of RISC's rankings in project prioritization.

meet this objective. Subsequently, the RISC issued an updated report in August 2013 identifying a fifth area of focus: adaptation and planning for change.[42]

In addition to the activities described above, in November 2012, the RISC participated in a NERC-sponsored conference in which reliability topics were discussed with technical experts. The conference, conducted as a series of panel discussions, highlighted several existing and emerging reliability risks and created an opportunity for informed dialogue about technical topics. A second conference, the Reliability Leadership Summit, was held in October 2013, with key industry decision-makers gathering to discuss reliability priorities and industry trends.[43]

Efforts to review the risk areas identified by the RISC and to develop appropriate risk management strategies are ongoing. Integrating these priorities into the annual business plan and budget process will be a cornerstone of NERC's annual planning process going forward. To effect this change in planning, NERC has developed the Reliability Risk Management (RRM) process, a multi-year strategy development method that uses industry expertise through the RISC and other standing committees to develop actionable, measureable efforts to manage reliability risk. The RRM process is discussed in detail below in §II.D.1.

c. Realignment of Resources in the Reliability Standards Program

NERC is constantly assessing the alignment of resources to be responsive to the changes necessary to move the NERC Reliability Standards to a steady-state. In 2013, NERC realigned resources in its Reliability Standards department by creating multiple small teams of Reliability Standards developers and one team focused on information management. This realignment focused resources on the production of Reliability Standards rather than on executing and

[42] *ERO Priorities – RISC Updates and Recommendations* is available at: http://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_Priority_Recommendations-Jul_26_2013.pdf.

[43] NERC intends for this summit meeting to be an annual event; the next Reliability Leadership Summit is scheduled for September 2014.

monitoring the development process, thereby increasing the throughput to complete outstanding projects and resolve outstanding directives. In 2013, each of the three "developer" teams was assigned one of the following high-level goals:

(1) Resolving directives;

(2) Conducting the required five-year reviews for current Reliability Standards;[44] or

(3) Overseeing emerging issue projects and the completion of remaining open projects.

The small developer teams closely coordinate with one another to ensure a balance in workload and to create an expertise in each of the major work areas.

Additionally, NERC has improved the composition of standard drafting teams by enhancing the selection process to identify, for each project, the necessary technical, writing, and project management expertise to form a balanced team that will foster improved effectiveness and enhanced efficiency. Standard drafting teams also now receive increased NERC staff support, including dedicated legal support, for each project. Each standard development project is staffed by a lead standard developer, and many projects have a second supporting standard developer. Standard developers provide project management and facilitation experience as well as additional skills, including technical writing, legal skills, and outreach/consensus-building skills, to the standard drafting team, which contributes to the development of high-quality Reliability Standards. With this enhanced staffing, standard drafting teams are better able to reach milestones and build consensus among industry stakeholders in advance of balloting. Further, NERC now provides facilitation training to all newly appointed standard drafting team leaders. Finally, NERC has developed a Standards Development Process Participant Conduct

[44] Section 13.0 of the revised SPM now requires periodic reviews every five years for those Reliability Standards that have been adopted by ANSI as an American national standard, and every ten years for all other Reliability Standards.

Policy to ensure that the Reliability Standards development process is conducted in a professional and constructive environment.

d. Developing and Implementing Procedures for the Cost-Effective Analysis Process

NERC has developed the Cost-Effective Analysis Process (CEAP) in response to requests by registered entities and regulators to incorporate consideration of costs more directly into Reliability Standard development activity.[45] The CEAP affords stakeholders an opportunity to share projected cost information regarding implementation of draft Reliability Standards and provides the opportunity to offer alternatives that would be equally, or more, efficient at achieving the reliability objective of the draft Reliability Standard while also taking into consideration implementation costs. CEAP has been used for a limited number of new and revised Reliability Standards projects, with limited success. NERC continues to explore options for improving both the process and the quality of the resulting information.

The current CEAP process provides for a two-phase process for identifying projected implementation costs. The first phase of the CEAP, identified as the Cost Impact Analysis, is conducted during the standard authorization request stage of Reliability Standard development. It provides an opportunity to identify approximate implementation costs associated with a proposed Reliability Standard prior to its development. Information related to the mission and forecasted implementation costs of the proposed Reliability Standard is collected from the industry during the initial standard authorization request comment period. The information collected is shared with the NERC SC and the standard drafting team, and is posted on the NERC website.

[45] This was an issue raised in response to the five-year performance assessment survey.

The second phase of the CEAP, identified as the cost effective analysis, typically comes after the draft Reliability Standard is developed by the standard drafting team and is ready for the first combined formal comment period and ballot. During this phase, NERC again solicits industry to provide forecasted implementation costs of the proposed requirements and to propose alternative methods to achieve the proposed Reliability Standard's reliability objective more efficiently. Any alternative proposals provided by industry during this phase should contain sufficient technical justification, and if possible, cost comparison data for consideration.

7. Improved Stakeholder Access to Reliability Standards Information

All Reliability Standards are available to stakeholders through NERC's public website, including: (i) Reliability Standards that are currently enforceable in specific jurisdictions (i.e., in the U.S. and Canadian provinces); (ii) Reliability Standards pending regulatory approval; (iii) Reliability Standards approved by the NERC Board and pending regulatory filing; and (iv) Reliability Standards no longer subject to enforcement. In 2012, NERC launched an improved interface to allow stakeholders to filter the complete set of Reliability Standards so that they could identify which Reliability Standards are applicable to their respective registered functions. Work is ongoing to improve the completeness and timeliness of this information for non-U.S. jurisdictions (i.e., Canadian provinces or Mexico).

Additionally, beginning in 2013, interested entities can track current Reliability Standards development projects in a publicly posted spreadsheet, the *Project Tracking Spreadsheet*.[46] NERC updates this spreadsheet monthly. The spreadsheet also provides a link to the projects page, the deliverables, the number of Paragraph 81 requirements, the number of regulatory directives or guidance, the PMOS liaison assigned to the project, the NERC standards developer,

[46] NERC regularly updates the *Project Tracking Spreadsheet: 2014 Project Work Plan* and the link to the file is located on the left side of NERC's Standards webpage available at: http://www.nerc.com/pa/Stand/Pages/Default.aspx.

and a month-by-month timeline. Also in 2013, NERC began posting the *Projected Standards Posting Schedule*, which provides the industry with an outlook of near term postings.

8. Specific Reliability Standards Projects

a. Critical Infrastructure Protection Version 5 Reliability Standards

On November 22, 2013, the Commission issued Order No. 791 approving the Critical Infrastructure Protection Version 5 (CIP Version 5) Reliability Standards.[47] The CIP Version 5 Reliability Standards provide a cybersecurity framework for the categorization and protection of BES cyber systems to support the reliable operation of the grid. NERC worked with industry to ensure that the CIP Version 5 Reliability Standards address the differing roles of each registered entity in the operation of the BES, the criticality and vulnerability of the BES cyber systems needed to support BES reliability, and the risks to which the BES cyber systems are exposed. In Order No. 791, the Commission found that CIP Version 5 is an improvement over the currently approved CIP Reliability Standards. The Commission also determined that categorizing BES cyber systems based on their impact on the reliable operation of the BES (Low, Medium, or High), with all BES cyber systems categorized as at least Low Impact, offers more comprehensive protection of the BES.[48] The Commission directed NERC to address several new directives, some of which must be addressed within a year. To meet these directives, NERC has established a standard drafting team and set an aggressive schedule to address all the Commission's concerns, consistent with the timeline set by the Commission.

In Order No. 791, the Commission also approved NERC's proposal to bypass CIP Version 4 and move directly to implement CIP Version 5. Recognizing that registered entities

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

[48] In Order No. 791, the Commission directed NERC to develop modifications to address specified concerns with the CIP Version 5 standards, including: (i) the "identify, assess, and correct" language; (ii) protections for Low Impact BES Cyber Systems; (iii) the risks posed by transient devices; and (iv) the protection of communication networks.

are in various stages of implementation of CIP Versions 3 and 4, NERC tackled the need for flexibility as well as the need to identify and address the associated transition challenges for industry. In October 2013, NERC launched the CIP Version 5 Transition Implementation Study (CIP Version 5 Study) to collect and to evaluate relevant data from select responsible entities regarding their experience in implementing CIP Version 5 requirements. Through this study, NERC is identifying successful implementation methods and challenges that the industry faces in transitioning to CIP Version 5. On October 11, 2013, NERC submitted an informational filing to the Commission that described how the CIP Version 5 Study would assist responsible entities in making the transition to CIP Version 5.[49] As part of the CIP Version 5 Study, NERC selected a group of six responsible entities, based on factors including willingness to participate, past performance under the CIP Reliability Standards, and expected relevance to the CIP Version 5 Study's goals. NERC is sharing the experience and information obtained through the CIP Version 5 Study with industry throughout the study period. NERC will also prepare a final report that synthesizes the study participants' experiences in applying CIP Version 5. The report will focus on the effectiveness of meeting the CIP Version 5 requirements and the methods employed during implementation. The report will also focus on the following:

(1) Methods, approaches, and policies that were effective in implementing the technical controls of CIP Version 5;

(2) Tools, policies, and training that were effective in aligning employees' skills and cooperation with the responsible entity's mission and the CIP Version 5 Reliability Standards;

(3) Hurdles encountered by the participating responsible entities and the relevant outcomes; and

(4) Requirements and concepts of CIP Version 5 that the responsible entities had difficulty implementing and why.

[49] *Informational Filing of the North American Electric Reliability Corporation Regarding the CIP Version 5 Reliability Standards Implementation Study*, Docket No. RM13-5-000 (Oct. 11, 2013).

b. Transmission Vegetation Management

During the assessment period, the Commission approved two new versions of the FAC-003 Reliability Standard. In Order No. 777,[50] the Commission approved NERC's proposed FAC-003-2, a Reliability Standard that requires responsible entities to minimize encroachments from vegetation located adjacent to transmission rights-of-way and within a transmission owner's control. Historically, vegetation-related outages have been a recurring contributor to blackouts. In fact, inadequate vegetation management practices causing tree contact was one of the initiating causes of the 2003 Northeast blackout. Industry compliance with FAC-003-2, together with a continued industry focus on best practices for vegetation management, enhances the reliability of the BPS.

FAC-003-2 is the first results-based Reliability Standard approved by the Commission, and contains several improvements over FAC-003-1. For example, while FAC-003-2 continues to apply to overhead transmission lines operated at or above 200 kV, it additionally applies to any lower voltage overhead transmission line that is either an element of an interconnection reliability operating limit or a major WECC transfer path. Another improvement is that FAC-003-2 makes explicit a transmission owner's obligation to prevent an encroachment into the minimum vegetation clearance distance for a line subject to this standard, regardless of whether that encroachment results in a sustained outage or fault. FAC-003-2 also requires transmission owners, for the first time, to annually inspect all transmission lines subject to the Reliability Standard and complete 100 percent of their annual vegetation management work plan.

[50] *Revisions to Reliability Standard for Transmission Vegetation Management*, Order No. 777, 142 FERC ¶ 61,208 (2013) (Order No. 777).

On September 19, 2013, the Commission approved FAC-003-3,[51] which extends FAC-003-2 vegetation management requirements to certain generator interconnection facilities to address a reliability gap that existed when the requirements only applied to transmission owners. Certain generator owners with overhead lines, particularly those with generator interconnection facilities longer than one mile and which run through areas that may be densely populated with trees and other plants, are now also required to perform vegetation management of those lines. For purposes of this Reliability Standard, these lines are treated as transmission lines.

NERC is conducting additional research relating to vegetation management issues in response to Commission directives in Order No. 777. The Commission directed NERC to conduct or contract testing to develop empirical data regarding the flashover distances between conductors and vegetation.[52] To carry out this project, NERC is contracting support to conduct the necessary research and testing that will provide empirical evidence to statistically validate the calculation of the minimum vegetation clearance distances (MVCD), as specified in Reliability Standard FAC-003-3. Significant industry support for the application of the Gallet Equation, which uses the gap factor to calculate MVCD, was a key factor in achieving approval for this NERC Reliability Standard. A final report summarizing this research will be filed with the Commission in June 2015 and will advise the Commission about the issues encountered and how best to address them.

c. Protection System Maintenance and Testing

NERC has identified protection systems, and in particular reduction of protection system misoperations, as a top reliability priority. Likewise, the RISC has named protection systems as one of four high priority areas to be addressed in Reliability Standards. In particular, properly

[51] *Generator Requirements at the Transmission Interface*, 144 FERC ¶ 61,221 (2013).

[52] Order No. 777 at P 59.

maintaining protection systems supports the ERO's goal of reducing protection systems misoperations. By reducing misoperations, maintenance and testing of protection systems helps provide reliable system performance when responding to abnormal system conditions.

In 2007, NERC initiated Project 2007-17 – Protection System Maintenance and Testing – to consolidate four currently enforceable Reliability Standards[53] that pertain to various aspects of maintenance and testing of protection and control systems into a single Reliability Standard, PRC-005-2. This project also seeks to address: (i) certain Commission directives from Order No. 693 related to these four Reliability Standards;[54] and (ii) fundamental issues identified by the NERC System Protection and Control Task Force (SPCTF) in its assessment of these four Reliability Standards.

On December 19, 2013, the Commission approved Reliability Standard PRC-005-2,[55] Protection System Maintenance, which establishes requirements for a time-based maintenance program, where all relevant devices are maintained according to prescribed maximum

[53] The four Reliability Standards at issue were PRC-005-1, PRC-008-0, PRC-011-0, and PRC-017-0. *See NERC SPCTF Assessment of Standards: PRC-005-1 — Transmission and Generation Protection System Maintenance and Testing, PRC-008-0 — Underfrequency Load Shedding Equipment Maintenance Programs, PRC-011-0 — UVLS System Maintenance and Testing, PRC-017-0 — Special Protection System Maintenance and Testing*, Mar. 8, 2007 (SPCTF Assessment), available at: http://www.nerc.com/docs/standards/sar/PRC-005-008-011-017_Report_Approved_by_PC.pdf.

A supplement to the SPCTF Assessment was also considered. *See NERC SPCTF Supplemental Assessment Addressing FERC Order 693 Relative to PRC-005-1 — Transmission and Generation Protection System Maintenance and Testing, PRC-008-0 — Underfrequency Load Shedding Equipment Maintenance Programs, PRC-011-0 — UVLS System Maintenance and Testing, PRC-017-0 — Special Protection System Maintenance and Testing*, May 17, 2007, available at: http://www.nerc.com/docs/pc/spctf/Supplemental_Report_on_PRC-005-008-011-017_Approved_by_PC_2.pdf.

[54] The Commission approved Reliability Standard PRC-005-1 in Order No. 693 and directed NERC "to develop a modification … through the Reliability Standards development process that includes a requirement that maintenance and testing of a protection system must be carried out within a maximum allowable interval that is appropriate to the type of the protection system and its impact on the reliability of the Bulk-Power System." The Commission also directed NERC to consider suggestions made by commenters to "combine PRC-005, PRC-008, PRC-011, and PRC-017 into a single Reliability Standard." Order No. 693 at P 1475.

[55] On March 30, 2011, NERC submitted a petition for Commission approval of a proposed modification to the definition of "Protection System" to close a reliability gap created by an omission in the prior definition. The Commission approved the modified definition, which is used in PRC-005-2. *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,095 (2012).

intervals.[56] It also establishes requirements for a condition-based maintenance program, where the hands-on maintenance intervals are adjusted to reflect the known and reported condition of the relevant devices. For a performance-based maintenance program, the hands-on maintenance intervals are adjusted to reflect the historical performance of the relevant devices. PRC-005-2 also provides a comprehensive set of requirements that define a strong protection systems maintenance program. It also includes detailed tables of minimum maintenance activities and maximum maintenance intervals for all five component types addressed within the NERC definition of protection system. Functional entities that monitor the actual condition of their protection system components are further empowered to utilize monitoring to improve the efficiency and effectiveness of their protection systems maintenance program. With the benefit of extensive protection system performance data, these entities will improve the efficiency and effectiveness of their programs.

This Reliability Standard will go into effect on April 1, 2015, and implementation will continue over a twelve-year phased-in period, which includes milestones for implementation during the implementation timeframes. In furtherance of the important issues surrounding the maintenance and testing of protection systems, the System Protection and Control Subcommittee (SPCS) issued a report that suggested improving commissioning practices through: (i) analysis of protection system misoperations; (ii) sharing of lessons learned; and (iii) development of an industry reference document on protection system commissioning practices.[57]

[56] *Protection System Maintenance Reliability Standard*, 145 FERC ¶ 61,253 (2013)

[57] *See* the Planning Committee-approved final report, *SPCS Response to Standards Committee Request for Research*, (Mar. 5, 2013), available at: http://www.nerc.com/docs/pc/spctf/SPCS%20Commissioning%20Testing%20Response_Final.pdf.

d. Geomagnetic Disturbances

As high-impact, low-frequency (HILF) events, severe GMDs pose a unique threat to BPS reliability. NERC is committed to working with stakeholders and the Commission to mitigate the risks posed by such events. The science concerning GMDs is still maturing and there is significant disagreement in the scientific and manufacturing communities about the most likely effects of a GMD event on the BPS, but NERC recognizes the potential for GMDs to adversely affect the BPS. Occurrences such as the 1989 event in Hydro-Québec demonstrate that severe solar storms have potential to cause loss of reactive power support, voltage instability, relay misoperations, and possibly equipment loss of life or damage to the BPS.

Through the efforts of the Geomagnetic Disturbance Task Force (GMDTF), NERC released the *2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System* in February 2012.[58] The GMDTF identified four recommendations for industry in the report:

(1) Improve tools for industry planners to develop geomagnetic mitigation strategies;

(2) Improve tools for system operators to manage geomagnetic impacts;

(3) Develop education and information exchanges between researchers and industry; and

(4) Review the need for enhanced NERC Reliability Standards.

With implementation of these recommendations well underway, the Commission issued Order No. 779 concerning Reliability Standards for GMDs on May 16, 2013.[59] In Order No. 779, the Commission directed NERC to submit for approval proposed Reliability Standards that address the impact of GMD on the reliable operation of the BPS, in two stages. In the first stage,

[58] Available at: http://www.nerc.com/pa/stand/pages/geomagnetic-disturbance-resource.aspx.

[59] *Reliability Standards for Geomagnetic Disturbances*, Order No. 779, 143 FERC ¶ 61,147 (2013).

NERC was directed to develop one or more Reliability Standards that require owners and operators of the BPS to implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the BPS. On November 14, 2013, well within the six-month time frame directed by the Commission, NERC submitted a petition requesting Commission approval of the first GMD Reliability Standard.[60] The proposed standard, EOP-010-1, requires entities to develop tailored operating plans, processes, and procedures.

In the second stage, NERC was directed to submit one or more Reliability Standards that require owners and operators of the BPS to conduct initial and on-going assessments of the potential impact of benchmark GMD events on BPS equipment and the BPS as a whole. NERC and the standard drafting team assigned to develop GMD Reliability Standards have completed development of a technically justified benchmark GMD event during the first half of 2014 in preparation for completion of Reliability Standard development in late 2014.

The following efforts resulting from implementation activities have been important in supporting development of technically sound Reliability Standards, as ordered by the Commission:

(1) Development of operating procedure templates for transmission operators that reflect best practices and consensus among technical experts;

(2) Improved ground conductivity models that represent the geological regions of North America and a published guidance for modeling geomagnetically-induced current; and

(3) Initiation of a transformer modeling and testing project to validate models used to assess the effects of geomagnetically-induced current on transformers.

NERC is continuing efforts to expand the technical foundation for understanding the potential impact of GMD by supporting the work of the GMDTF and collaborative research with

[60] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard EOP-010-1 – Geomagnetic Disturbance Operations*, Docket No. RM14-1-000 (Nov. 14, 2013).

the Electric Power Research Institute, U.S. Geological Survey, Natural Resources Canada, and other public and private research organizations. The GMDTF and the Electric Power Research Institute are giving focused attention toward improving the suite of publicly available and technically valid tools, guidelines, and transformer models to evaluate potential impacts of GMD. The results of this work will support registered entities in conducting vulnerability assessments as required by the second stage Reliability Standards being developed in response to Order No. 779.

e. Physical Security Reliability Standard

On March 7, 2014, FERC issued an order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the BPS. FERC's order focused on critical facilities, directing steps to evaluate physical security threats and implement security plans that continues NERC's ongoing physical security efforts. In the order, FERC stated, among other things, that the proposed Reliability Standard(s) should require entities to take at least the following three steps:

(1) Perform a risk assessment to identify facilities that, if damaged or rendered inoperable, could result in instability, uncontrolled separation, or cascading failures on the BPS;

(2) Evaluate the potential threats and vulnerabilities to those identified facilities; and

(3) Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

The Commission's order also specified that the Reliability Standard should require procedures for a third party to verify the list of identified facilities and add or remove facilities from the list, procedures for a third party to review the evaluation of threats and vulnerabilities and the

physical security plan, and that the three steps listed above be periodically re-evaluated and revised.

In response to the order, NERC staff and the NERC SC worked together to develop an action plan for meeting the June 5, 2014 deadline. The NERC SC approved several waivers to facilitate meeting the required timelines and formed the eleven member standard drafting team on March 21, 2014. Also on March 21, 2014, the NERC SC approved waivers to support drafting activities to meet the June 5, 2014 deadline. Additionally, on March 21, 2014, the NERC SC also accepted the Project 2014-04 standard authorization request for a seven calendar-day informal comment period posting, pursuant to the NERC SC-approved waiver. On April 1, 2014, NERC staff convened a technical conference to focus stakeholder discussion on developing a draft of a Physical Security Reliability Standard, with the intent of assisting the standard drafting team to quickly develop and post a Reliability Standard for comment and ballot. The conference provided a forum for industry input on the concepts in the draft Reliability Standard, to include criteria for determining applicable entities, identification of critical facilities, evaluation of potential threats and vulnerabilities, development and implementation of physical security plans, and the proposed standard's implementation plan. NERC Compliance staff also provided an overview of the RSAW approach.

The Physical Security standard drafting team developed the proposed Reliability Standard, CIP-014-1 through the Reliability Standards development process. The Reliability Standard was posted under a NERC SC-approved waiver for a 15-day concurrent comment and initial ballot period from April 10, 2014 through April 24, 2014. The initial ballot achieved a quorum of 88.60 percent and an industry approval of 82.07 percent. The final ballot was posted, under an SC-approved waiver, for a 5-day period from May 1, 2014 through May 5, 2014 and

achieved a quorum of 92.53 percent and an industry approval of 85.61 percent. The NERC Board adopted the standard on May 13, 2014, and it was filed with FERC by NERC on May 23, 2014.

B. The ERO Is Implementing Processes to Register Entities Commensurate with Risk to the Bulk Power System

The starting point for the ERO's program for monitoring and enforcing compliance with Commission-approved Reliability Standards is its processes for comprehensively identifying and registering owners, operators and users of the BPS that are responsible for performing reliability-related functions in accordance with the approved Reliability Standards. This section discusses major enhancements to the registration process initiated during the assessment period.

1. Improved Registration Processes, Information Systems, and Methods Across Regional Entities

NERC's organization registration process identifies entities that are responsible for compliance with the Commission-approved Reliability Standards. Entities that are registered are included on the NERC Compliance Registry (NCR) and are responsible for compliance with all applicable Reliability Standards. Pursuant to Section 500 of the NERC ROP and the terms of the approved Regional Entity delegation agreements (RDAs), the Regional Entities are responsible to provide timely and accurate information to NERC relating to registrations to enable NERC to maintain a NCR that is accurate and up-to-date.[61] To further consistency and increase transparency in registrations across the Regional Entities, as well as to address the problem of obtaining timely updates of registration information from entities, NERC developed a Common Registration Form (CRF) which registered entities use to provide the Regional Entities with real-

[61] The amended and restated RDAs, effective January 1, 2011, included revisions to the provisions concerning the Regional Entities' responsibilities in the registration process. In addition, revisions to the registration criteria and registration processes were effectuated through amendments to NERC ROP Section 500, Appendix 5A, *Organization Registration and Certification Manual*, and Appendix 5B, *Statement of Compliance Registry Criteria*, during the assessment period.

time updates of the information recorded in the NCR pertaining to ownership, operations, contact information, asset lists and other information that may affect registration status. A corollary benefit of the CRF is that it serves as a check for the Regional Entities to ensure that owners, users, and operators of the BPS are appropriately registered. NERC is also undertaking an effort to map all the inter-relationships between registered entities on the NCR, to ensure that all owners, users and operators of the BPS are registered in the NCR.

In January 2014, NERC launched the Risk-based Registration Assessment Initiative to enhance the compliance registration and certification program to be more efficient and better aligned with reliability benefit. Through this initiative, NERC will register entities and assign appropriate Reliability Standard requirements commensurate with the need to mitigate the risk that each entity poses to the BES, by scaling registration criteria based on their contributions to reliability. NERC will also develop tools that will enhance registered entities' understanding of the relevant Reliability Standards and requirements that apply to them. Scoping compliance responsibilities according to BPS reliability risks equates to better use of resources at both the registered entity level in the implementation of compliance programs, and at the Regional Entity level in their overall compliance monitoring efforts.

2. BES Definition

During the assessment period, NERC revised the definition of the BES in the NERC *Glossary of Terms Used in Reliability Standards*, in response to Commission directives in Order Nos. 743 and 743-A.[62] The objective of the revisions is to ensure consistent inclusion or exclusion of entities and elements that are subject to Reliability Standard requirements. With the strong support and participation of industry representatives and the Regional Entities, NERC

[62] *Revision to Electric Reliability Organization Definition of Bulk Electric System*, Order No. 743, 133 FERC ¶ 61,150 (2010), *order on reh'g*, Order No. 743-A, 134 FERC ¶ 61,210 (2011).

delivered a technically grounded and legally supportable foundation for identifying the elements and facilities that comprise the BES.

In Phase 1 of this process, NERC proposed to eliminate regional discretion and establish a bright-line threshold that includes in the BES all facilities operated at or above 100 kV. The Commission accepted the revised definition in Order No. 773.[63] NERC also identified specific categories of facilities and configurations as inclusions and exclusions to the BES definition. These inclusions and exclusions are set forth in the revised BES definition. The process for requesting an inclusion or exclusion in or from the BES, is set forth in Appendix 5C, *Procedure for Requesting and Receiving an Exception from the Definition of the Bulk Electric System*, of NERC's ROP, which FERC has also approved.[64] Appendix 5C establishes an exception process to bring elements within, or remove elements from, the BES definition on a case-by-case basis.

In Phase 2 of the BES definition process, NERC addressed additional regulatory directives from Order Nos. 773 and 773-A, as well as industry comments received during Phase 1. As part of Phase 2, and with industry input, NERC proposed substantive changes to Inclusion I4 (dispersed power producing resources), Exclusion E1 (radial systems), Exclusion E3 (local networks), and Exclusion E4 (reactive power devices). The Commission approved the additional proposed revisions to the BES definition in an order issued March 20, 2014.[65]

The Commission-approved revised BES definition enables NERC and the Regional Entities to identify assets that are material to the reliability of the interconnected transmission

---

[63] *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012); *order on reh'g*, Order No. 773-A, 143 FERC ¶ 61,053 (2013), *order on reh'g and clarification*, 144 FERC ¶ 61,174 (2013).

[64] Available at: http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_5C_ProcForReqAndRecExFromAppOfNERCDefBES_20140701.pdf.

[65] *North American Electric Reliability Corporation, Order Approving Revised Definition*, 146 FERC ¶ 61,199 (2014).

network. By using a set of continent-wide, "bright line" criteria that eliminates regional discretion, the revised definition effectively ensures that the users, owners and operators of BES assets are identified and registered on a consistent basis in order to comply with applicable Reliability Standards. The revised BES definition provides improved clarity for industry by identifying specific categories of facilities and configurations as inclusions and exclusions to the BES. Additionally, the case-by-case exception process to add elements to, and to remove elements from, the BES provides transparency and uniformity to the determinations of what constitutes the BES.

To implement the revised BES definition, which became effective on July 1, 2014, NERC developed a web-based, ERO Enterprise-wide application, the BESnet Enterprise Application Tool (BESnet tool), to provide a consistent platform for registered entities to submit self-determined notifications and to submit exception requests for inclusions in or exclusions from the BES. Once a registered entity applies the BES definition to a specific element within its system, it must notify its applicable Regional Entity of any newly identified system elements that are inclusions or exclusions (i.e., system elements with changed BES classifications under the revised BES definition). Inclusion and exception decisions on the self-determined notifications are made by the Regional Entity through the BESnet tool in order to support uniform reviews and evaluations by the Regional Entity and NERC. If a Regional Entity receives notification of a self-determined exclusion, then it must evaluate whether that registered entity can stop its compliance obligations for that excluded system element. If a Regional Entity receives notification of a self-determined inclusion, then the Regional Entity must evaluate whether that registered entity should take steps to bring that system element into compliance with applicable Reliability Standard requirements within a fixed implementation period. NERC

will also use the BESnet tool to manage associated support materials and records related to technical reviews by the Regional Entities and NERC.

NERC is finalizing implementation materials that will guide the consistent evaluation of inclusions, exclusions and self-notifications of BES elements across the ERO Enterprise. NERC has created a single portal location to provide a central site to obtain useful materials to support registered entities' review of their BES elements. Additionally, the BES exception process was identified by NERC and the Regional Entity Management Group as having sufficient similarities in business processes and function across the ERO to be deemed an ERO Enterprise application, which will be used by both NERC and the Regional Entities to eliminate disparate applications across the ERO. NERC is also developing a Reliability Standard reference document to explain the intended application of the BES definition to yield consistent results. Development of additional reference documents to promote further consistency across the ERO Enterprise includes:[66]

(1) *BES Definition Reference Document*, which addresses how to apply the BES definition using several examples;

(2) *BES Definition Implementation Guidance*, which shows how the Regional Entities and NERC will review self-determined notifications and includes a high-level summary of notification requirements; and

(3) *BES Exception Request Evaluation Guideline*, which demonstrates how the Regional Entities and NERC will evaluate exception requests, and provides a high-level summary of the exception request evidentiary requirements.

During the first two quarters of 2014, NERC held communications and training sessions for Regional Entities, registered entities, and NERC staff to address, among other things: (i) evidentiary requirements for BES determinations; (ii) review and appeal mechanisms; and (iii) Reliability Standards applicability. These sessions included workshops and webinars.

[66] *See* the Bulk Electric System (BES) Definition, Notification, and Exception Process Page at: http://www.nerc.com/pa/rapa/pages/bes.aspx.

C. The ERO Monitors and Enforces Compliance with Reliability Standards in an Efficient and Transparent Manner Using Enforcement Processes that Match the Risk and Importance of Possible Violations to BPS Reliability

A key, strategic transformation that NERC, in collaboration with the Regional Entities and stakeholders, embarked upon during the assessment period is the construction of a risk-based model for compliance monitoring and enforcement. This risk-based approach enables NERC to focus ERO and industry resource investment on the most important issues to BPS reliability. In this section of the assessment report, NERC highlights initiatives to improve the Compliance Monitoring and Enforcement Program (CMEP) during the assessment period, including the FFT program. The FFT program and its subsequent enhancements began to implement this risk-based approach. The FFT program enables the ERO Enterprise to achieve major efficiencies in enforcement. Through the use of FFT, the ERO resolves noncompliances that pose a lesser risk to BPS reliability more efficiently, recognizing that efficient disposition of such issues allows the ERO Enterprise and industry to devote its emphasis and resources to more important reliability matters. Further, through careful planning and coordination and collaboration between NERC and the Regional Entities, NERC has achieved major enforcement efficiencies. These efforts have also resulted in a drastically reduced NERC caseload; for the past two years, NERC and the Regional Entities have worked to eliminate all items in the caseload which are older than 24 months. In 2012, that effort resulted in a reduction of those items by 80%. In 2013, the ERO Enterprise reduced those items by 93%. By the end of 2013, only 65 violations in inventory were older than 24 months. Additionally, taking advantage of the FFT process, which provides incentives for self-reporting, registered entities continue to aggressively self-identify, self-report and mitigate reliability issues.

Building upon the success of FFT through the RAI, NERC and the Regional Entities created additional incentives to discourage poor performance and encourage positive behaviors

that contribute to higher accountability and improved reliability performance. RAI processes that promote more effective reliability risk mitigation by encouraging development and enhancement of internal management controls and corrective action programs at registered entities began to be implemented in 2013.[67]

1. Compliance Enforcement Initiative and Find, Fix, Track and Report

Recognizing the need and the importance of ensuring that reliability risks are addressed properly through a scaled approach, NERC devised the FFT initiative in 2011 as a risk control strategy that differentiates and addresses compliance issues according to their significance to the reliability of the BPS. FFT emphasizes proportionality and enforcement discretion. The FFT process enables NERC to report lesser-risk possible violations of Reliability Standards through a streamlined process that results in the posting of a minimal record associated with the noncompliance on NERC's website.[68] The FFT initiative illustrates that NERC continually reevaluates, redirects and rebalances its CMEP implementation efforts.

NERC developed FFT in conjunction with the Regional Entities. The development of the process benefited from collaboration with representatives of registered entities through a series of focus groups. During these focus group sessions, participants indicated that registered entities typically allocated time and resources equally among violations, regardless of the risk to reliability posed by each violation. Implementation of the FFT initiative was the first step towards addressing this mis-allocation of resources.

Since the launch of FFT in 2011, NERC has implemented additional enhancements to the process. Specifically, NERC expanded FFT treatment to: (i) a limited pool of possible moderate

[67] As noted previously, NERC will submit a separate informational filing to the Commission describing these processes.

[68] In contrast, NERC submits violations that pose a greater risk to reliability or do not otherwise meet the FFT criteria to the Commission in a spreadsheet Notice of Penalty (SNOP) or full Notice of Penalty (NOP) format.

risk violations; and (ii) some unmitigated possible violations so long as mitigation occurs within 90 days from the date the FFT item is filed or posted. To streamline processing of FFT items, NERC now posts FFTs collected by the Regional Entities on its website at the end of each month without prior review of such items. This replaces the prior procedure in which NERC submitted monthly informational filings to the Commission describing FFT items. While the Regional Entities post FFT items on a monthly basis, NERC maintains its enforcement oversight by reviewing a representative sample of FFTs during the 60-day window following the Regional Entities' monthly postings and by conducting an annual spot check of FFTs.

The FFT program has been highly successful in promoting a risk-based approach to resolving noncompliance. All Regional Entities utilize FFT to resolve a large number of minimal risk issues. Further, through its monthly reviews and annual spot checks, NERC verifies that the parameters for identifying minimal risk issues are consistently applied throughout the ERO Enterprise.

2. Reliability Assurance Initiative

In November 2012, NERC management proposed RAI as a multi-year effort to identify and implement changes to enhance the effectiveness of the ERO Enterprise's compliance and enforcement functions. RAI will help NERC foster consistency and efficiency in its compliance monitoring and enforcement processes. NERC expects RAI to improve BPS reliability by refocusing efforts on serious and substantial reliability risks and promoting the development and enhancement of the internal controls that mitigate those risks. Increased consistency in the ERO Enterprise's compliance and enforcement efforts yields a level of predictability for registered entities to understand how Reliability Standards are applied and enforced and to model positive behaviors.

To foster dialogue and seek industry feedback on the various aspects of RAI, NERC hosted a series of workshops in 2013 that addressed defining internal controls, conducting risk assessment, launching pilot programs, enhancing the FFT process, and improving self-reporting.

a. RAI Improvements to Compliance Monitoring Processes

The core concept of risk-based compliance monitoring is intended to guide Regional Entities in allocating resources for compliance monitoring activities and methods based on a registered entity's potential impact on the BPS. Compliance-related activities under the RAI program will help achieve a risk-based approach for compliance monitoring by evaluating current compliance monitoring practices, identifying improvements, and addressing the consistent application of audit techniques and the use of uniform tools to carry out compliance monitoring activities.

In 2013, NERC and the Regional Entities began to develop and implement tools that will define techniques and methods to perform compliance monitoring in a consistent manner across the ERO Enterprise. The Regional Entities began using the first of these tools, the *Compliance Auditor Checklist*, in August 2013. In December 2013, NERC and the Regional Entities completed the first draft of a companion document for the *Compliance Auditor Checklist*, specifically, the *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual* (Auditor Manual). NERC disseminated the Auditor Manual and provided initial training to Regional Entity auditors during the first quarter of 2014. In the second quarter of 2014, the Regional Entities began to use the Auditor Manual and its related processes and procedures on a select number of audits. Throughout 2014, NERC and the Regional Entities will revise and expand the Auditor Manual to address additional audit topics, reflect additional processes developed through RAI activities, and include lessons learned.

A second key RAI compliance activity, the Prototypes and Pilot program, focuses on the development and implementation of a formalized approach to risk assessments and testing of management controls. NERC and the Regional Entities initiated the first phase of the Prototypes and Pilot program during 2013. This phase explored different approaches to applying risk-based auditing concepts (e.g., audit scoping, reliability risk assessments, and management controls review and testing). For 2014 and beyond, a team consisting of NERC, Regional Entity, and industry representatives as well as an independent audit consultant will evaluate the findings and determine the best audit approach to implement throughout the ERO enterprise.

NERC and the Regional Entities are also developing and implementing activities that will address the transition to CIP Version 5 and redesign the tools and information available for compliance monitoring. In addition, and as discussed in further detail below, NERC and the Regional Entities have consolidated the annual CMEP Implementation Plans with the goal of implementing certain risk-based compliance enhancements.

b. RAI Improvements to Compliance Enforcement Processes

The enforcement aspect of the RAI builds on the success of FFT to develop incentives for registered entities to distinguish between poor performance and positive behaviors that contribute to higher accountability and improved reliability performance. The RAI calls for NERC to do the following by 2016: (i) exercise discretion to focus resources on the most serious and substantial risks to the reliability of the BPS; and (ii) empower registered entities to self-identify, mitigate and record noncompliance subject to NERC and Regional Entity oversight.

Similar to the RAI compliance monitoring effort, the enforcement element of RAI seeks to align the ERO's enforcement processing activities with levels of risk to the reliability of the BPS. Achieving this alignment will promote efficiencies for both the ERO Enterprise and

registered entities by eliminating undue regulatory burdens, streamlining documentation and filing requirements, and substantially improving the processing of noncompliance and related mitigating activities.

In 2013, NERC began implementing a series of activities in connection with RAI. These activities consisted of both short-term and long-term solutions to address registered entity concerns and improve enforcement processes. For example, in 2013, NERC and the Regional Entities developed the *ERO Self-Report User Guide*. This document explains the type and quality of information that a registered entity should submit with a self-report in order to allow for a prompt evaluation of noncompliance, and, if appropriate, a prompt disposition of the noncompliance if it poses a minimal risk to the reliability of the BPS. A companion *ERO Mitigation Plan Guide* document was also developed. NERC posted the draft guides in January 2014 for public review and comment. The final user guides are now available on the RAI page on the NERC website.[69]

Second, NERC and the Regional Entities began two pilot programs to test RAI enforcement concepts. The first pilot, the Aggregation of Minimal Risk Issues program, tests selected registered entities' ability to proactively self-address, identify, and mitigate minimal risk issues. The second pilot is testing the application of enforcement discretion; the purpose of this pilot is to identify minimal risk issues that would be recorded and mitigated without triggering an enforcement action. These pilot programs began a six-month testing cycle in October 2013. NERC and the Regional Entities are gradually expanding the programs to include additional registered entities.

[69] Available at: http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

In addition, as of January 2014, all Registered Entities implemented the triage process. Under this process, all Regional Entities will review instances of noncompliance and make an initial determination as to whether an issue will proceed through enforcement or whether additional information is needed.

Going forward, NERC will continue to implement and evaluate these enforcement concepts. These processes will be further discussed in an informational filing on the RAI that NERC will submit to the Commission in 2014.

3. Development of a Consolidated CMEP Implementation Plan

NERC and the Regional Entities no longer create nine separate CMEP Implementation Plans, but rather have consolidated these documents into a single integrated CMEP Implementation Plan for the ERO Enterprise. The consolidated CMEP Implementation Plan uses a streamlined format that eliminates redundant information, improves the transparency of CMEP activities, and promotes consistency among the Regional Entities' Implementation Plans.

During the implementation year, NERC or a Regional Entity (with NERC approval) may update the Implementation Plan to change the *Actively Monitored List of Reliability Standards*, compliance monitoring processes, Regional Entity processes, or to provide updates. When updates occur, NERC will post a revised Implementation Plan to its website and issue a compliance communication. A Regional Entity may also update its Implementation Plan, with NERC approval. NERC is responsible for updating the ERO CMEP Implementation Plan to reflect any Regional Entity's changes and for posting the updated plan to its website and issuing compliance communications.

Following each implementation year, the Regional Entities will complete a CMEP Implementation survey due in January of the following implementation year (e.g., the 2014

CMEP Implementation Plan survey is due in January 2015). This survey will provide Regional Entity-specific information on compliance monitoring, outreach, enforcement, CMEP program effectiveness, and other regional activities. NERC will use this information to monitor Regional Entity CMEP implementation and to plan for the following implementation year.

4. Improvements in Processing of Compliance and Enforcement Items by NERC and the Regional Entities

a. NERC and the Regional Entities Have Improved the Speed and Efficiency of Processing Enforcement Items

During the assessment period, NERC and the Regional Entities have continued to hold industry accountable for violations that create serious risk to the BPS, and to implement improvements to ensure that enforcement actions are timely and transparent to industry. As discussed in further detail in the "Enforcement" section of the NERC Assessment of Regional Entity Delegated Functions (**Attachment 3**), by the end of 2013, NERC had reduced the number of active violations older than 24 months (excluding those held by appeal, a regulator, or a court)[70] so that only 65 such active violations remained. There has been consistent progress since 2012 in achieving the goal of processing all violations within 24 months following discovery.

By working to reduce the number of aging violations while improving the processing speed for newer violations, NERC and the Regional Entities reduced the average age of violations in the ERO caseload by six percent in 2013, from 11.86 months in 2012 to 11.2 months.

NERC's successes in improving the efficiency of violation processing can be attributed to several factors, including the implementation and use of streamlined enforcement processing

[70] "Held by appeal, a regulator or a court" (or "on hold") refers to violations that are not currently being processed by NERC or the Regional Entities as a result of a court or administrative proceeding that will impact the resolution of the violation.

mechanisms, such as FFT and the SNOP. The use of streamlined enforcement processing mechanisms has allowed NERC to increase substantially the number of violations filed in a given year, reducing the caseload and in turn, improving processing times.

In 2009 and 2010, NERC filed NOPs with the Commission for a combined total of 1,540 violations. In 2011, after implementing the use of streamlined enforcement processing mechanisms, NERC filed a total of 1,697 violations – more than the two previous years combined. In 2012, NERC filed a total of 1,767 violations. In 2013, NERC filed a total of 1,862 violations. NERC processed approximately 43 percent of the violations filed in 2013 using the FFT mechanism.

In addition to the use of streamlined enforcement mechanisms, NERC has dedicated substantial resources to improving its enforcement processing activities and performance. In fact, during the period covered by this *Five-Year ERO Performance Assessment Report,* NERC has more than doubled the size of its enforcement processing staff, going from four full time equivalent personnel (FTEs) in 2010 to nine FTEs as of January 1, 2014.

Lastly, NERC has taken several steps to enhance collaboration and consistency across the entire ERO Enterprise. NERC enforcement processing has assigned staff to work closely with each Regional Entity to enhance the relationships with each Regional Entity and to develop greater knowledge and expertise concerning each Regional Entity and identify areas for collaboration and process enhancement. In addition, NERC is continuing to provide training to the Regional Entities with the goal of increasing the consistency of enforcement processes and documents. Through collaboration with the Regional Entities, NERC expects to build on its past successes and continue to work toward reducing aging caseload, reducing enforcement processing times, and ensuring consistency in enforcement processes and procedures.

NERC and the Regional Entities have continued to work collaboratively to develop and implement a set of metrics to measure the efficiency with which enforcement items are processed. Development of these performance items was an area for improvement identified in the Commission's order on NERC's Three-Year ERO Performance Assessment.[71] A set of final metrics has been agreed upon and a set of common parameters was developed to ensure that metrics measurements by NERC and the Regional Entities remain consistent. To that end, in the third quarter of 2013, NERC and the Regional Entities developed a set of business rules to ensure integrity and alignment across NERC and Regional Entity data. Ensuring the integrity of this data is important for analyzing trends and calculating processing metrics.

The four metrics developed to monitor the performance of NERC and the Regional Entities in processing enforcement items are:

(1) Caseload Index – computes the number of months it would take to clear the violations in a Compliance Enforcement Authority's (CEA, i.e., NERC or a Regional Entity) inventory based on the CEA's average monthly processing rate for the preceding twelve month period;

(2) Violations in Inventory – reports the number of violations in the CEA's caseload;

(3) Violation Aging – reports, by Regional Entity, the number of violations discovered in each year beginning with 2007 that have not been filed with the Commission or otherwise resolved;[72] and

(4) Mitigation Activity Aging – identifies the status of mitigation activity based upon age of violations.

NERC will continue to analyze and evaluate violation processing data. The purpose of analyzing violations and violation processing information is to identify trends and emerging risks. This analysis will provide NERC with insight into the effectiveness of NERC's and the

[71] *Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010) at PP 138 and 217.

[72] NERC also monitors Violation Aging by Disposition Method. This includes the average turnaround time for each disposition method for violations discovered within a specified time horizon (i.e., discovery to date filed with NERC, date filed with NERC to date filed with the Commission, and discovery to date filed with the Commission).

Regional Entities' processes and programs. The analysis informs the development of enforcement policies and processes and offers feedback for other departments such as Standards.

NERC's departments collaborate to leverage analytics as a risk management and resource allocation tool. As an example of this effort, NERC is closely monitoring the status of mitigation activity completion, regardless of whether or not the violation is on hold. NERC aims to work with the Regional Entities to reduce the amount of time from discovery of a violation to completion of the mitigating activity, thereby reducing the ongoing risk that these violations may pose to reliability.

b. Oversight of Regional Entity Processes and Actions

NERC is continuously evaluating and improving its methods of overseeing the Regional Entities' implementation of CMEP processes and procedures. During the assessment period, NERC adopted a more methodical approach to evaluating Regional Entity performance with respect to enforcement activities. NERC has also enhanced its approach to evaluating Regional Entity compliance activities. These oversight activities ensure that the Regional Entities are meeting their obligations under the NERC ROP and the RDAs. These oversight activities also promote transparency and consistency, and drive the identification and implementation of best practices across the ERO Enterprise.

For additional information regarding NERC's oversight of Regional Entity enforcement program and processes, see the "Enforcement" section of the NERC Assessment of Regional Entity Delegated Functions, **Attachment 3** to this *Five-Year ERO Performance Assessment Report.*

c. Developing Common Compliance Auditor Qualifications Across the ERO Enterprise

NERC and the Regional Entities are developing common ERO auditor qualification

requirements and auditor job descriptions that will be consistently used across the ERO Enterprise. Establishing common ERO auditor qualifications is an initiative specified in the 2013-2016 ERO Strategic Plan.[73] NERC and the Regional Entities will establish key attributes and skill sets that audit team members should possess to ensure the audit team composition includes competencies needed to complete an effective audit. Establishing common ERO job descriptions promotes a consistent approach in attracting and retaining the necessary talent for auditor positions. Common auditor qualification criteria, training, and audit approach help promote high-quality audits and consistency in CMEP implementation activities across the ERO Enterprise.

d. Enhancing the Training Program for Auditors so that Processes and Procedures Developed in the RAI are Implemented Consistently Across the ERO Enterprise

As part of its Regional Entity Assurance and Oversight function, NERC is responsible for supporting the development of qualified and trained compliance operations and auditing staffs at both NERC and the Regional Entities. In addition to the development of a common set of auditor qualifications, described in the immediately preceding subsection, NERC ensures the proper qualifications of personnel for auditing and other essential compliance roles through training. As noted above, NERC and the Regional Entities collaborated to create the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the Auditor Manual.[74] These documents will be reviewed and revised to incorporate lessons learned from the RAI pilots. NERC will train auditors to ensure that Regional Entities are consistently applying the

[73] The *Electric Reliability Organization Enterprise Strategic Plan 2013-2016* is available at: http://www.nerc.com/gov/bot/FINANCE/Documents/ERO%20Enterprise%20Strategic%20Plan%202013-2016%20FINAL%2005%2009%2013.pdf

[74] Available at: http://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/ERO_Enterprise_Compliance_Auditor_Manual_version_1.pdf.

procedures and methodologies of these documents. Auditor training will also incorporate relevant changes related to enforcement processing, including changes to the self-reporting process and enhancements to the FFT process. Setting clear expectations for registered entities regarding audit practices and procedures should also allow registered entities to increase the efficiency and effectiveness of their pre-audit preparation.

D. Identification, Prioritization, and Dissemination of Information on Risks to the BPS

NERC is an expert resource for industry on reliability risks and information because it is uniquely positioned to assess potential impacts to reliability and raise awareness of threats to reliability. NERC draws upon a plethora of resources, discussed below, to make its assessments, including the RISC priorities, robust databases of information on transmission, generator and demand-response availability, the annual NERC *State of Reliability* report, and other assessments and reports, as well as internal core analyses of events. In its risk-informed approach, NERC uses performance analysis, solid technical foundation, sophisticated statistical analyses, and integrated validation with actual system events to enhance BPS reliability. As described in §II.D.1 below, at the direction of its Board of Trustees, NERC has developed and is implementing a specific RRM process to create and execute plans for managing reliability risks.

As an example of risk identification, NERC's *2013 Long-Term Reliability Assessment* (LTRA) identified significant emerging reliability issues that industry will face over the next decade.[75] These challenges stem from, among other things, a changing resource mix comprised of significant increases in variable energy resources to meet renewable portfolio standards, increased reliance on natural gas-fired generation and demand-side management primarily driven by economics, and the retirement of nearly 10% of North America's generation capacity.

[75] Available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2013_LTRA_FINAL.pdf.

Another resource for identifying and prioritizing risks is NERC's Event Analysis process. This process, which is described in greater detail in §II.D.3 below, establishes a systematic approach to capturing details about all BPS events, from minor Category 1 Events that typically do not have a significant impact on electricity users, to Category 4 and 5 Events that result in widespread customer outages.

Collectively, these resources provide an independent and complete picture of risks to reliability and key BPS reliability indicators such as resource adequacy, peak demand, energy forecasts and transmission developments. These efforts and well-developed resources are critical to how NERC approaches reliability, learns from events on the BPS, and prioritizes resources.

NERC draws upon these resources to inform industry and policymakers about trends and challenges to reliability. One example is the work of the NERC Integration of Variable Generation Task Force (IVGTF), which developed several recommendations that support the reliability considerations for accommodating large amounts of variable generation.[76] These recommendations guided the California Independent System Operator (CAISO) in finding solutions to how it will ensure reliability given the significant development of variable energy resources in that region of the country. Another example is the *Accommodating an Increased Dependence on Natural Gas for Electric Power* report that examined the different risks, arising out of the interdependence of the BPS and the natural gas delivery system, which can affect reliability.[77] Recommendations from this report are being used by WECC, the CAISO, and the Midcontinent Independent System Operator, among others, to identify approaches to minimize vulnerabilities due to electric system-gas system interdependence.

[76] Information about the IVGTF is available at: http://www.nerc.com/comm/PC/Pages/Integration-of-Variable-Generation-Task-Force-(IVGTF)-2013.aspx.

[77] Available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf

1. Establishing a Structured Reliability Risk Management Process

In response to direction from the NERC Board in February 2013, NERC has developed a RRM process to create and execute plans for managing reliability risk and to integrate these plans with the business planning and budgeting process. The RRM process leverages: (i) the business acumen of the RISC; (ii) the technical knowledge of the NERC Operating Committee, Planning Committee, and CIP Committee (CIPC); (iii) the diverse set of tools that can be employed by the ERO to manage risk; and (iv) the open and transparent nature of the ERO. The RRM process is comprised of the following stages:

(1) Strategic Planning: In this phase, the RISC works to collection information and to identify broad areas of reliability risk to be recommended to the NERC Board for further analysis and study.

(2) Analysis: In this phase, members of the RISC work with the technical committees they represent to identify specific risks within the broad areas accepted by the NERC Board. This phase includes problem definition, gap analysis, and selection of measurement approaches.

(3) Solution Design: In this phase, members of the RISC develop potential solutions to the problems identified in the previous stage. NERC uses this information to develop the *ERO Top Priority Reliability Risks* for the upcoming business planning and budget cycle.

(4) Business Planning and Budgeting: In this phase, NERC staff and the Regional Entities work together to include in the annual business plans and budgets descriptions of the reliability risks that are to be addressed in the coming year and the resources needed to support those efforts.

(5) Preparation: In this phase, ERO staff, stakeholders, and third parties[78] discuss the plans identified in the latest business plan and budget. At this stage, NERC's committees have an opportunity to align their work plans with the business plan and budget.

(6) Execution: In this phase, stakeholders, staff, and third parties execute the detailed plans developed in the prior phase.

Specific documentation or other aids to assist in the implementation of the RRM

[78] "Third parties" in this context might refer to industry manufactures and service vendors, who might be asked to work on a specific problem, tool or application.

process,[79] document templates, and detailed instructions and training are being developed to support the execution of this process. NERC intends that the RRM process will become an integral part of ERO operations.

NERC will continue the work of the RISC to develop risk profiles (including HILF issues) for the ERO. These profiles of the BPS will inform how the ERO prioritizes and ranks reliability risks. For high priority risks, NERC will develop project plans and business case assessments outlining initiatives to address those risks.

2. ERO Top Priority Reliability Risks for 2014-2017

As described immediately above, the RRM process includes the identification of the *ERO Top Priority Reliability Risks* for each upcoming business planning and budget cycle. The development of the list of top ten high priority reliability risks is intended to focus the efforts of the ERO Enterprise program areas, including training and education, Reliability Standards development, and compliance. NERC developed a set of the ten top priority reliability risks to be focused on in the development of the *ERO Enterprise Strategic Plan 2014-2017*. The development of this list started with a reliability gap analysis that the RISC presented to the NERC Board in August 2013. NERC staff then undertook further review and analysis to identify any additional reliability risk areas of strategic importance for the ERO. Next, qualitative estimates of probability, consequence, and current level of risk management were prepared for each of the identified reliability risks within the chosen areas. NERC used this information to identify ten top priority reliability risks requiring increased attention or additional activity. Following this analysis, recommendations were developed based on previous committee discussions; industry dialogue at the Reliability Leadership Summit; and past work products such

[79] This documentation and other aids may include worksheets, diagrams, task descriptions, and similar items.

as the LTRA, the *State of Reliability* report, and various special reports and assessments. The ten high priority reliability risks are:

(1) Changing Resource Mix: As the generation and load on the power system changes (e.g., integrated variable resources, increased dependence on natural gas, increased demand-side management, new technologies deployed), the system is being brought into states that are significantly different than those considered when the system was designed and planned, exposing new vulnerabilities not previously considered. Fundamental operating characteristics and behaviors are no longer a certainty.

(2) Resource Planning: Plant retirements (largely due to implemented environmental regulations; increased uncertainty in future resources due to other potential environmental regulations; and lower natural gas prices, which significantly affect power plant economics) are leading to cases where resources may be inadequate to ensure firm demand is served at all times. As the system continues to change, some regional assessments identify concerns with insufficient reserve margins as early as 2014 and 2015 in the ERCOT and Midcontinent ISOs.

(3) Protection System Reliability: A fault accompanied by a failure of any protection system component could in some cases result in instability, violation of applicable thermal or voltage ratings, unplanned or uncontrolled loss of demand or curtailment of firm transfers, or cascading outages.

(4) Uncoordinated Protection Systems: A lack of protection system coordination has the potential to increase the size and magnitude of events due to unnecessary trips. Uncoordinated protection systems were identified as contributing to the September 8, 2011, and August 14, 2003 events.

(5) Extreme Physical Events: While the probability of extreme physical events (such as physical attack, GMD, or severe weather) that lead to extensive damage is low, the potential consequences are significant enough that risk avoidance (reducing the probability) is insufficient as a sole risk management strategy.[80]

(6) Availability of Real-Time Tools and Monitoring: Not having the right tools and monitoring available to manage reliability in real time is a latent problem waiting for the right combination of events to exploit it.

(7) Protection System Misoperations: NERC's 2012 and 2013 *State of Reliability* reports identified protection system misoperations as a significant threat to BPS reliability.

(8) Cold Weather Preparedness: Lack of generator preparedness for cold weather extremes may result in forced outages, de-ratings, and failures to start.

[80] Additional strategies may incorporate factors like improving resiliency and reducing restoration times.

Insufficient availability of intra-regional generation and limits on import transfer capability may result in insufficient generation to serve forecasted load, resulting in load shedding.

(9) Right-of-Way Clearances: Transmission owners and applicable generation owners may have established incorrect ratings based on design documents, rather than on the actual facilities built. Managing to stay within system operating limits and interconnection reliability operating limits that are based on incorrect ratings may be inadequate to prevent equipment damage and/or instability, cascading outages, or separation. Ensuring clear right-of-ways can reduce adverse impacts to reliability even when SOLs and IROLs are based on incorrect ratings.

(10) 345-kV Breaker Failures: NERC has identified a potential trend of 345 kV SF6 puffer type breakers failing. Circuit breaker failures, in conjunction with another fault, may lead to more BES facilities removed from service than required to clear the original fault.

3. NERC Event Analysis Process and How it is Used to Identify Risks to the BPS and Disseminate Lessons Learned

NERC has developed a voluntary Event Analysis process that delivers quality, timely and actionable lessons learned to registered entities. Development of the Event Analysis process was led by the Event Analysis Subcommittee (EAS), a cross-functional group of industry experts.[81]

The Event Analysis process begins with a registered entity making an initial assessment of an occurrence and determining if the occurrence falls within one of five qualifying event categories.[82] The event category is determined by weighing the level of significance of a qualifying event and its impact on the interconnected BPS. After a qualifying event occurs, the applicable Regional Entity holds a planning meeting with all involved parties, including other registered entities. If a qualifying event is categorized as Category 3 or higher, the registered entity will prepare an Event Analysis Report (EAR), in which the registered entity describes the

[81] The EAS is a subcommittee of the NERC Operating Committee.

[82] A description of each event category is included in the *Electric Reliability Organization Event Analysis Process – Version 2* report, available at: http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx.

sequence of events and identifies causal factors and appropriate corrective actions. The registered entity then submits the EAR to the applicable Regional Entity(ies) for review, and then to NERC. The registered entity, in collaboration with the ERO, drafts the proposed lessons learned from the event and submits them to the applicable Regional Entity. Once the event analysis is complete, NERC shares any lessons learned with industry by publishing them as soon as practical. NERC staff analyzes EARs to identify reliability risks, trends, and potential gaps in Reliability Standards, compliance, and other programs. NERC also reviews the EARs to assign descriptive cause codes, which assist in identifying trends and corrective actions that will prevent recurrence of similar events.

Since initial implementation of the Event Analysis process in 2010, there have been more than 388 qualified events reported to the ERO and more than 77 lessons learned produced, including 14 published in 2013.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Event Counts

Event Category	Count (Total)	Count (2013)	Comments
CAT 1	256	91	
CAT 2	114	33	
CAT 3	14	6	
CAT 4	3	0	SW Winter Weather (2011) SW Blackout (2011) Derecho (2012)
CAT 5	1	0	Hurricane Sandy (2012)
Total CAT 1-5 Events	**388**	**130**	
Non-Qualified Occurrences reported	**1711**	**338**	

RELIABILITY | ACCOUNTABILITY

Participation in the voluntary Event Analysis process does not relieve registered entities of their obligation to comply with NERC Reliability Standards. While performing the steps of the Event Analysis process, the registered entity is encouraged to continue performing critical self-assessments of compliance with Reliability Standards in connection with the event and to conduct compliance self-assessments for review by applicable Regional Entities. If a registered entity discovers a possible violation in the process of analyzing an event, it is encouraged to self-report that possible violation to the applicable Regional Entity.

NERC is continuously improving how it defines, catalogs and trends the causes of system events. NERC assesses every event submitted through the voluntary Event Analysis process to identify and share possible risks to reliability with industry. Further, the cause code assignment allows for greater historical trending and predictive analysis.

NERC provides Regional Entity and registered entity staff with cause analysis training. As of December 2013, 164 personnel from all eight Regional Entities and over 600 people from 115 different registered entities have received more than 4,000 hours of cause analysis training, with 432 hours of continuing education hours awarded to 54 NERC-certified system operators in connection with this training. NERC is adding a training and education component to the Event Analysis process to increase the relevance and impact of lessons learned for the Regional Entities, industry, and other stakeholders. Through the Event Analysis process, NERC continues to establish the appropriate balance of data reporting for analysis and use by industry.

NERC continues to work with the Regional Entities to obtain from and review with registered entities information regarding qualifying events and disturbances. The primary goal of this process is to identify reliability risks through robust data gathering, validation, rigorous analysis, and rapid dissemination to industry of information on identified risks and remediation

options. NERC is working collaboratively with the Regional Entities to prioritize analytical efforts based on the Event Analysis process categories. Determining root and contributing causes for each event allows for trend and risk identification. NERC plans to further facilitate event analysis by merging its event-driven databases and defining the relationships between various system cause codes. This analysis of system events will inform NERC of gaps in Reliability Standards, compliance monitoring and enforcement effectiveness, registration, and risk controls effectiveness.

Additionally, NERC is collaborating with the North American Transmission Forum and the North American Generator Forum to further enhance the Event Analysis process and lessons learned dissemination in identifying risks to the BPS. Further, NERC plans to improve the timeliness of the availability of and access to final event reports by creating a secure portal that will be accessible by industry to obtain these reports.

4. Reports on Reliability

In May 2012, NERC released its first *State of Reliability* report assessing grid reliability based on performance trends identified through data and analysis of system disturbance events. The report presented NERC's integrated view of ongoing BPS reliability and performance trends. It assessed 18 reliability performance metrics that measure whether an adequate level of reliability exists in North America. The report also included an analysis from the frequency response initiative, the 2011 demand response availability assessment, event analysis trends, and post-seasonal assessments. The initial *State of Reliability* report included the following key findings:

(1) Reliability of the BPS remains adequate with little change in trends between 2008 and 2011;

(2) Frequency response is stable with no deterioration;

(3) Protection system misoperations are a significant reliability issue;

(4) Equipment failure warrants further analysis; and

(5) Resource mix changes necessitate new metrics.

Subsequently, *State of Reliability* reports have been issued for 2013 and 2014.[83] Going forward, NERC will continue to prepare its annual *State of Reliability* report and the associated reliability metrics.

As noted earlier, for many years NERC has prepared and issued an annual 10-year LTRA Report for the North American BPS. The LTRA provides an independent view of the reliability of the BPS and identifies trends, emerging issues, and potential concerns. Recent LTRAs have focused on a variety of emerging issues expected to impact BPS reliability. Most notably, a rapidly changing resource mix with substantial retirements of coal-fired and nuclear capacity, paralleled by a growing reliance on natural gas-fired generation that has created fuel transportation concerns in certain areas. Ongoing unit retirements are also contributing to diminishing reserve margins that fall below reference reserve margin levels during the 10-year outlook. Finally, continued penetration of variable resources and a growing dependence on demand-side management programs create uncertainties for system planners and operators. Each LTRA report also provides high-level recommendations for each emerging issue and tracks ongoing industry progress.

In addition to the annual LTRA, NERC issues two seasonal (i.e., summer and winter) assessment reports each year in which it identifies, assesses, and reports on the industry's preparations to manage potential seasonal issues such as significant generation or transmission

[83] NERC's *State of Reliability 2014* report is available at: http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf.

constraints or potential fuel-related impacts. NERC also issues other, special reports from time to time that focus on current or emerging technical or other reliability concerns, such as changing resource mix (increasing amounts of variable generation and potential retirements of fossil-fueled generation), misoperations, HILF event concerns, and smart grid considerations.

NERC has implemented several enhancements to the LTRA processes and reports in response to areas for improvement identified in the three-year ERO performance assessment. NERC has revised its reliability assessment guidelines to establish a requirement for an annual scenario analysis.[84] Scenario analyses are typically included in separate special assessments prepared by the Reliability Assessment program, including the following reports that NERC issued during the assessment period:

- *Reliability Impacts of Climate Change Initiatives: Technology Assessment and Scenario Development* (2010);
- *Special Reliability Scenario Assessment: Potential Reliability Impacts of Swift Demand Growth After a Long-Term Recession* (2010);
- *Special Reliability Scenario Assessment: Resource Adequacy Impacts of Potential U.S. Environmental Regulations* (2010);
- *Potential Impacts of Future Environmental Regulations* (2011); and
- *Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power* (2013).

5. Bulk Power System Awareness Department

Previously a functional responsibility of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[85] NERC created the Bulk Power System Awareness department

[84] *See Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010), at P 180.

[85] The activities of ES-ISAC are described in §II.E.2 below.

(BPSA) in 2012 to improve NERC's capability to monitor BPS conditions, significant events, and emerging risks to reliability across the 15 reliability coordinator regions in North America.

BPSA develops and disseminates timely, accurate and complete information regarding the status of the BPS from a near-term operational reliability perspective, complementary to RAPA's seasonal and long-term assessments and ES-ISAC's cyber and physical security perspective. BPSA shares this continuous assessment across NERC, the eight Regional Entities and FERC staff through a number of channels, including a *System Awareness Daily Report* that highlights current day potential risks to wide-area reliability, significant operational and security occurrences for the previous day, and high-level information on forecasted loads and reserves.

During major system disturbances, BPSA facilitates information sharing and a common operational picture of BPS status with a broader audience of industry and governmental agencies. BPSA provides ES-ISAC operational reliability information in support of its government and cross-sector coordination activities, and hosts periodic update conference calls for technically oriented government agencies including FERC, the Department of Energy, the Nuclear Regulatory Commission, the Department of Homeland Security, and the Federal Emergency Management Agency.

BPSA administers the NERC Alerts program, which is used to disseminate important reliability and security information to industry, pursuant to §810 of the NERC ROP. Additionally, BPSA actively participates in the Event Analysis Process described in §II.D.3 above, by identifying qualifying events and other items of interest for further trending and analysis.

E. The ERO Facilitates Information Sharing on Cybersecurity and Cyber and Physical Threats to the BPS among Industry, Regional Entities, and Government

Section 215(a) of the FPA and the Commission's regulations at 18 C.F.R. §39.1 define "reliable operation" of the BPS 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 Cybersecurity Incident, or unanticipated failure of system elements." The FPA and the regulations define "Cybersecurity Incident" as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmatic electronic devices and communications networks including hardware, software and data that are essential to the Reliable Operation of the Bulk-Power System." As the Commission is fully aware, identifying, assessing, and preventing threats and risks to both the physical security and the cybersecurity of the BPS, while always matters of concern, have attained increasing significance in the last three to four years.

Two of NERC's principal programs focused on these areas are the Critical Infrastructure department (CID) and the ES-ISAC. The CID supports efforts to develop and administer critical infrastructure standards, conducts security and reliability outreach visits, provides training and exercise opportunities, and coordinates between industry and governmental entities on CIP matters. The CID accomplishes these activities through active CIP standards drafting team participation, and programs such as the Sufficiency Review Program (SRP),[86] the annual Grid Security Conference (GridSecCon), and the biennial Grid Security Exercise (GridEx). The CID also leverages public-private partnerships to examine CIP policy issues, and it provides staff-

[86] In 2014, CID renamed the SRP to "Security Readiness Program" to reflect the program's focus.

level support to NERC's CIPC, an industry-led committee comprised of industry experts in the areas of cybersecurity, physical security, and operational security. The ES-ISAC monitors the physical security and cybersecurity of the electricity sub-sector, gathers information on threats to the physical security and cybersecurity of the sub-sector, and actively disseminates information on such threats and means to avoid or mitigate them to users, owners, and operators of the BPS as well as to applicable government entities and other stakeholders.

Both programs focus significant attention on public-private partnerships, which are critical to effective information sharing. CID and the ES-ISAC work closely with NERC entities, industry trade associations, national and international government departments and agencies, and other sectors to share information, discuss sector priorities, and respond to legislative and executive branch requests. Recent partnership activity includes sector responses to Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*. This work included coordinating with government and across sectors to develop a voluntary cybersecurity framework, based on existing standards, guidelines, and practices, for reducing cyber risks to critical infrastructure. In addition, NERC worked closely with government and industry to rewrite the *National Infrastructure Protection Plan*, which outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

This section of this *Five-Year ERO Performance Assessment Report* describes NERC's activities in these areas during the assessment period, with an emphasis on activities during the latter part of the period. Included in this section are descriptions of CID programs, such as the

CIPC, the SRP, the GridSecCon, and the GridEx, as well as ES-ISAC activities, including the Cyber Risk Preparedness Assessment (CRPA) program.

1. Critical Infrastructure Department Activities

a. Critical Infrastructure Protection Committee

NERC's CIPC focuses on advancing the physical and cybersecurity of the critical electricity infrastructure of North America. The committee consists of both NERC–appointed regional representatives and technical subject matter experts. The CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board, to the ES-ISAC, and to NERC standing committees, in the areas of cybersecurity and physical security. During quarterly CIPC meetings, CIPC members receive security training and participate in briefings regarding the latest security issues. To address issues related to cybersecurity and physical security, the CIPC establishes working groups or task forces comprised of subject matter experts who review and examine specific issues and develop reports and recommendations.

In 2012, the CIPC reorganized and expanded to allow it to produce more deliverables. This reorganization established new subcommittees and created new task forces and working groups to address emerging issues and initiative requests from the NERC CEO and NERC Board. The reorganization included forming task forces to address cybersecurity-related subjects identified in the 2010 *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* report.[87] One CIPC task force, the Cyber Attack Task Force, considered the impact of a coordinated cyber-attack on the BPS and developed flexible options for detecting, operating, and recovering from such an attack. A key component of the resulting Cyber Attack

[87] Available at: http://www.nerc.com/pa/ci/resources/documents/hilf_report.pdf.

Task Force report was the development and use of an attack tree tool that provides key insight into the attack surface of the interconnected BPS of North America.

Following NERC Board approval of the Cyber Attack Task Force report, the CIPC established a High-Impact, Low-Frequency Implementation Task Force to review the recommendations in this and other related reports, and to determine which recommendations the CIPC should address. The High-Impact, Low-Frequency Implementation Task Force determined that the CIPC should continue its analysis of cyber attack trees and analyze issues relating to information sharing, security clearances, security metrics, and physical security guidelines. The CIPC established task forces for all of these issue areas, and most groups have completed their reviews and issued recommendations.

b. Security Readiness Program

NERC conducts SRP visits, which consist of visits to registered entities to focus on the sufficiency of industry implementation of the CIP Standards. An SRP visit both examines CIP Version 3 compliance in a retrospective review and helps registered entities address transitioning from CIP Version 3 to CIP Version 5 in a prospective view. While compliance with CIP Version 3 and its risk-based assessment methodology remains mandatory until March 31, 2016, many registered entities are concerned about how to transition their compliance and security efforts to Version 5 to meet the April 1, 2016, compliance deadline. Registered entities are exploring how to best manage the transition process to CIP Version 5 while remaining compliant with CIP Version 3. NERC invites Regional Entity representatives to participate in SRP discussions; however, no content from those discussions may be used during a subsequent audit or compliance action unless that content reveals an imminent threat to the BES. NERC staff,

Regional Entity representatives, and outside consultants sign non-disclosure agreements to ensure strict confidentiality of all discussions and materials.

c. Grid Security Conferences

In 2011, NERC hosted the first GridSecCon focusing on physical security and cybersecurity issues facing the electricity sub-sector. NERC has continued to hold these conferences annually to achieve the following objectives:

- Build on NERC's mission to ensure the reliability of the North American BPS through education and training;
- Discuss and provide solutions to emerging industrial control system security issues;
- Deliver expert analysis on social engineering and phishing attacks;
- Focus strategically on public-private partnerships; and
- Provide an update on ES-ISAC activities and issue a call for increased industry participation and communication.

Over 300 industry and government stakeholders attended the most recent GridSecCon in October 2013. More than 20 speakers led discussions focused on industry being transformational, strategic, and tactical in its approach to securing systems. Participants were asked to consider different information sharing techniques; determine if their organizations are resilient through self-assessments; test response activities through exercises; work to ensure that security is built into operations; and enhance the workforce by recruiting, training, and retaining individuals who can address these and other issues. Additionally, almost 200 stakeholders attended credentialed training sessions in cybersecurity and physical security.

d. Grid Security Exercises

In 2011, NERC hosted the first GridEx, which focused on analyzing industry's response to a physical and cybersecurity scenario. NERC now holds a biennial distributed play exercise and executive tabletop discussion to achieve the following:

- Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned;
- Review existing command, control, and communication plans and tools for NERC and its stakeholders;
- Identify potential improvements in cybersecurity and physical security plans, programs, and responder skills; and
- Explore senior leadership policy decisions and triggers in response to a coordinated cyber and physical event of national significance with long-term grid reliability issues.

Over 200 organizations participated in GridEx II, which took place November 13, 2014 through November 14, 2013. During the exercise, participants identified five key lessons learned:

- Information sharing has increased;
- NERC has improved ES-ISAC and BPSA coordination functions;
- Simultaneous cyber and physical attacks pose significant challenges;
- Industry continues to refine and enhance its all-hazard incidence response plans and protocols; and
- Industry and government information-sharing stakeholders can better inform incident response through coordination and consolidation of content.

GridEx II included an executive tabletop exercise involving about 30 participants, including electricity industry executives representing a broad cross-section of the industry and senior officials from the federal government. Participants considered a severe cyber and physical

attack scenario of national and international significance, and discussed the policy-level challenges that would need to be addressed by industry and government.

e. Electricity Sub-sector Coordinating Council

NERC established the Electricity Sub-sector Coordinating Council (ESCC) in 1998 at the request of the Department of Energy to foster and facilitate the coordination of sector-wide, policy-related activities and initiatives designed to improve the reliability and resilience of the Electricity Sub-sector, including physical and cyber infrastructure. In 2010, NERC restructured the ESCC to consist of industry senior executives with NERC's CEO as the ESCC chair. The ESCC provided advice to the NERC Board on policy-level matters related to critical infrastructure, developed a Critical Infrastructure Strategic Roadmap, and provided oversight on several NERC and industry initiatives to address HILF events and other critical infrastructure risks to the BPS.

In August 2013, the NERC Board approved a new ESCC charter, which amended, superseded, and terminated the existing charter. The new charter provides for a total of 30 CEO-level representatives, including members of the ESCC Steering Committee. NERC's CEO continues to serve on the ESCC and its Steering Committee. The transition formally recognized the significant increased CEO interest and participation on cybersecurity issues, focused industry association activities through an existing channel recognized by government agencies, and provided a unified industry framework upon which to build in response to President-issued orders and directives, such as EO-13636 and PPD-21.

2. ES-ISAC Tools and Activities

a. ES-ISAC Portal

The ES-ISAC has seen a tremendous leap in its user base since its inception in 1998, with

more reporting from organizations and more information sharing between members of industry. The ES-ISAC portal, which became functional in April 2012, is the industry's first and often primary interface with the ES-ISAC. The portal is continuously updated with technical and trend reports, watch lists, advanced sector information sharing tools, and other relevant resources. The portal receives "Indicators of Compromise" from various sources, including U.S. government departments and agencies, and NERC distributes this information to electricity sector entities. The portal allows the ES-ISAC to reach thousands of users and hundreds of organizations across industry to discuss and exchange security-related information. The ES-ISAC is concentrating its efforts on increasing the user base of this important portal. The success of this effort relies on the value of information available on the portal as well as the timeliness with which information reaches users. To achieve this goal, the ES-ISAC is enhancing portal capabilities to improve the ease of use and to improve analytic collaboration across the sub-sector.

Current capabilities of the portal include publishing alerts and other informational products, exchanging threat indicator information, and providing self-service access to portal users. Upgrades underway will increase flexibility to support additional functionality and capacity using a cloud-based, secure platform solution. The improved portal will facilitate direct data exchange with other ISACs and government partners. The portal will also support ES-ISAC analysts in their information analysis functions and tie the ES-ISAC analysts together with their counterparts in other sectors and in national laboratories. Finally, the portal will add private social media information sharing tools, automated access to enhanced cybersecurity information flows, and predictive analytics.

b. Analytics

The ES-ISAC has also improved its analytic capabilities by building out its operations

room to include data feeds from multiple sources, such as NERC's situation awareness monitoring tool, and procuring services that deliver cyber awareness information. As a result, the ES-ISAC is uniquely positioned to enhance grid and sector-level resilience by quickly evaluating and addressing potential cybersecurity impacts to BPS operations.

c. Industry and Government Coordination

The ES-ISAC was initiated to gather information from industry participants about security-related events, disturbances, and off-normal occurrences in the electricity sub-sector. The ES-ISAC shares that information with industry as a whole and with government partners. In turn, government entities provide information regarding risks, threats, and warnings to the ES-ISAC. The ES-ISAC adds analytic value to shared information and coordinates with other sectors. It is also responsible for developing industry and government products, including the NERC crisis action plan and the U.S. Department of Homeland Security incident response analysis. In addition, the ES-ISAC co-hosts annual cleared briefings to industry to ensure the electricity sub-sector maintains awareness of new and ongoing threats to the BPS.

Most recently, the ES-ISAC collaborated with the Department of Homeland Security, the Department of Energy, and the Federal Bureau of Investigation to host a series of briefings focused on tactics and tools of emerging cyber threat actors. In addition, in the wake of the April 16, 2013 Metcalf substation incident in California, the ES-ISAC worked with these agencies and other organizations and governmental partners to raise awareness of physical attack threats, to increase local, regional and federal security partnerships, and to support mitigation efforts. These briefings continued through the first quarter of 2014.

d. Cyber Risk Preparedness Assessments

The ES-ISAC conducts CRPAs to assess the cybersecurity capabilities of registered

entities through facilitated tabletop exercises. Conducting these assessments allows the ES-ISAC staff to gain a better understanding of industry capabilities, identify key sector level areas for improvement, and share best practices across industry. Through CRPA exercises, participants gain an improved understanding of their cybersecurity programs and capabilities. These exercises also help participants identify areas for improvement and enhance their abilities to respond to and recover from cybersecurity events. The CRPA also educates participants through defined deliverables and best practices. During 2013, the ES-ISAC incorporated elements of the Electricity Sub-sector Cybersecurity Capability Maturity Model program into the CRPA. Additionally, the ES-ISAC has developed a CRPA kit for entities to use in developing and running their own CRPAs. The kit allows more entities to leverage the CRPA methodology to enhance their preparedness. In February 2013, ES-ISAC staff hosted initial training and education sessions on the kit to accelerate adoption of the methodology across the sector and move the program towards self-sustainment within industry.

III. NERC CONTINUES TO MEET THE §39.3(b) CRITERIA

An explicit requirement for the five-year ERO performance assessment is that it include an explanation of how the ERO satisfies the requirements of 18 C.F.R. §39.3(b). Section 39.3(b) sets forth the requirements for certification as the ERO, which specify that the entity:

(1) Has the ability to develop and enforce, subject to 18 C.F.R. §39.7, Reliability Standards that provide for an adequate level of reliability of the BPS;[88] and

(2) Has established rules that:

(a) Assure its independence from users, owners and operators of the BPS while assuring fair stakeholder representation in the selection of its directors and balanced decisionmaking in any ERO committee or subordinate organizational structure;

[88] 18 C.F.R. §39.7 sets forth the Commission's regulations concerning the enforcement of Reliability Standards by the ERO, including provisions pertaining to the imposition of penalties for violations of Reliability Standards.

(b) Allocate equitably reasonable dues, fees, and charges among end users for all activities under Part 39;

(c) Provide fair and impartial procedures for enforcement of Reliability Standards through the imposition of penalties in accordance with 18 C.F.R. §39.7, including limitations on activities, functions, operations, or other appropriate sanctions or penalties;

(d) Provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards and otherwise exercising its duties; and

(e) Provide appropriate steps to gain recognition in Canada and Mexico.

Attachment 1 to this *Five-Year ERO Performance Assessment Report* shows in detail that NERC continues to satisfy the requirements of §39.3(b).

With respect to the requirements of §39.3(b)(1), NERC continues to have the ability to develop and enforce, subject to 18 C.F.R. §39.7, Reliability Standards that provide for an adequate level of reliability of the BPS. This requirement encompasses two distinct functions of the ERO: (i) the ability to develop reliability Standards that provide for an adequate level of reliability of the BPS, and (ii) the ability to enforce those Reliability Standards. NERC develops Reliability Standards pursuant to §300 of its ROP and its SPM, Appendix 3A to the ROP. These documents have been revised since NERC was certified as the ERO, including during the current assessment period, and the current versions of §300 and Appendix 3A have been approved by the Commission as ERO Rules. Further, NERC's SPM has been accredited by the ANSI as meeting ANSI's essential requirements for standards development. Moreover, as shown in detail in **Attachment 1**, NERC's Reliability Standards development process contains the essential attributes of the standards development process as set forth in prior Commission orders. As noted, during this assessment period, NERC has made improvements to its SPM, which the Commission has approved.

Further, NERC systematically manages the development of new Reliability Standards

and revisions to standards, in areas of highest need and importance, through its rolling three-year RSDP. The RSDP is revised annually and identifies and prioritizes Reliability Standards development projects in the immediate three-year time horizon, taking into account, among other information, perceived gaps in the Reliability Standards, proposals for closing those gaps, and timing priorities for standards development projects.

NERC enforces compliance with approved Reliability Standards through its CMEP, which is embodied in §400 and Appendix 4C of the ROP; its Organization Registration and Certification Program, which is embodied in §500 and Appendices 5A and 5B of the ROP; and its *Sanction Guidelines*, Appendix 4B of the ROP (all of the foregoing have been approved by the Commission as ERO Rules), as well as through its RDAs with the Regional Entities, which have also been approved by the Commission. Through the organization registration provisions of its ROP, NERC and the Regional Entities identify the users, owners, and operators of the BPS that are obligated to comply with Commission-approved Reliability Standards.

Monitoring and enforcement of compliance with Reliability Standards is conducted primarily by the eight Regional Entities pursuant to §401.4 of the ROP and the RDAs, subject to NERC oversight. Provisions of the ROP describe in detail the required attributes of Regional Entity compliance programs, including compliance program structure, resources and design. The controlling document for NERC's compliance monitoring and enforcement activities is the *Compliance Monitoring and Enforcement Program*, Appendix 4C to the ROP. Appendix 4C specifies compliance monitoring methods to be used and the detailed process steps for each method. Additionally, Appendix 4C specifies the process steps to be followed when a potential violation of a Reliability Standard by a registered entity is identified; as well as the actions required of the registered entity if it is found to be in violation of a Reliability Standard. The

Sanction Guidelines, which were significantly revised during this assessment period, specify the factors to be taken into account by the ERO in determining the financial penalty to be assessed for a violation of a Reliability Standard.

Pursuant to the RDAs, each Regional Entity has either adopted the NERC CMEP or a modified version of the CMEP as its compliance monitoring and enforcement program. Compliance monitoring and enforcement activities are further guided by the annual NERC and Regional Entity CMEP Implementation Plans (as described earlier, now combined into a single annual CMEP Implementation Plan document).

As detailed in **Attachment 1**, over this assessment period, NERC and the Regional Entities have continued to increase the resources devoted to compliance monitoring and enforcement activities. In their approved business plans and budgets for 2009, NERC and the Regional Entities provided for, collectively, 158.25 FTE staff and approximately $32.5 million of direct expenditures in their CMEPs. In their business plans and budgets for 2014, NERC and the Regional Entities provided for, collectively, 303.40 FTE staff and approximately $57.1 million of direct expenditures in their CMEPs.

With respect to the requirements of §39.3(b)(2)(i), NERC continues to have in place rules that assure its independence from users, owners, and operators of the BPS while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organizational structure. This criterion encompasses three distinct considerations: (i) independence of NERC from users, owners and operators of the BPS; (ii) fair stakeholder representation in the selection of NERC's directors (i.e., its trustees); and (iii) provision for balanced decision-making in any NERC committee or organizational structure.

As described in detail in **Attachment 1**, provisions of NERC's Commission-approved Bylaws,[89] along with several NERC policy documents[90] assures NERC's independence from users, owners, and operators of the BPS. Provisions of the NERC Bylaws also assure fair stakeholder representation in the selection of NERC's trustees. Finally, provisions of the NERC Bylaws and of §1300 of the ROP specify requirements for selection of members for and voting procedures on, NERC committees and sub-groups, that provide for balanced decision-making.

With respect to the requirements of §39.3(b)(2)(ii), NERC's Bylaws and §1102 of its ROP provide for equitable allocation of reasonable dues, fees and charges among end users for all of the ERO's statutory activities. Section 1102 provides for the assessments to recover NERC's approved funding requirements to be allocated among countries, regions, and load-serving entities in the North American BPS based on Net Energy for Load (NEL), except where direct assignment of costs to a specific country or region(s) is appropriate. The NEL-based allocation of the annual assessments to cover NERC's and the Regional Entities' annual funding requirements is provided to the Commission for approval in NERC's annual business plan and budget filing.

With respect to the requirements of §39.3(b)(2)(iii), NERC's rules also continue to provide fair and impartial procedures for enforcement of Reliability Standards through the imposition of penalties in accordance with 18 C.F.R. §39.7. These rules and procedures include §400 of the ROP; Appendix 4B, *Sanction Guidelines*, of the ROP; and Appendix 4C, the *Compliance Monitoring and Enforcement Program*, of the ROP, which includes the Hearing

[89] NERC's Bylaws are considered "ERO Rules." 18 C.F.R. §39.1.

[90] NERC's *Governance Guidelines* is available at: http://www.nerc.com/gov/Annual%20Reports/Governance%20Guidelines%20-%20Approved%202.6.14.pdf; NERC's *Employee Code of Conduct* is available at*:* http://www.nerc.com/gov/Annual%20Reports/Employee-Code-of-Conduct.pdf; and NERC's *Policy on Reporting Complaints Regarding Accounting and Code of Conduct Matters*, is available at: http://www.nerc.com/gov/Annual%20Reports/Whistleblower_Policy_Final-May%202014.pdf.

Procedures to be followed by Regional Entity Hearing Bodies in presiding over and ruling on disputes raised by a registered entity with respect to a Regional Entity's proposed finding of a violation or the proposed amount of penalty for a violation. All of these provisions have been approved by the Commission as ERO Rules. All of these provisions have been extensively revised, and the revisions approved by the Commission, during this assessment period. **Attachment 1** to this report describes in detail NERC's rules and procedures for the determination and imposition of penalties for violations of Reliability Standards and how they comply with the requirements of §215(e)(6) of the FPA and §39.3(b)(2)(iii) and §39.7 of the Commission's regulations.

With respect to the requirements of §39.3(b)(2)(iv), NERC continues to maintain rules that provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards and otherwise exercising its duties. NERC's Bylaws require that Reliability Standards be developed through an open, transparent, and public process that provides for reasonable notice and opportunity for public comment, due process, and balancing of interests; and that participation in the Reliability Standards development process shall not be limited to NERC members but rather shall be open to all persons and entities with an interest in the reliable operation of the BPS. As noted in the discussion of the first §39.3(b)(1) criterion, above, NERC's Reliability Standards development process is embodied in §300 and Appendix 3A of the ROP. The ROP specify "Essential Principles for the Development of Reliability Standards," which include openness, transparency, consensus-building, fair balance of interest, due process, and timeliness. With respect to balance of interests, the ROP provide for balloting on proposed Reliability Standards to be conducted on the basis of a broad set of ten industry segments, which collectively encompass persons and

entities with an interest in the reliable operation of the BPS. The detailed process steps for developing and approving new or revised Reliability Standards, set forth in the NERC SPM, is based on the procedures of the ANSI and other standards-setting organizations in the U.S. and Canada.

In addition to its rules and procedures for the development of Reliability Standards, NERC's rules provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in the exercise of NERC's other duties, including in the appointment and election of trustees, meetings of trustees, approving amendments to the Bylaws and amendments to the ROP, selection of members for and the conduct of business by committees and subgroups, development and approval of annual business plans and budgets, and the conduct of compliance monitoring and enforcement activities.

Finally, with respect to the requirements of §39.3(b)(2)(v), NERC continues to engage in substantial efforts to gain and maintain recognition as the ERO in Canada and Mexico. One of NERC's corporate purposes, as set forth in its Certificate of Incorporation, is "to act as the electric reliability organization for the United States as certified by the Federal Energy Regulatory Commission and for Canada and Mexico as recognized by applicable government and regulatory authorities in Canada and Mexico, all pursuant to law." In Canada, where by its Constitution the regulation of electricity is primarily within the jurisdiction of each province rather than the national government, NERC's activities to obtain and maintain recognition are conducted on a province-by-province basis. **Attachment 1** details NERC's efforts and accomplishments in the provinces of Alberta, British Columbia, Manitoba, New Brunswick, Nova Scotia, Ontario, Québec, and Saskatchewan, as well as at the National Energy Board. Depending on the particular circumstances of each province, NERC has gained recognition

through statutes or other provisions of provincial law, or through a memorandum of understanding with appropriate entities in the province. As described in **Attachment 1**, NERC's efforts in each province fall into three areas: recognition of NERC Reliability Standards; provisions for sharing of information on issues related to compliance with NERC Reliability Standards; and monitoring and enforcement of compliance with Reliability Standards.

With respect to Mexico, the Comisión Federal de Electricidad (CFE), through the Centro Nacional de Control de Energia (CENACE), and the Area de Control Baja California (ACBC), have entered into a membership and operating agreement (MOA) with WECC. The MOA provides for WECC to assist CENACE and ACBC in monitoring compliance by Designated Entities (the Mexican equivalent of U.S. registered entities) with Mexico Reliability Standards for Baja California, Mexico. CENACE has approved ten Mexico Reliability Standards. Pursuant to the MOA, WECC monitors compliance with Mexico Reliability Standards, but does not have enforcement or registration (designation) authority for CFE. WECC provides compliance monitoring, reviews proposed and completed mitigation plans, and provides assessment recommendations with respect to alleged violations.

In summary, and as shown in detail in **Attachment 1** to this *Five-Year ERO Performance Assessment Report*, the Commission should find that NERC continues to satisfy the requirements of 18 C.F.R. §39.3(b).

IV. REGIONAL ENTITY PERFORMANCE AND EFFECTIVENESS CONTINUES TO IMPROVE

Attachment 3 provides NERC's evaluation of the performance of the Regional Entities in carrying out their delegated authorities and responsibilities during the assessment period.

The Commission's regulation specifying the required contents of the ERO's periodic performance assessment reports states that the performance assessment must include, among

other subjects, the ERO's evaluation of the effectiveness of each Regional Entity and recommendations by the ERO for improvement of the Regional Entity's performance of delegated functions.[91] In its September 16, 2010 Order on NERC's *Three-Year ERO Performance Assessment Report*, the Commission stated that future assessments should include, among other things, separate sections addressing each Regional Entity's satisfaction of statutory and regulatory criteria.[92]

In this five-year performance assessment, NERC organized its evaluation of the Regional Entities' performance based on their principal delegated authorities and responsibilities under the RDAs and the NERC ROP. These segments also correspond to the programmatic organization structures generally followed by NERC and the Regional Entities:

- Regional Reliability Standards Development (**Attachment 3**, §I)
- Compliance Monitoring and Enforcement (**Attachment 3**, §II)
  - Organization Registration and Certification (**Attachment 3**, §II.A)
  - Compliance Monitoring[93] (**Attachment 3**, §II.B)
  - Compliance Investigations (**Attachment 3**, §II.C)
  - Compliance Enforcement (**Attachment 3**, §II.D)
- Reliability Assessments (**Attachment 3**, §III)
- Reliability Risk Management (Situation Awareness and Event Analysis) (**Attachment 3**, §IV)
- Business Planning and Budgeting, Finance and Accounting (**Attachment 3**, §V).

[91] 18 C.F.R. §39.3(c)(1)(iii).

[92] *North American Electric Reliability Corporation, Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010), at P 36.

[93] The evaluation of the Regional Entities' performance in Compliance Monitoring includes evaluation of their efforts in providing training, education, and outreach to registered entities and other industry stakeholders on compliance-related matters.

To evaluate the Regional Entities' performance during the assessment period, NERC believed it to be important to use assessment criteria that were well-known to the Regional Entities and that were established at the beginning of, or early in, the assessment period. Accordingly, NERC has generally used the Regional Entities' obligations and responsibilities under the RDAs and the NERC ROP as the basis for evaluating the Regional Entities' performance or as the source for more specific assessment criteria. Although, during the assessment period, the RDAs were significantly revised through a collaborative process among NERC and the Regional Entities, with the revised RDAs going into effect on January 1, 2011 (i.e., approximately 18 months into the assessment period), the Regional Entities' fundamental delegated authorities and responsibilities under the RDAs were not changed in the revised RDAs.

Further, in evaluating the Regional Entities' performance during the assessment period, NERC placed greater emphasis on each Regional Entity's performance during the latter half of the assessment period rather than earlier in the assessment period. Although the assessment is intended to cover the entire five-year period, NERC views the success of a Regional Entity in improving its programs over the course of the period – particularly where improvements have been implemented in response to specific comments, criticisms or recommendations from NERC, the Commission, or the Regional Entity's stakeholders – as especially important to the evaluation. The quality of a Regional Entity's programs and performance as of the end of the assessment period is much more important to the objectives of this review than is a historical review of the Regional Entity's programs and performance at the start of, or in the early portion of, the assessment period. Further, a Regional Entity's willingness to cooperate in implementing new ERO Enterprise initiatives and improvements intended to improve the reliability of the BPS and increase consistency and efficiency across the ERO Enterprise is particularly important to

the evaluation. This focus on improvements, responses to comments and recommendations, and the state of the Regional Entities' programs and performance as of the end of the assessment period, is consistent with the emphasis in the Commission's applicable regulation on comments and recommendations from stakeholders for improvements and the Regional Entity's responses to such comments and recommendations.

In this evaluation of the Regional Entities' performance in the various program areas, NERC has also provided a significant amount of description of NERC's oversight activities of the Regional Entities. NERC's oversight of the Regional Entities' programs and activities provides important context for the performance assessment because, for almost all of the Regional Entities' delegated authorities and responsibilities, NERC's oversight is frequent, and in some areas, virtually continuous. NERC's oversight activities are a significant component of the informational and observational basis for NERC's evaluation of the Regional Entities' performance. Moreover, although this *Five-Year ERO Performance Assessment Report* is appropriately required by the Commission's regulations, it is NERC's ongoing oversight of the Regional Entities' activities that gives NERC both an up-to-date basis for evaluation, and a continuous platform to evaluate the need for and make recommendations for improvements, both in the performance of discrete tasks by individual Regional Entities and on a programmatic, ERO Enterprise-wide basis.

V. NERC HAS SURVEYED STAKEHOLDERS FOR COMMENTS AND SUGGESTIONS FOR IMPROVEMENTS

One of the components of the ERO's periodic assessment reports as specified in 18 C.F.R. §39.3(c) is that the assessment include "[r]ecommendations by Regional Entities, users, owners, and operators of the Bulk-Power System, and other interested parties for improvement of the ERO's operations, activities, oversight and procedures, and the ERO's response to such

recommendations."[94] NERC has addressed this component by soliciting comments and recommendations through (i) a stakeholder survey conducted for purposes of the five-year ERO performance assessment, and (ii) posting drafts of the five-year performance assessment report for stakeholder comment.

The stakeholder survey was initiated on October 31, 2013, near the end of the five-year assessment period, when NERC distributed an online survey seeking stakeholder responses. The survey contained 36 specific questions on topics relating to (i) Reliability Standards development; (ii) compliance monitoring; (iii) compliance enforcement; (iv) organization registration and certification; (v) reliability assessment; (vi) performance analysis and metrics; (vii) training, education and personnel certification; (viii) event analysis; (ix) critical infrastructure protection; (x) shareholder communications, public relations and information technology; (xi) business plan and budget; and (xii) independence and stakeholder input. Stakeholders were invited to respond to the questions using a numerical scoring system and, more importantly, to provide free-form narrative comments on the topics covered by the survey. A total of 326 registered entity responses were received. The respondents were located in all Regional Entities, ranging from a low of 23 responses to a high of 97 responses from respondents located within particular Regional Entities. **Attachment 4** provides the text of the questions that were asked in the survey and also provides summary data on the numbers and distribution of respondents.

With respect to posting drafts of the five-year performance assessment for stakeholder comment, on March 3, 2014, NERC posted a draft statement of its activities and accomplishments during the five-year assessment period, as well as drafts of the Regional

[94] 18 C.F.R. §39.3(c)(1)(ii).

Entities' self-assessments, on the NERC website for stakeholder comment. Subsequently, on June 17, 2014, NERC posted a draft of the *Five-Year ERO Performance Assessment Report* and attachments on its website for stakeholder comment.[95]

Attachment 4 to this *Five-Year ERO Performance Assessment Report* provides the content specified by 18 C.F.R. §39.3(c)(1)(ii). As noted above, **Attachment 4** provides the questions included in the stakeholder survey, reports the average scores from the responses, and provides summary information on the number and distribution of respondents.[96] More importantly, **Attachment 4** provides the significant narrative comments and recommendations submitted by stakeholders and NERC's responses to those comments. To focus on the key issues, questions and recommendations posed or raised by commenters, and for simplicity, NERC has attempted to summarize the comments and to combine them where appropriate, in order to report the gist of the comments and recommendations. The comments are organized in **Attachment 4** in table format by subject matter area: Reliability Standards; Compliance Operations; Enforcement; Registration and Certification; Reliability Assessment & Performance Analysis Metrics; Training, Education and Personnel Certification; Event Analysis; Critical Infrastructure Protection; Stakeholder Communications, Public Relations and IT; and Business Plan and Budget. A separate table, organized into the same topical sections, provides a summary of key stakeholder comments of the Regional Entities. For each stakeholder comment reported in one of the two tables, NERC has provided in the table, opposite the comment, (i) where applicable, the section or sections of the *Overview of NERC Activities and Accomplishments in*

[95] The June 17, 2014 posted draft of **Attachment 4** was incomplete, since completion of that attachment required receipt of the stakeholder comments in response to the posting of the draft report and the preparation of responses to the comments for inclusion in the attachment.

[96] Some of the questions by their nature, pertained only to NERC, while others of the questions pertained to both NERC and the Regional Entities. Average scores are reported for NERC or for NERC and the individual Regional Entities as applicable to the particular survey questions.

the Five-Year Period or of an attachment to this report in which the subject matter of the comment is addressed, and (ii) for most of the comments, a brief narrative response to the comment as well. NERC submits that the tables provided in **Attachment 4** show that NERC has responded to and addressed, or is in the process of responding to and addressing, the key stakeholder comments and recommendations provided in connection with the development of this *Five-Year ERO Performance Assessment Report*.

VI. NERC HAS MADE SUBSTANTIAL PROGRESS IN COMPLETING ACTIONS ON ITEMS IN THE COMMISSION'S ORDER ON THE *THREE-YEAR ERO PERFORMANCE ASSESSMENT REPORT*

NERC's *Three-Year ERO Performance Assessment Report*, filed on July 20, 2009, identified and listed a number of actions to be taken in response to comments received from stakeholders as part of the three-year assessment process.[97] Additionally, the Commission's Order on the three-year ERO performance assessment, issued on September 16, 2010, identified a number of areas for improvement.[98] NERC was directed to submit an informational report to the Commission within six months addressing the directives, concerns and requests for information and/or feasibility reports discussed in the Order. NERC filed the Informational Report on March 16, 2011.[99] NERC was able to report either completion or significant progress with respect to many of the items listed in the Commission's Order.

As part of this *Five-Year ERO Performance Assessment Report*, NERC is providing a further report on its progress in addressing the directives, concerns and requests for information

[97] These actions were listed in Appendix A to **Attachment 1** of the *Three-Year ERO Performance Assessment Report*.

[98] *Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010). Appendix A to that Order provided an "Index of Directives" in the Order.

[99] *Informational Filing of the North American Electric Reliability Corporation in Response to the Federal Energy Regulatory Commission's September 16, 2010 Order*, filed March 16, 2011 in Docket Nos. RR09-7-000 and AD10-14-000.

and/or feasibility reports discussed in the Commission's Order on the three-year ERO performance assessment that were not discussed in the March 2011 informational filing. This information is provided in a chart format in **Attachment 5** to this report. As noted in the chart provided as **Attachment 5**, NERC's actions in connection with a number of the items are also discussed in the body of this five-year assessment report.

VII. NERC HAS A VISION AND PLAN FOR IMPROVING COORDINATED OPERATIONS ACROSS THE ERO ENTERPRISE TO REACH THE END STATE OF A HIGHLY EFFECTIVE AND EFFICIENT ERO ENTERPRISE

As described above and in the Attachments to this report, since being certified as the ERO in 2006 and, in particular, during this five-year assessment period, NERC has made substantial progress and recorded significant accomplishments in structuring the ERO Enterprise organization and improving the reliability of the BPS. Despite the achievements to date, the nine-entity structure of the ERO Enterprise, NERC and the eight Regional Entities, is not without certain challenges and risks. Going forward, NERC needs and intends to focus attention on the actions necessary to reach an end-state of a fully-integrated ERO Enterprise that can exercise effective and well-coordinated reliability oversight that mitigates reliability risks to the BPS. Achieving the end-state of a fully integrated ERO Enterprise entails creating greater clarity about the allocation of roles and responsibilities between NERC and the Regional Entities, achieving improved coordination of goals, and establishing more uniform work processes, tools and performance across the ERO Enterprise.

NERC has a vision and plan for achieving this end state of a fully integrated, highly effective and efficient ERO Enterprise. This vision and plan are described in detail in **Attachment 6** to this report.

Reaching this end state necessitates adherence to certain fundamental principles. The ERO Enterprise must:

- Apply technical expertise that is focused on risks to the BPS and important reliability outcomes;
- Achieve results and methods across the ERO Enterprise that are predictable, consistent and timely;
- Share common goals, objectives and measures of success;
- Build relationships that are founded on candor and mutual trust, openness and cooperation;
- Apply collaborative decision-making;
- Ensure efficiencies while minimizing duplication and any activities not affecting reliability outcomes; and
- Avoid undue burden, discrimination, or capriciousness for affected regulated entities.

As detailed in **Attachment 6**, NERC's plan for achieving excellence in the oversight and execution of its statutory functions and in the mitigation of BPS reliability risks requires actions in five areas relating to the relationships and allocations of responsibilities between and among NERC and the Regional Entities:

(1) Clarifying roles and responsibilities. A clear understanding of the roles and responsibilities of NERC and the Regional Entities is required, as well as a clear set of expectations in the execution of the activities performed across the ERO Enterprise. This in turn will necessitate ERO Enterprise program oversight that includes the following essential oversight elements to be provided by NERC in consultation with the Regional Entities:

- An overall program design indicating the program purpose and goals, and design of controls to manage risks;
- Documentation of common methods, practices and procedures to be applied in the program, and performance expectations for each;
- Statements of necessary qualifications of key positions within the Regional Entities for conducting certain statutory activities, and identification of any standards for critical positions;

- Training of NERC and Regional Entity staff for select positions in the conduct of delegated functions;

- A documented and transparent set of process controls and measures to assure delegated responsibilities are properly completed, and to assess the effectiveness of the delegated activities in managing BPS and ERO Enterprise risk; and

- Periodic reporting of results and feedback to Regional Entities on trends and providing opportunities to enhance consistency and effectiveness of results.

To improve the delegation process, it will be important that NERC and the Regional Entities work together to update and refine the RDAs, due for renewal as of January 1, 2016, to provide a clearer division of responsibilities, both related to the division of performance of statutory functions and oversight of those functions, and to provide effective mechanisms to resolve routine differences.

(2) Coordinating strategic planning. NERC and the Regional Entities have collaboratively made significant progress in developing a shared, rolling three-year strategic plan for the ERO Enterprise. However, adoption of the ERO Enterprise goals and objectives into business plans at all of the Regional Entities has varied. In May 2014, the NERC Board approved the 2014 performance metrics. These performance metrics will be used to assess the overall effectiveness of the ERO Enterprise in addressing risk to the BPS, achieving reliability results, assuring Reliability Standards and compliance effectiveness and improving risk mitigation and program execution. They include four overarching metrics focused on overall effectiveness in addressing BPS risks and improving reliability. They also include a number of supporting measures that assess the effectiveness of the key operational elements of the ERO Enterprise. The intent is to report the results of these metrics on an ERO Enterprise-wide basis, and also as applicable, distinguish results for NERC and individual Regional Entities.[100]

[100] *See* http://www.nerc.com/gov/Annual%20Reports/ERO%20Enterprise%20Strategic%20Plan%202014-2017%20and%20Performance%20Metrics.pdf.

(3) Coordinating operational decision-making. The ERO Enterprise model depends on successful delegation of activities, but also requires coordination of operational decisions that arise in the execution of these activities. To date, coordination of policy and directional decisions has been achieved through: (i) coordination meetings between NERC and Regional Entity CEOs, which have become more routinized in recent years and include an agreed-upon protocol for reaching consensus decisions; and (ii) the activities of approximately two dozen working groups collaborating across various functional areas of the ERO Enterprise. The preferred approach going forward is to proactively establish a more collaborative model and recognize that Regional Entity staffs for most functions typically have valuable first-hand experience in implementing the activities on the front lines with registered entities. However, success depends on collaboration that results in timely and effective decisions that all entities in the enterprise agree to implement, and the avoidance of unilateral decision-making that steers portions of the ERO Enterprise into alternative methods and practices for delegated functions.

(4) Achieving consistency. Achieving consistency of methods, practices, procedures and tools has been a challenge throughout the history of the ERO Enterprise. At the outset, given a lack of common processes and procedures from NERC, Regional Entities developed their own methods, practices, procedures and tools. While there has been significant progress made, through the leadership and working groups referred to in the preceding paragraph, in addressing substantive differences, there remain significant variations in methods, practices, procedures and tools across NERC and the eight Regional Entities. Today, the biggest challenge in addressing consistency is gaining common agreement on processes and procedures with the backdrop of years of institutionalized differences among NERC and the Regional Entities.

The ultimate success of the ERO Enterprise depends on there being one compliance

program, one enforcement program, one event analysis program, and so forth. Registered entities will have greater confidence and trust in the ERO Enterprise if they believe regulatory oversight is not subject to arbitrary variations and possible discrimination from one region to the next. Outcomes will be more predictable and consistent if each statutory function is conducted in a unified fashion across the ERO Enterprise. Outcomes will also be more readily measurable to demonstrate the reliability impacts and benefits of the ERO Enterprise programs. In the long term, after the transition from legacy approaches, there will be significant efficiencies.

This transition requires the development of a core set of common methods, practices, procedures, and tools, which NERC is principally responsible to produce, working in collaboration with the Regional Entities. Consistency does not necessarily require identical internal procedures at each Regional Entity, and some flexibility must be maintained to allow for progress through innovation. However, consistency does mean that the approach, methods and practices are the same across the ERO Enterprise and that outcomes produced from application of the local and regional expertise and judgment of the Regional Entity staffs are fair, reasonable and without bias. In other words, the goal is consistent methods, practices, procedures and tools that deliver fair and reasonable outcomes. The move to greater consistency must occur under the close scrutiny of the ERO Executive Management Group, with accountability for progress to the NERC and Regional Entity boards, and all entities must be prepared to adopt changes to drive to more consistent methods, practices, procedures and tools.

(5) Coordinating external and cross-ERO Enterprise communications. Communications are important to the effectiveness of the ERO Enterprise. Communications can help set expectations for registered entities and stakeholders and demonstrate a common and consistent approach for regulators and the public. To facilitate effective communications across the ERO

Enterprise, in May 2013 the NERC Board initiated a practice of meeting twice yearly as a group with all the chairs and vice-chairs of the Regional Entities, with a portion of these meetings conducted with the NERC and Regional Entity CEOs also present. Additionally, a NERC-Regional Entity communications working group has been active for several years, coordinating consistent messaging across the ERO Enterprise. Further, NERC and the Regional Entities have coordinated outreach to FERC Commissioners and staff and to Canadian governments. However, although efforts to coordinate key messages and direction have been successful, areas for improvement remain. Thus, going forward, this area requires further attention to arrive at a desired end-state for the ERO Enterprise.

To reach the desired end-state for the ERO Enterprise in the five areas described above, NERC intends to focus on the following eleven action items:

(1) NERC includes in its review of Regional Entity business plans adequacy of resources and alignment of the plans for achieving delegated function objectives and outcomes described in the three-year plan.

(2) NERC, in collaboration with the Regional Entities:

(a) Develops a comprehensive overarching design and set of controls, reporting requirements, and feedback mechanisms for each delegated statutory function, including the essential oversight elements listed above;

(b) Re-evaluates its organizational structure and leadership qualifications necessary to provide effective design and oversight of statutory activities;

(c) Identifies functional qualifications for select delegated activities, such as auditors and investigators;

(d) Adopts risk-based approaches to monitoring performance of delegated functions and providing effective feedback and coaching to continuously improve overall ERO Enterprise performance; and

(e) Re-evaluates the ERO working group structure to enhance effectiveness.

(3) Regional Entities:

(a) Work in a coordinated fashion to support NERC in the development of comprehensive functional program designs and controls;

(b) Adapt existing regional programs for delegated functions to conform with emerging program designs provided by NERC; and

(c) Ensure Regional Entity staffs meet qualification and training requirements.

(4) NERC and the Regional Entities develop and maintain a joint three-year strategic plan for the ERO Enterprise describing the goals and deliverables for statutory functions and this plan should guide the development of each Regional Entity's annual business plans. Additional goals and deliverables that are complimentary or supplemental to the strategic plan may be developed at the Regional Entity level.

(5) NERC and the Regional Entities transparently report results, based on a common set of performance measures focused on BPS reliability outcomes and effectiveness of the statutory programs. These measures are considered in the performance management program at each entity.

(6) ERO Enterprise senior leadership continues maturing the collaborative decision-making process and setting the direction and policy for the enterprise as well as driving this collaboration throughout the ERO Enterprise organizations.

(7) All nine ERO entities abide by the joint enterprise decisions of the ERO Enterprise senior leadership, and the NERC CEO should make final determinations if consensus is not otherwise achievable for an action that is required.

(8) With NERC leading, the ERO Enterprise develops a core set of methods, practices, procedures, and tools to support unified implementation of the major statutory functions of NERC. In doing so, the ERO Enterprise commits to put the best talent available throughout the collective organizations to achieve this goal.

(9) The ERO Enterprise senior leadership develops ERO Enterprise Information Technology applications, where appropriate, to support common processes, to enhance the efficiency and effectiveness of Regional Entities' practices, to increase the consistency of the interface with registered entities, and to facilitate NERC's oversight function.

(10) All parties of the ERO Enterprise, including leadership and staffs, convey shared and consistent messages from the enterprise perspective and communicate together to minimize messages emphasizing self-importance or uniqueness.

(11) NERC and Regional Entities continue the joint board coordination to ensure oversight and accountability of all elements of the enterprise and should continue to refine and expand coordinated outreach to government entities in the U.S. and Canada, stakeholders, and media.

VIII. CONCLUSION

As detailed in this *Five-Year ERO Performance Report* and its Attachments, NERC has reached an important level of development in identifying, understanding and addressing reliability risks to the BPS. NERC has implemented targeted initiatives that benefit the electric industry and its customers through improved BPS reliability. These initiatives also allow NERC to measure and be accountable for the effectiveness and value of the investments made by the industry to enhance and maintain reliability. NERC's approach allows it to target results around specific issues that benefit the industry and its customers through improved BPS reliability. Further, NERC's programs are continuing to evolve, thereby sharpening its focus on reliability and accountability through risk-based processes.

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 1

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

DISCUSSION OF HOW NERC MEETS THE ERO CERTIFICATION CRITERIA OF 18 C.F.R. §39.3(b)

JULY 21, 2014

Attachment 1

TABLE OF CONTENTS

I. DISCUSSION OF HOW NERC MEETS THE ERO CERTIFICATION CRITERIA OF 18 C.F.R. §39.3(b) 1

A. Criterion 1 - The ERO has the ability to develop and enforce, pursuant to 18 C.F.R. §39.7, Reliability Standards that provide for an adequate level of reliability of the BPS. 1

B. Criterion 2 - The ERO has established rules that assure its independence of users, owners and operators of the BPS while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committees and subordinate organizational structure. 17

C. Criterion 3 - The ERO has established rules that allocate equitably reasonably equitable dues, fees and charges among end users for all statutory activities. 23

D. Criterion 4 - The ERO has established rules that provide fair and impartial procedures for enforcement of Reliability Standards through the imposition of penalties in accordance with 18 C.F.R. §39.7, including limitations on activities, operations, or other appropriate sanctions or penalties. 24

E. Criterion 5 - The ERO has established rules that provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards, and otherwise exercising its duties. 28

F. Criterion 6 - The ERO has established rules that provide appropriate steps to gain recognition in Canada and Mexico. 34

I. DISCUSSION OF HOW NERC MEETS THE ERO CERTIFICATION CRITERIA OF 18 C.F.R. §39.3(b)

A. Criterion 1 - The ERO has the ability to develop and enforce, pursuant to 18 C.F.R. §39.7, Reliability Standards that provide for an adequate level of reliability of the BPS.

This criterion encompasses two distinct functions of the ERO: (i) the ability to develop Reliability Standards that provide for an adequate level of reliability of the bulk power system (BPS); and (ii) the ability to enforce those Reliability Standards.

Development of Reliability Standards

NERC develops Reliability Standards pursuant to §300 of its Rules of Procedure (ROP) and its *Standard Processes Manual* (SPM), Appendix 3A to the ROP, both of which have been approved by the Commission as ERO Rules.[1] In addition to having been approved by the Commission, the SPM has been accredited by the American National Standards Institute (ANSI) as meeting ANSI's essential requirements for standards development.

The overall purpose of NERC's Reliability Standards development process, as stated in §301 of the NERC ROP, is to develop and maintain Reliability Standards that apply to BPS owners, operators, and users and that enable NERC and the Regional Entities to measure the reliability performance of the owners, operators, and users and to hold them accountable for the reliable operation of the BPS. Section 301 of the ROP requires that Reliability Standards developed by NERC must be technically excellent, timely, just, reasonable, not unduly discriminatory or preferential, in the public interest, and consistent with other applicable standards of governmental authorities.[2]

In Order No. 672 and the *ERO Certification Order*, the Commission stated that the ERO's Reliability Standards development process must ensure that each Reliability Standard is technically sound; that its operational specifications are designed to achieve a valuable reliability goal; that the standard is clear and unambiguous regarding what is required and who is required to comply; and that there be clear criteria to measure whether an entity is in compliance with the Reliability Standard, so that enforcement can be applied in a consistent and non-preferential manner.[3] Consistent with these requirements, §302 of the ROP specifies the essential attributes of

[1] Sections 304 and 308.1 of the ROP specify that "NERC shall develop Reliability Standards in accordance with the NERC *Standard Processes Manual*, which is incorporated into these Rules of Procedure as Appendix 3A." The current version of the SPM is version 3 which became effective June 26, 2013.

[2] Section 304 of the ROP sets forth NERC's "Essential Principles for the Development of Reliability Standards." These principles, which include openness, transparency, consensus-building, fair balance of interests, due process and timeliness, are discussed under criterion 5, below.

[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 (2006), at PP 258, 262, 325, 327; *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (*ERO Certification Order*), at PP 239, 241.

technically excellent Reliability Standards to be developed by NERC.[4] These essential attributes include:[5]

1. **Applicability** — Each Reliability Standard shall clearly identify the functional classes of entities responsible for complying with the Reliability Standards, with any specific additions or exceptions noted.[6]

2. **Reliability Objectives** — Each Reliability Standard must have a clear statement of purpose that describes how the Reliability Standard contributes to the reliability of the BPS. Section 302.2 of the ROP lists the general objectives for the BPS that provide a foundation for determining the specific objective(s) of each Reliability Standard:[7]

    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.

    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.

---

[4] In the *ERO Certification Order*, the Commission recognized that NERC's proposed ROP provided that the characteristics for technical excellence of a Reliability Standard must be met for a proposed Reliability Standard to be approved. *ERO Certification Order* at P 235.

[5] The descriptions of the essential attributes that follow are summaries, not direct quotes from §302.

[6] The functional classes of entities, or reliability functions, have been developed through NERC's functional model of the BPS, and are defined in its: (i) *Glossary of Terms Used in NERC Reliability Standards*, and (ii) *Statement of Compliance Registry Criteria* which is incorporated into the ROP as Appendix 5B. Currently, the functional classes of entities are: Balancing Authorities (BAs), Distribution Providers, Generator Operators (GOPs), Generator Owners (GOs), Interchange Authorities, Load-Serving Entities, Planning Authorities, Purchasing-Selling Entities, Reliability Coordinators (RCs), Resource Planners, Reserve Sharing Groups, Transmission Operators (TOPs), Transmission Owners (TOs), Transmission Planners, and Transmission Service Providers.

[7] In the *ERO Certification Order*, the Commission recognized that NERC's proposed rules provided that the purpose of a Reliability Standard, or its reliability objective, should derive from one or more of these eight general objectives. *ERO Certification Order* at P 236.

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 responsibility and authority to implement actions.

2.7. **Wide-Area View** — The reliability of 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 BPS, consistent with good utility practices and the public interest. Each Requirement is not a "lowest common denominator" compromise, but instead shall achieve an objective that is the best approach for BPS 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 the 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 field.

6. **Completeness** — Reliability Standards shall be complete and self-contained. The Reliability 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 and other ERO and Regional Entity compliance documents, the consequences of violating a Reliability Standard are clearly presented to the entities responsible for complying with the Reliability 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 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.[8]

In the *ERO Certification Order*, the Commission concluded that by specifying the eight general objectives for which a Reliability Standard must be intended, and by incorporating other requirements for Reliability Standards development into the essential attributes of technically excellent Reliability Standards, NERC's ROP satisfied the requirements of Order No. 672 for the ERO's Reliability Standards development process.[9]

The NERC SPM also specifies the performance elements of a Reliability Standard.[10] The requirement that each Reliability Standard contain these elements applies a systematic discipline in the development and revision of standards, in order to produce standards that are measurable, enforceable, and consistent. The SPM allows for a clear statement of the purpose, requirements, measures, and compliance elements associated with each standard. The performance elements of a Reliability Standard, as specified in the SPM §2.5, are as follows:

- Title: A brief, descriptive phrase identifying the topic of the Reliability Standard.
- Number: A unique identification number assigned in accordance with a published classification system to facilitate tracking and reference to the Reliability Standards.
- Purpose: The reliability outcome achieved through compliance with the Requirements of the Reliability Standard.
- Applicability: Identified which entities are assigned reliability requirements. The specific Functional Entities and Facilities to which the Reliability Standard applies.
- Effective Dates: Identification of the date or pre-conditions determining when each Requirement becomes effective in each jurisdiction.
- Requirement: An explicit statement that identifies the Functional Entity responsible, the action or outcome that must be achieved, any conditions achieving

[8] In furtherance of the essential attribute of "Consistent Terminology," NERC has developed and maintains the *Glossary of Terms Used in NERC Reliability Standards*, containing definitions of terms that are used in one or more Reliability Standards.

[9] *ERO Certification Order* at PP 239, 241.

[10] SPM at pp. 6-9.

the action or outcome, and the reliability-related benefit of the action or outcome. Each Requirement shall be a statement for which compliance is mandatory.

- Compliance Elements: Elements to aid in the administration of ERO compliance monitoring and enforcement responsibilities.

- Measure: Provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.

- Violation Risk Factors and Violation Severity Levels: Violation risk factors (VRFs) and violation severity levels (VSLs) are used as factors when determining the size of a penalty or sanction associated with the violation of a requirement in an approved Reliability Standard. Each requirement in each Reliability Standard has an associated VRF and a set of VSLs. VRFs and VSLs are developed by the drafting team, working with NERC staff, at the same time as the associated Reliability Standard, but are not part of the Reliability Standard. The Board of Trustees is responsible for approving VRFs and VSLs.

    - Violation Risk Factors: VRFs identify the potential reliability significance of noncompliance with each requirement. Each requirement is assigned a VRF in accordance with the last approved set of VRF criteria.
    - Violation Severity Levels: VSLs define the degree to which compliance with a requirement was not achieved. Each requirement shall have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs. Each requirement is assigned one or more VSLs in accordance with the latest approved set of VSL criteria.

- Version History: The version history is provided for informational purposes and lists information regarding prior versions of Reliability Standards.

- Variance: A Requirement (to be applied in the place of the continent-wide Requirement) that is applicable to a specific geographic area or to a specific set of registered entities.

- Compliance Enforcement Authority: The entity that is responsible for assessing performance or outcomes to determine if an entity is compliant with the associated Reliability Standard. The Compliance Enforcement Authority [(CEA)] will be NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

- Application Guidelines: Guidelines to support the implementation of the associated Reliability Standard.

- Procedures: Procedures to support implementation of the associated Reliability Standard.

The NERC SPM sets forth the detailed process steps for the development and approval of a new Reliability Standard or a revision to an existing standard; the SPM also sets forth the detailed roles of the different persons and groups in in the process.[11] Under the ROP and the SPM, the key groups involved in development of a proposed new Reliability Standard or revision to an existing standard are: (i) the NERC Standards Committee; (ii) the standards authorization request (SAR) drafting team; (iii) the standard drafting team; and (iv) the Registered Ballot Body (RBB).

The Standards Committee is an elected body comprised of two members from each segment of the RBB.[12] The Standards Committee, with the assistance and facilitation of the professional staff of the NERC Reliability Standards development program, oversees the overall standards development process. The Standards Committee ensures that standard development teams have the technical resources and capabilities required to develop technically sound standards that will gain industry support. Among other things, the Standards Committee determines whether SARs submitted by interested persons and entities should be pursued for development, and it appoints members to SAR drafting teams and standard drafting teams.[13] A SAR drafting team is a team of technical experts that, among other responsibilities, assists in refining a SAR and considers and responds to comments.[14] The standard drafting team is a team of technical experts that develops the details of the proposed new or revised Reliability Standard, analyzes results of field tests of the standard (if applicable), and considers and responds to comments.[15] The RBB, which is open to any person or entity and is organized by industry segments, votes on the adoption or rejection of proposed Reliability Standards or revisions to existing standards.[16]

The SPM also specifies roles in the standards development process for the NERC Reliability Standards staff, which is led by the director of standards.[17] Staff provides support to the Standards Committee in managing the Reliability Standards processes and in supporting the work of all drafting teams. More specifically, staff is responsible for ensuring that development

[11] The ROP also provides for an expedited standards development process in the event an applicable governmental authority directs the development of a Reliability Standard within a certain timeframe. This process is described in §309.3 of the ROP.

[12] The segment organization of the RBB is set forth in detail in the *Registered Ballot Body Criteria,* Appendix 3D to the ROP.

[13] *See* SPM at §§3.4 and 3.6.

[14] *See* SPM at §4.2.

[15] SPM at §4.3.

[16] ROP §305; SPM at §§3.2 and 4.7-4.15 (pp. 10, 20-24). Following successful balloting by the ballot pool, a proposed standard is submitted to the NERC Board of Trustees for approval, and if approved by the Board, is filed with the Commission for approval in accordance with §215(d) of the FPA and 18 C.F.R. §39.5. NERC Bylaws, Article IX, §1; ROP §§308.2, 308.3, and 309; and SPM at §§4.0 and 4.16.

[17] SPM at §3.5; *see also* ROP §307.

and revision of standards is in accordance with the SPM, works to ensure the integrity of the Reliability Standards development process and the consistency of quality and completeness of NERC Reliability Standards, and facilitates all steps in the standards development process.

The NERC standards development process relies on the legal and technical expertise provided by the industry experts comprising the SAR drafting teams and standard drafting teams, the technical and administrative assistance provided by the NERC standards process managers and the NERC standards process staff, and the overall oversight and direction of the Standards Committee. Thus, the NERC standards development process ensures that the essential attributes of technically excellent Reliability Standards, including the accomplishment of one of the eight general reliability objectives specified in §§302.2.1 through 302.2.8 of the ROP, are represented in each Reliability Standard that is developed or revised through the process and submitted to the NERC Board of Trustees and, ultimately, to the Commission for approval.

As demonstrated by the table below, NERC has invested significant resources to support its Reliability Standards program. Since 2009, NERC has increased its budgeted resources (direct expenses) for the Reliability Standards program by approximately 143.10% percent from 2009 to 2014:[18]

Year	**Amount**	**Increase over 2009**
2009:	$3,599,454	N/A
2010:	$4,189,050	116.38%
2011:	$4,863,139	135.11%
2012:	$5,307,943	147.47%
2013:	$5,134,738	142.65%
2014:	$5,150,854	143.10%

Leveraging its resources and standards development process, NERC has developed and submitted to the Commission a total of 293 continent-wide Reliability Standards that, as of December 1, 2013, have been approved by the Commission pursuant to §215(d) of the Federal Power Act (FPA) and 18 C.F.R. §39.5 to be mandatory and enforceable. NERC has also approved and submitted to the Commission, and the Commission has approved, a total of 23 regional Reliability Standards as of December 1, 2013. NERC's success to date in developing Reliability Standards that the Commission subsequently approved as mandatory and enforceable

[18] *See December 2008 Budget Compliance Filing* Attachment 1 at 1; *NERC 2010 Business Plan and Budget* at 36 and Attachment 2 at 15; *NERC 2011 Business Plan and Budget* at 35 and Attachment 2 at 27; *NERC 2012 Business Plan and Budget* at 37 and Attachment 2 at 26; *NERC 2013 Business Plan and Budget* at 42 and Attachment 2 at 34; *NERC 2014 Business Plan and Budget* at 43 and Attachment 2 at 29. The amounts cited are direct expenses only and do not include NERC indirect expenses (General and Administrative, Information Technology, Legal and Regulatory, Human Resources, and Finance and Accounting) allocated to the Reliability Standards Program Area.

demonstrates that NERC has, and has exercised, the ability to develop Reliability Standards that provide for an adequate level of reliability of the BPS.

Further, the continent-wide Reliability Standards that have been developed by NERC and approved by the Commission cover the full range of reliability objectives specified in §302 of the NERC ROP:

- Resource and Demand Balancing (25 approved standards)
- Communications (3 approved standards)
- Critical Infrastructure Protection (55 approved standards)
- Emergency Preparedness and Operations (21 approved standards)
- Facilities Design, Connections and Maintenance (21 approved standards)
- Interchange Scheduling and Coordination (18 approved standards)
- Interconnection Reliability Operations and Coordination (29 approved standards)
- Modeling, Data, and Analysis (33 approved standards)
- Nuclear (2 approved standards)
- Personnel Performance, Training and Qualifications (9 approved standards)
- Protection and Control (29 approved standards)
- Transmission Operations (21 approved standards)
- Transmission Planning (15 approved standards)
- Voltage and Reactive Power (12 approved standards)

In accordance with the template and performance elements specified in the SPM, each approved Reliability Standard contains the following clearly-identified sections and subsections: (i) Applicability — stating the title of the standard, its identification number, its purpose, the reliability functional entities to which it is applicable, and its effective date; (ii) Requirements; (iii) Measures; (iv) Compliance — stating the entity responsible for monitoring compliance; the compliance monitoring period and reset timeframe; data retention requirements for the registered entities; and the levels of noncompliance for specified types of violations of the standard; and (v) Regional Differences, if any.

The inclusion of these elements helps to ensure that Reliability Standards clearly state who is responsible for compliance with a Reliability Standard, the Requirements for which compliance is required, and how compliance may be measured by the CEA.

NERC systematically manages the development of new standards and revisions to standards, in areas of highest need and importance, through its rolling three-year *Reliability Standards Development Plan*. The *Reliability Standards Development Plan* identifies and prioritizes the Reliability Standards development projects in the immediate three-year time horizon. The three-year *Reliability Standards Development Plan* is revised annually, based on input from NERC staff, the standard drafting teams, the NERC technical committees and subgroups, other industry participants, and government authorities. The annual *Reliability Standards Development Plan* revision considers: (i) perceived gaps in NERC's Reliability Standards and proposals for closing those gaps; (ii) timing priorities of the projects in the *Reliability Standards Development Plan* and recommendations for adjusting the timing of individual projects; and (iii) potential new projects for development of new standards or revisions to existing standards. The three-year rolling *Reliability Standards Development Plan*, as revised each year, is submitted to the NERC Board of Trustees for approval and then filed with the Commission for information. The *Reliability Standards Development Plan 2014-2016* was approved by the NERC Board of Trustees on November 7, 2013 and continues the approach set forth in the *Reliability Standards Development Plan 2013-2015*; namely, to facilitate the transformation of NERC Reliability Standards to "steady-state," a set of standards that are stable, clear, concise, high-quality, results-based, and technically sound, while emphasizing addressing outstanding regulatory directives and the retirement of Reliability Standards that do little to promote reliability.[19]

Enforcement of Reliability Standards

NERC's program for monitoring and enforcing compliance with Commission-approved Reliability Standards is implemented through its *Compliance Monitoring and Enforcement Program* (CMEP) (§400 and Appendix 4C to the ROP), its Organization Registration and Certification Programs (§500 to the ROP), its *Sanction Guidelines* (Appendix 4B to the ROP), and its delegation agreements with the eight Regional Entities.[20]

Section 6(a) of NERC's delegation agreements with the Regional Entities specifies that the Regional Entity shall enforce Reliability Standards within its geographic boundaries through the compliance enforcement program set forth in Exhibit D to the agreement, and that the Regional Entity's compliance monitoring and enforcement program meets all applicable requirements of the FPA, Commission Order No. 672, and the Commission's regulations, including, *inter alia*, the requirement for an audit program pursuant to 18 C.F.R. §39.7(a), the assessment of penalties pursuant to 18 C.F.R. §39.7(c) through 39.7(g), and the requirements for due process. Additionally, §6(f) of the delegation agreements requires the Regional Entity to maintain the

[19] The *Reliability Standards Development Plan 2014-2016*, along with previous versions of the plan, are available at: http://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsDevelopmentPlan.aspx.

[20] The delegation agreements were originally approved by the Commission in an order issued April 19, 2007 (*Order Accepting ERO Compliance Filing, Accepting ERO/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans*, 119 FERC ¶ 61,060 (2007)), subject to various compliance requirements, which have been addressed in subsequent compliance filings and Commission orders. The currently-effective delegation agreements will expire on December 31, 2015.

capability to conduct investigations of potential violations of Reliability Standards and to conduct such investigations in a confidential manner. It also requires the Regional Entity to maintain a program of proactive enforcement audits, including procedures for spot checks of self-reported compliance and periodic audits of all registered entities.

Through the NERC Organization Registration and Certification Programs, NERC and the Regional Entities have identified users, owners, and operators of the BPS that are obligated to comply with Commission-approved NERC Reliability Standards.[21] Section 500 of the NERC ROP governs the registration of users, owners, and operators of the BPS as responsible for compliance with the requirements of Reliability Standards that are applicable to the reliability function for which the entity is registered. The purpose of the NERC Compliance Registry, established pursuant to §501 of the ROP, is to clearly identify those entities that are responsible for compliance with Reliability Standards. The NERC Compliance Registry identifies the reliability functions to be performed by each organization responsible for meeting the requirements of Reliability Standards. Organizations listed in the NERC Compliance Registry are responsible for knowing the contents of, and complying with, Reliability Standards applicable to the reliability function(s) for which the entity is registered.[22] The criteria upon which users, owners and operators of the BPS will be registered for one or more reliability functions are specified in §501 of the ROP and in NERC's FERC-approved *Statement of Compliance Registry Criteria* (Appendix 5B to the ROP). The purpose of the *Organization Registration and Certification Manual* (Appendix 5A) is twofold: (i) to define the process utilized in the Organization Registration Program by identifying which functional entities must register as owners, operators, and users of the BPS for compliance with Reliability Standards; and (ii) to define the process utilized in the Organization Certification Program for certifying the following entities: RC, BA, and TOP.

Typically, a user, owner or operator of the BPS is identified, in the first instance, for placement on the NERC Compliance Registry by the Regional Entity in whose territory the user, owner or operator is located. Upon the entity being notified by NERC that it is being placed on the NERC Compliance Registry, the entity may challenge its inclusion on the NERC Compliance Registry by filing a written objection with NERC.[23] Challenges to inclusion on the NERC Compliance Registry are heard and decided by the NERC Board of Trustees Compliance Committee (BOTCC). If the entity is not satisfied with the decision of the BOTCC, the entity may appeal the registration determination to the Commission.[24] NERC may remove a registered entity from the NERC Compliance Registry for one or more of the reliability functions for which the

[21] Section 215(b)(2) of the FPA requires all users, owners and operators of the BPS to comply with Reliability Standards approved by the Commission. Similarly, the Commission's regulations at 18 C.F.R. §39.2 and §40.2 require all users, owners, and operators of the BPS to comply with applicable Reliability Standards and applicable rules of the ERO and Regional Entities approved by the Commission.

[22] ROP §501. The current categories of reliability functional entities are listed in ROP Appendix 5B, *Statement of Compliance Registry Criteria*. *See also supra* n. 6.

[23] A user, owner, or operator of the BPS may be listed on the NERC Compliance Registry for several reliability functions. A registered entity may challenge its listing for one or more of the reliability functions for which it has been registered while accepting its listing for other reliability function(s).

[24] The registration, challenge, and appeal process described in this paragraph is set forth in §501.1.3 of the ROP.

entity is listed, based on changed circumstances. As of December 31, 2013, there were 1,920 organizations listed on the NERC Compliance Registry, registered for 4,794 reliability functions.

Monitoring and enforcement of compliance with Reliability Standards is conducted primarily by the eight NERC Regional Entities, pursuant to §401.4 of the NERC ROP and the delegation agreements between NERC and the Regional Entities. Each Regional Entity is responsible for compliance monitoring and enforcement activities within its regional footprint.[25] The ROP provide for NERC to take responsibility for CMEP activities where a Regional Entity is unable to perform those functions, as well as to be responsible for overseeing the CMEP activities of the Regional Entities.[26] Section 403 of the ROP describes in detail the required attributes of Regional Entity compliance programs, covering compliance program structure, compliance program resources, and compliance program design. Section 403 emphasizes the requirement that the Regional Entity's governance of its compliance program, and its compliance program staff, be independent.[27] Each Regional Entity must develop a Regional Entity Compliance Enforcement Implementation Plan that identifies the Reliability Standards to be actively monitored by the Regional Entity (both those required by NERC and any additional Reliability Standards the Regional Entity proposes to monitor), and how the identified Reliability Standards will be monitored, evaluated, reported, sanctioned, and appealed.[28] These plans must be developed on an annual basis and submitted to NERC for approval. In its annual Implementation Plan, each Regional Entity must also report to NERC how the Regional Entity carried out its delegated compliance enforcement authority in the previous year, the effectiveness of its CMEP, and changes expected to correct any identified deficiencies.[29]

NERC is required to conduct an audit, at least once every five years, to evaluate how each Regional Entity implements the NERC CMEP.[30] The evaluation is based on the ROP including the NERC CMEP, the delegation agreement with the Regional Entity, the approved Regional Entity annual CMEP Implementation Plans, the required CMEP attributes, and the CMEP procedures. NERC must provide its evaluations to the Commission and other appropriate ERO

[25] ROP §401.4.

[26] ROP §§401.5, 402, and 404. The Commission has also approved the practice of one Regional Entity entering into an agreement with another Regional Entity to administer the compliance processes in the NERC CMEP with respect to the Regional Entities' registered functions. *See*, e.g., *Order Conditionally Accepting Compliance Monitoring and Enforcement Program Agreements and Revised Delegation Agreements, and Ordering Compliance Filing*, 132 FERC ¶ 61,024 (2010).

[27] ROP §§403.1 and 403.6.

[28] ROP §§402.1.1.1 and 403.16.

[29] ROP §403.16.

[30] ROP §402.1.1.3.

governmental authorities to demonstrate the effectiveness of each Regional Entity in compliance monitoring and enforcement.[31]

NERC has also conducted spot checks of different aspects of the Regional Entities' implementation of the CMEPs in 2013 and 2014. In 2013, NERC conducted a spot check of Regional Entity dismissal procedures. NERC also conducted a spot check of Regional Entity processes and procedures relating to settlement agreements and notices of confirmed violation. In 2014, NERC plans to conduct a spot check of Regional Entity processes regarding mitigation plans. These spot checks are in addition to NERC's ongoing spot check of issues filed pursuant to NERC's Find, Fix, Track and Report (FFT) program.

The controlling document for NERC's compliance monitoring and enforcement activities is the NERC CMEP, Appendix 4C to the ROP. Pursuant to Exhibit D to its delegation agreement with NERC, each Regional Entity has either adopted the NERC CMEP or a modified version of the CMEP; in the latter case, the modified CMEP, or an enumeration of any deviations in the Regional Entity's CMEP from the uniform CMEP, is included in Exhibit D to the Regional Entity's delegation agreement. All CMEPs have been approved by the Commission.[32]

The NERC CMEP (as well as each of the modified Regional Entity CMEPs) provides for seven compliance monitoring methods: (i) audits of registered entities for compliance with Reliability Standards;[33] (ii) self-certifications by registered entities of their compliance with standards;[34] (iii) spot checks of registered entities' compliance with Reliability Standards;[35] (iv) compliance investigations (CIs), which may be conducted and led by the Regional Entity or by NERC;[36] (v) self-reports by registered entities of violations of Reliability Standards;[37] (vi) periodic

[31] ROP §402.1.3. The audit procedure for NERC's audits of the Regional Entity CMEPs is contained in *Audit of Regional Entity Compliance Programs*, Appendix 4A to the ROP.

[32] The Commission initially approved the NERC CMEP and modified CMEPs adopted by certain Regional Entities in their respective delegation agreements, subject to various compliance requirements, in its Order issued April 19, 2007. *Order Accepting ERO Compliance Filing, Accepting ERO/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans*, 119 FERC ¶ 61,060 (2007). Subsequent Commission orders have approved modifications to the NERC CMEP and Regional Entity CMEPs (both modifications in response to Commission directives and modifications initiated by NERC and/or Regional Entities). *See*, e.g., *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); *Order Conditionally Accepting Compliance Monitoring and Enforcement Program Agreements and Revised Delegation Agreements, and Ordering Compliance Filings*, 132 FERC ¶ 61,024 (2010); *Order Conditionally Approving Revisions to North American Electric Reliability Corporation Rules of Procedure*, 141 FERC ¶ 61,241 (2012).

[33] CMEP §3.1.

[34] CMEP §3.2.

[35] CMEP §3.3.

[36] CMEP §3.4.

[37] CMEP §3.5.

data submittals by registered entities as requested by the CEA;[38] and (vii) investigation of complaints.[39] The NERC CMEP sets forth detailed process steps for each of the seven compliance monitoring methods, including requirements for the results of the processes to be reported by the Regional Entity to NERC and ultimately to the Commission. The NERC CMEP provides for due process for a registered entity by including provisions that address avoidance of conflicts of interest,[40] preservation of confidentiality,[41] provision of notice, and opportunities to respond.[42]

As specified by §4.1 of the NERC CMEP, NERC develops and posts an annual CMEP Implementation Plan each year. The annual NERC CMEP Implementation Plan specifies, among other information, the Reliability Standards to be actively monitored during the upcoming year and the compliance process(es) to be used by the CEAs to monitor each Reliability Standard. The annual NERC CMEP Implementation Plan is used by the Regional Entities in developing their individual annual regional Compliance Enforcement Program Implementation Plans.

The NERC CMEP also specifies the processes to be followed when an alleged violation of a Reliability Standard by a registered entity is identified,[43] including notification to the registered entity of an alleged violation and the required contents of the notice;[44] the registered entity's response to the notification of alleged violation;[45] the opportunity for the registered entity to obtain a hearing on the alleged violation and/or proposed penalty or sanction before the CEA hearing

[38] CMEP §3.6. The CEA is the entity (either NERC or the Regional Entity, as applicable) responsible for monitoring and enforcing the registered entity's compliance with Reliability Standards. CMEP §1.1.7.

[39] CMEP §3.7.

[40] For example, the registered entity is notified in advance of a compliance audit as to the members of the audit team (who are required to be free of conflicts of interest) and their backgrounds and is given the opportunity to object to individual members of the audit team on grounds of a conflict of interest or other circumstance that could interfere with the team member's impartial performance of his or her duties. *See* CMEP §3.1.5. Similar notice and opportunity to object is provided with respect to spot checking teams (*id.* at §3.3.1) and CI teams (*id.* at §3.4.1). In addition, §6 of the NERC-Regional Entity delegation agreements requires the Regional Entity to maintain a conflict of interest policy that assures the integrity of its compliance enforcement program and the independence of the compliance program staff from those subject to enforcement actions.

[41] CMEP §§2.0 and 9.3. In addition, §6 of the NERC-Regional Entity delegation agreements specifies that each violation or alleged violation of a Reliability Standard shall be treated as nonpublic until the matter is filed with the Commission as a notice of penalty or resolved by an admission that the owner, operator, or user of the BPS violated a Reliability Standard or by a settlement or other negotiated disposition.

[42] For example, the CEA must notify the registered entity in advance of a compliance audit as to the Reliability Standards to be covered by the audit, and must provide a pre-audit questionnaire to the registered entity at least two months before commencement of the audit. NERC uniform CMEP §3.1.1. At the conclusion of the audit, the compliance audit team is required to provide a draft audit report to the registered entity for comment. *Id.* §3.1.6. Similarly, in the spot check and periodic data submittal processes, the CEA is required to provide its draft assessment of compliance to the registered entity for comment. *Id.* §3.3.1 and §3.6.1.

[43] CMEP §5.0.

[44] CMEP §§5.1 and 5.3.

[45] CMEP §5.4.

body;[46] the process the registered entity may engage in to negotiate a settlement with the CEA;[47] the registered entity's right to appeal a hearing body decision to NERC;[48] and the process for reporting a penalty or sanction to the Commission for confirmation.[49]

The NERC CMEP requires that a registered entity found to be in violation of a Reliability Standard must file a mitigation plan with the CEA to correct the violation, or a description of how the violation has been mitigated.[50] The NERC CMEP describes the required contents of the registered entity's proposed mitigation plan;[51] the processes for submittal of the proposed mitigation plan by the Regional Entity[52] and for review and acceptance or rejection of the proposed mitigation plan by the Regional Entity and review and approval or disapproval by NERC (and, in the latter event, modification of the mitigation plan by the registered entity);[53] the timetable for completion of an accepted mitigation plan;[54] and the process for completion and confirmation by the CEA of implementation of the registered entity's mitigation plan.[55] Key components required by the NERC CMEP to be in any mitigation plan are the registered entity's action plans to correct the violation(s) and to prevent recurrence.[56]

Additionally, the NERC CMEP provides the procedure for the CEA to issue a remedial action directive to a registered entity.[57] A remedial action directive may be issued, when immediately necessary to protect the reliability of the BPS from an imminent threat, to a registered entity the CEA believes is committing or has committed a violation of a Reliability Standard. The remedial action directive may include, but is not limited to, specifying operating or planning

---

[46] CMEP §5.5 and Attachment 2, *Hearing Procedures*. The *Hearing Procedures* set forth the detailed procedures for the hearing to be conducted before the CEA hearing body should a registered entity dispute a notice of alleged violation, proposed penalty or sanction, proposed mitigation plan, or a remedial action directive.

[47] CMEP §5.6.

[48] CMEP §5.7. The NERC appeal process is addressed in §§408 and 409 of the ROP.

[49] CMEP §5.9.

[50] CMEP §6.1.

[51] CMEP §6.2.

[52] CMEP §6.4.

[53] CMEP §6.5.

[54] CMEP §6.3.

[55] CMEP §6.6.

[56] CMEP §6.2.

[57] CMEP §7.0. A remedial action directive is "[a]n action (other than a [p]enalty or sanction) required by a Compliance Enforcement Authority that (1) is to bring a [r]egistered [e]ntity 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." CMEP §1.1.27.

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 the registered entity to cease an activity that may constitute a violation of a Reliability Standard.[58]

As a key component of the enforcement of compliance with mandatory Reliability Standards, a violation of a standard can result in the imposition of a financial penalty or other penalty or sanction on the registered entity. NERC has established, and is applying, rules and procedures for determining the amount of financial penalties, or other penalties or sanctions, to be imposed on registered entities for violations of Reliability Standards. These rules and procedures are embodied in the NERC *Sanction Guidelines*, Appendix 4B to the ROP. The *Sanction Guidelines* must be followed by the Regional Entities in the implementation of their CMEPs.[59] Penalties and sanctions must bear a reasonable relation to the seriousness of the violation and take into consideration timely remedial efforts by the registered entity.[60] NERC's rules and procedures for determining appropriate penalties and sanctions for violations of Reliability Standards are discussed in greater detail under criterion 4.[61]

In order to carry out their responsibilities to monitor and enforce compliance with Reliability Standards, NERC and the Regional Entities, over the period from 2009 to date, have developed substantial professional staffs for, and are devoting substantial resources to, their CMEP and Organization Registration Programs. The following table shows the direct expenses and the numbers of full-time equivalent (FTE) staff budgeted by NERC and each Regional Entity in 2009 and in 2014.[62]

[58] CMEP §7.0.

[59] ROP §§403.14 and 407.

[60] ROP §401.7.

[61] The ERO has established rules that provide fair and impartial procedures for enforcement of Reliability Standards through the imposition of penalties in accordance with 18 C.F.R. §39.7, including limitations on activities, operations, or other appropriate sanctions or penalties.

[62] *See NERC 2009 Business Plan and Budget; December 2008 Budget Compliance Filing; NERC 2014 Business Plan and Budget.* The amounts cited are direct expenses only and do not include NERC indirect expenses (General and Administrative, Information Technology, Legal and Regulatory, Human Resources, and Finance and Accounting) allocated to the Compliance Monitoring and Enforcement and Organization Registration and Certification Program Area.

Regional Entity	2009 Budgeted FTEs	2009 Budgeted Direct Expense ($)
NERC	35.50	7,358,536
FRCC	9.10	1,991,643
MRO	10.00	2,071,510
NPCC	9.00	2,095,204
ReliabilityFirst	23.00	5,099,328
SERC	21.50	4,805,617
SPP RE	6.00	1,283,653
Texas RE	14.15	1,628,935
WECC	30.00	6,165,303
Totals	**158.25**	**32,499,729**

Regional Entity	2014 Budgeted FTEs	2014 Budgeted Direct Expense ($)
NERC	41.28	7,902,272
FRCC	19.26	4,281,909
MRO	21.26	3,864,192
NPCC	16.00	5,080,485
ReliabilityFirst	43.00	9,788,246
SERC	42.50	7,389,556
SPP RE	22.10	4,258,217
Texas RE	40.00	5,991,654
WECC	58.00	8,592,053
Totals	**303.40**	**57,148,584**

As demonstrated in the tables above, the number of budgeted FTEs increased approximately 191.72% across NERC and the Regional Entities from 2009 to 2014, while the budgeted direct expense increased by nearly 175.84%.

In addition to their compliance program staffs, NERC and a number of the Regional Entities have also made use of consultants and contractors to assist in compliance audits, CIs, and other compliance monitoring and enforcement activities, and to provide subject matter expertise as needed to supplement the expertise of their staffs.

As explained in the *Joint Regional Entity Self-Assessment*, included in **Attachment 2** of this *Five-Year ERO Performance Report*, the Regional Entities describe how they execute their delegated function of enforcing Reliability Standards. Also in **Attachment 2**, the Regional Entities describe their compliance monitoring activities during the 2009 through 2013 assessment period.

NERC has participated in some Regional Entity compliance audits and will continue to do so as an observer to observe the performance of audits by the Regional Entities and to help ensure

consistent implementation and application of the CMEP and consistent application of the requirements of standards across the Regional Entities.

The foregoing discussion amply demonstrates that NERC has developed and is implementing the ability to develop and enforce Reliability Standards that provide for an adequate level of reliability of the BPS.

B. Criterion 2 - The ERO has established rules that assure its independence of users, owners and operators of the BPS while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organizational structure.

This criterion encompasses three distinct considerations: (i) independence of NERC from users, owners and operators of the BPS; (ii) fair stakeholder representation in the selection of NERC's directors (trustees); and (iii) provision for balanced decision-making in any NERC committee or subordinate organizational structure.

Independence of Users, Owners, and Operators of the BPS

NERC's Bylaws provide that NERC's business and affairs shall be managed by a Board of Trustees.[63] The Bylaws provide that the Board of Trustees shall consist of ten independent trustees plus the President of NERC.[64] The Bylaws define "independent trustee" as follows:

> An independent trustee is a person (i) who is not an officer or employee of the Corporation [i.e., NERC], a member or an officer, director, or employee of a member of the Corporation, or an officer, director, or employee of any entity that would reasonably be perceived as having a direct financial interest in the outcome of board decisions and (ii) who does not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a trustee. Provided, that upon initial election to the board, an independent trustee shall within ten (10) days terminate any employee, officer, or director position that conflicts with this subparagraph and shall within sixty (60) days terminate any financial interest or other relationship that conflicts with this subparagraph, and prior to such termination shall not participate in discussion of or voting on any matter involving the entity of which the trustee is an employee, officer or director or in which the trustee has the financial interest or other relationship giving rise to the conflict.[65]

[63] NERC Bylaws Article III, §1.

[64] NERC Bylaws Article III, §1. On October 14, 2009, the Commission approved in a letter order, in Docket No. RR09-8-000, new §§1a and 1b that allows the Board of Trustees to exercise the authority to increase the number of trustees from eleven to twelve, and decrease from twelve to eleven, respectively.

[65] NERC Bylaws Article III, §3a. The last sentence of §3a, providing for brief time periods for a newly-elected trustee to terminate any employment, officer or director position or financial interest or other relationship that would prevent

In the *ERO Certification Order*, the Commission found that the NERC Bylaws definition of "independent trustee" was sufficient to provide for independence from users, owners and operators of the BPS, subject to one clarification.[66]

Thus, a NERC trustee cannot be an officer, director, or employee of a member of NERC nor of any other entity that would be perceived as having a direct financial interest in the outcome of board decisions, and may not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a trustee. The "responsibilities of a trustee" include, among other things, voting on: (i) board approval of proposed Reliability Standards;[67] (ii) board approval of the NERC ROP and amendments to the ROP;[68] and (iii) board approval of NERC and Regional Entity budgets.[69] Committees of the NERC Board, such as the BOTCC, are responsible for decisions such as hearing and deciding challenges by a user, owner or operator of the BPS to placement of the entity on the NERC Compliance Registry,[70] hearing and deciding appeals from a Regional Entity hearing body decision on a registered entity's challenge to a notice of alleged violation of a Reliability Standard and/or proposed penalty or sanction,[71] and approving the imposition of penalties or other sanctions for violations of Reliability Standards on registered entities, including by settlements.

In addition, the NERC *Conflict of Interest and Business Ethics Policy for Trustees, Officers and Employees* specifies that NERC Representatives "shall avoid and refrain from involvement in or situations where there is actually a conflict of interest (Conflict). A Conflict arises where the NERC Representative's personal financial interest is significantly affected or may reasonably appear to be significantly affected by his or her actions or decisions in his or her capacity at

---

the trustee from being independent, is a 2008 amendment to the Bylaws that was approved by the Commission by a letter order issued October 7, 2008 in Docket No. RR08-5-000.

[66] *ERO Certification Order*, 116 FERC ¶61,062 at P 42. The clarification is that the definition prohibits an independent trustee from having a relationship that would interfere with his or her exercise of independent judgment in carrying out the responsibilities of a trustee, regardless of whether he or she is an officer, director, or employee of an entity with an interest in the outcome of NERC Board of Trustees decisions. NERC confirmed this clarification in a compliance filing dated September 18, 2006, and made a modification, consistent with the clarification, to the definition of "independent trustee" in its Bylaws. *Compliance Filing of the North American Electric Reliability Council and the North American Electric Reliability Corporation Addressing Governance Issues and Request for Expedited Treatment*, Docket No. RR06-1, filed September 18, 2006 (*NERC ERO Governance Compliance Filing*) at 3-4.

[67] NERC Bylaws Article IX, §1; ROP §308.2.

[68] NERC Bylaws Article XI, §2; ROP §1402.

[69] NERC Bylaws Article XIII, §§2, 3, 4, and 5; ROP §1101. Each of the matters just listed, upon being approved by the NERC Board of Trustees, must then be submitted to the Commission for approval or confirmation. Sections 215(d) and (f) of the FPA and 18 C.F.R. §§39.4(b), (c), and (d), and 39.5.

[70] ROP §501.1.3.

[71] ROP §409.

NERC." NERC's *Process for Reviewing Conflicts of Interes*t outlines how potential conflicts of interest of the independent trustees, officers and employees are evaluated beginning in December of each calendar year.[72] The *NERC Employee Code of Conduct* mandates an "employee's faithful pursuit of the interests of NERC rather than his or her own financial or other interests of another person or organization." Finally, NERC's *Policy on Reporting Complaints Regarding Accounting and Code of Conduct Matters* prohibits retaliation against any NERC employee who lodges a code of conduct complaint about fraud, unethical business conduct, questionable accounting, problems with internal accounting controls, financial reporting or auditing, violations of NERC's codes of conduct for trustees and employees, or violations of law occurring within NERC.

Fair Stakeholder Representation in the Selection of NERC's Trustees

NERC's Bylaws provide for fair stakeholder representation in the selection of NERC's trustees. Candidates for election as a trustee are selected by a nominating committee. The nominating committee is appointed annually (or more frequently if needed in the event of a special election to fill a board vacancy) by the board. The nominating committee is to consist of those independent trustees whose terms do not expire during the current year and such number of other persons with such qualifications as the board shall specify, including at least three members of the NERC Member Representatives Committee (MRC).[73] The procedures to be followed by the nominating committee must include a means of permitting members of NERC to recommend to the nominating committee candidates for consideration as nominees for independent trustees.[74] NERC's Bylaws specify that the nominating committee "shall also endeavor to nominate candidates for election to the board consistent with the objectives that the board as an entity reflects expertise in the areas of technical electric operations and reliability, legal, market, financial, and regulatory matters, and familiarity with regional system operations issues; and reflects geographic diversity."[75]

NERC's Bylaws provide that the independent trustees shall be elected by the NERC MRC, from nominees proposed by the nominating committee. To be elected an independent trustee, a nominee must receive the affirmative vote of two-thirds of the members of the MRC.[76] The MRC

[72] On February 6, 2014, the NERC Board of Trustees approved *Governance Guidelines*, which consolidated NERC's (i) *Conflict of Interest and Business Ethics Policy for Trustees, Officers and Employees* and (ii) *Process for Reviewing Conflicts of Interest* into a single cohesive document.

[73] NERC Bylaws Article III, §5.

[74] NERC Bylaws Article III, §5.

[75] NERC Bylaws Article III, §5.

[76] NERC Bylaws Article III, §6. The NERC Bylaws also require that the number of trustees from Canada shall not be less than the percentage of the net energy for load (NEL) of Canada to the total NEL of the United States and Canada, times eleven (or twelve if the number of trustees has been increased to twelve pursuant to NERC Bylaws Article III, §1a), rounded up to the nearest whole number, with the management trustee (i.e., the president of NERC) counted as a trustee from Canada if he or she is a Canadian citizen. NERC Bylaws Article III, §2a. In the *ERO Certification Order*, the Commission approved this provision as "adequately provid[ing] for an international ERO," stating that "appropriate country representation helps to ensure that the ERO is truly international in addressing Bulk-

is comprised of representatives from the various sectors of the NERC membership.[77] As specified by Article II, §4 of the NERC Bylaws, the sectors of the NERC membership are: (i) investor-owned utilities; (ii) state/municipal utilities; (iii) cooperative utilities; (iv) federal or provincial utilities/federal power marketing administrations; (v) transmission-dependent utilities; (vi) merchant electricity generators; (vii) electricity marketers; (viii) large end-use electricity customers; (ix) small end-use electricity customers; (x) independent system operators/regional transmission organizations; (xi) regional entities; and (xii) government representatives.[78] The composition of the MRC, as specified in Article VIII, §2 of the NERC Bylaws, is as follows:

(1) Two representatives from each sector except the government representative sector and the regional entity sector;

(2) Two voting representatives from the regional entity sector, with the remaining members of that sector being non-voting members of the MRC;[79]

(3) The chairman and vice chairman of the MRC;[80]

(4) Any additional Canadian representatives as are selected pursuant to Article VIII, §4 of the Bylaws;[81] and

---

Power System reliability and considering the concerns of stakeholders in each of the three countries." *ERO Certification Order* at P 47.

[77] Membership in NERC is voluntary and is open to any person or entity that has an interest in the reliable operation of the North American BPS, registers as a member, and complies with the other conditions and obligations of membership specified in the NERC Bylaws (which do not include payment of any membership or initiation dues or fees). NERC Bylaws Article II, §1. In the *ERO Certification Order*, the Commission stated the availability of membership to any person or entity with an interest in the reliable operation of the North American BPS created an open membership structure that is consistent with the statutory requirement that the ERO establish rules that assure fair stakeholder representation. *ERO Certification Order* at P 54. Each member is assigned to one of the 12 membership sectors of NERC. NERC Bylaws Article II, §4.

[78] Article II, §4a of the NERC Bylaws specifies the types of persons or organizations that would be included in each of the membership sectors.

[79] The representation of Regional Entities in the MRC reflects changes made by NERC to the originally-proposed composition of the MRC in response to concerns expressed by the Commission in P 75 of the *ERO Certification Order*. *See NERC ERO Governance Compliance Filing* at 6-9. The Commission accepted these changes in an Order issued October 30, 2006. The Commission also accepted the overall structure and composition of the MRC in that Order. *North American Electric Reliability Corporation, Order on Petitions for Rehearing and Clarification; Order on Compliance Filing*, 117 FERC ¶ 61,126 (2006), at PP 30 and 44.

[80] The chairman and vice chairman of the MRC are selected annually by majority vote of the members of the MRC, and may not be from the same membership sector. Upon being selected as chairman and vice chairman, these individuals cease to be representatives of the MRC sectors to which they were originally elected, and are thereafter responsible to act in the best interests of the members of NERC as a whole. NERC Bylaws Article VIII, §5.

[81] Article VIII, §4 of the Bylaws contains provisions for the election of additional Canadian members to the MRC as and when necessary to ensure that the percentage of Canadian members on the MRC is approximately equal to the percentage the NEL of Canada is of the total NEL of the United States and Canada. See page 24 below for the definition of NEL.

(5) The following representatives of the government representatives sector: two representatives of the United States federal government, one representative of the Canadian federal government, two representatives of state governments, and one representative of a provincial government, all of whom shall be nonvoting members of the MRC except the two representatives of state governments.

The MRC is therefore comprised of 26 voting members when at full complement (or more if the election of additional Canadian members has been necessary in accordance with Article VIII, §4 of the Bylaws). The members of the MRC from each sector are nominated from, and elected by, the NERC members in that sector pursuant to the processes specified in Article VIII, §3 of the NERC Bylaws, which generally call for election of the two candidates from each sector receiving the highest numbers of votes in the sector. The members of the MRC are elected annually (or between annual elections if needed to fill a vacancy).[82]

In summary, NERC's trustees are nominated by a nominating committee comprised of independent trustees whose terms are not expiring, members of the MRC, and possibly others. NERC's trustees are elected by a two-thirds vote of the MRC, which is a committee established pursuant to the Bylaws to fairly represent the sectors of NERC's membership and is open to any person or entity with an interest in reliable operation of the North American BPS. Thus, the NERC Bylaws provide for fair stakeholder representation in the selection of NERC's trustees.

Balanced Decision-Making in any NERC Committee or Subordinate Organizational Structure

NERC's Bylaws authorize the Board of Trustees to create standing committees of NERC and such other committees as the Board deems necessary to carry out the purposes of NERC:

> In addition to those committees specified by these Bylaws, to which the board shall appoint members in accordance with the requirements of these Bylaws, the board may by resolution create standing committees of the Corporation; and may in addition by resolution appoint such other committees as the board deems necessary to carry out the purposes of the Corporation. *The board shall appoint standing committees and other committees of the Corporation that are representative of members, other interested parties and the public, that provide for balanced decision making, and that include persons with outstanding technical knowledge and experience. All appointments of committees of the Corporation shall provide the opportunity for an equitable number of members from the United States and Canada (and from Mexico after the Corporation receives recognition by appropriate governmental authorities in Mexico as its electric reliability organization) to be appointed to each committee in approximate proportion to each country's percentage of the total NEL*. All committees shall have such scope and duties, not inconsistent with law, as are specified in these Bylaws and the Rules of

[82] NERC Bylaws Article VIII, §3.

> Procedure of the Corporation or otherwise determined by the board. (Emphasis added.)[83]

Section 1300 of the NERC ROP provides additional criteria for the creation and appointment of NERC standing committees. In creating a standing committee, the NERC Board of Trustees must approve the charter of the committee and assign specific authority to each committee necessary to conduct business within its charter.[84] Each committee shall have a defined membership composition that is explained in its charter. The specified committee membership composition can provide for balanced decision-making (i) by providing for representatives from each sector of the NERC membership, or (ii) where sector-based membership 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.[85] Committee membership shall also provide the opportunity for an equitable number of members from the United States and Canada, based approximately on proportionate NEL.[86]

The NERC ROP require that committee members shall be selected in a manner that is open, inclusive, and fair.[87] Unless otherwise stated in the NERC ROP or approved by the NERC Board of Trustees, all committee member appointments are to be approved by the board, and committee officers are to be appointed by the Chairman of the Board.[88]

Further, the NERC ROP require that all NERC 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,

[83] NERC Bylaws Article VII, §1. "Committees specified by these Bylaws" include the MRC and the Nominating Committee for the NERC Board of Trustees (discussed above under "fair stakeholder representation in the selection of NERC's trustees"), and the Personnel Certification Governance Committee (PGCC) provided for in Article XII of the Bylaws. The purpose of the PGCC is to provide oversight to the policies and processes used to implement and maintain the integrity and independence of the NERC System Operator Certification Program. NERC Bylaws Article XII, §1. The members of the PGCC are appointed by the Board from candidates nominated by a nominating task force; nominations and appointments are to take into account the need to include representatives of all geographic regions of North America on the PGCC. *Id*., Article XII, §2. In addition to the aforementioned committees, NERC standing committees include the Standards Committee, Compliance and Certification Committee, Critical Infrastructure Protection Committee, Operating Committee, Planning Committee, and the Reliability Issues Steering Committee.

[84] ROP §1301.

[85] ROP §1302.

[86] ROP §1302.

[87] ROP §1303.

[88] ROP §1303.

and no single sector is able to defeat a matter.[89] Any committees and subgroups organized on other than a membership-sector basis must be reported to the NERC Board of Trustees and the MRC, along with the reason for constituting the committee or subgroup in the manner chosen. The ROP provide that for any committee or subgroup organized on other than a membership-sector basis, a reasonable opportunity for additional participation (as members or observers) shall be provided for sectors not represented on the committee or subgroup (subject to any reasonable restrictions as may be necessary to accomplish the mission of the committee or subgroup).[90] Additionally, a reasonable opportunity must be provided for membership from sectors desiring to participate in any committees and subgroups pertaining to development of, interpretation of, or compliance with Reliability Standards.[91]

The NERC ROP provide that NERC standing committees may appoint subgroups using the same principles as specified in §1302 of the ROP (summarized in the immediately preceding paragraph).[92]

The provisions of §§1301 and 1302 of the NERC ROP regarding committee composition reflect revisions to these provisions that were approved or directed by the Commission in its October 30, 2006 order on the *NERC ERO Governance Compliance Filing*.[93]

The requirement for balanced decision-making is also applicable to the Reliability Standards development process, and is discussed below under criterion 5, "The ERO has established rules that provide reasonable notice and opportunity for public comment, due process, openness and balance of interests in developing Reliability Standards, and otherwise exercising its duties."

C. Criterion 3 - The ERO has established rules that allocate equitably reasonable dues, fees and charges among end users for all statutory activities.

NERC's Bylaws require that the funding mechanism used to recover its net annual budget requirement (i.e., net of fees and other revenues received by NERC from users and purchasers of NERC products and services, and net of prior-period funding surplus or deficiency) "shall consist of such assessments as determined by the [NERC] board that result in an equitable allocation of the Corporation's funding requirement among end users of the North American electric utility system as established in the Corporation's Rules of Procedure."[94] Section 1102 of the NERC ROP,

[89] ROP §1302.

[90] ROP §1302.

[91] ROP §1302.

[92] ROP §1305.

[93] *See North American Electric Reliability Corporation, Order on Petitions for Rehearing and Clarification; Order on Compliance Filing*, 117 FERC ¶ 61,126 (2006), at PP 75-87.

[94] NERC Bylaws Article XIII, §3. NERC charges users/purchasers of some of its products and services directly for the products and services, at prices that cover some or all of the cost of providing the product or service. Examples include charges to purchasers of data sets from the Generating Availability Data System, charges to candidates for

"NERC Funding and Cost Allocation," prescribes the allocation methods to be used to recover NERC's funding requirements among regions of the United States and among countries in the North American BPS. Section 1102 specifies that NEL shall be used to allocate funding requirements among interconnections and Regional Entities except in those instances in which direct assignment of costs to a particular interconnection, Regional Entity, or group of entities is appropriate; however, in the case of direct assignment, NEL must be used to allocate the directly-assigned costs within the interconnection, Regional Entity, or group of entities:

> (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 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 Organization.
>
> (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 NEL.

The NERC ROP define NEL as:

> [N]et 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.[95]

In business plan and budget filings with the Commission, actual assessments for Canadian and Mexican entities vary after taking into account polices regarding the allocation of certain compliance and enforcement costs.

D. Criterion 4 - The ERO has established rules that provide fair and impartial procedures for enforcement of Reliability Standards through the imposition of penalties in accordance with 18 C.F.R. §39.7, including limitations on activities, operations, or other appropriate sanctions or penalties.

NERC has established rules that provide fair and impartial procedures for monitoring and enforcement of compliance with Reliability Standards. These rules and procedures are embodied

---

certification as NERC-certified operators for examinations and for renewal of credentials, and charges to continuing education providers for certification of their education programs.

[95] ROP Appendix 2.

primarily in §400 of the NERC ROP, the NERC CMEP (Appendix 4C to the ROP), and individual Regional Entity CMEPs (which conform generally to the NERC CMEP), all of which have been approved by the Commission. These rules and procedures were discussed in detail above under criterion 1, relating to the ERO's ability to develop and enforce Reliability Standards that provide for an adequate level of reliability of the BPS. As discussed above under criterion 1, §400 of the ROP, and the NERC uniform CMEP, include provisions for avoidance of conflicts of interest on the part of the CEA personnel conducting compliance monitoring processes, provisions for notice to registered entities and opportunity to respond to compliance monitoring processes, and provisions allowing registered entities to engage in settlement discussions with the CEA concerning notices of alleged violations, proposed penalties or sanctions, and mitigation plans.

In addition, Attachment 2, *Hearing Procedures*, to the uniform CMEP contains detailed due process procedures for the conduct of hearings before the CEA hearing body, when requested by the registered entity, concerning a disputed notice of alleged violation and/or proposed penalty or sanction, disputed mitigation plan provisions, or disputed remedial action directive. The *Hearing Procedures*, which were initially approved by the Commission in two orders, subject to various specific compliance requirements,[96] are based on, and in most respects are quite similar to, the Commission's Rules of Practice and Procedure[97] and to the rules of practice and procedure used by many state public utility commissions.

In 2013, the Regional Entity representatives to the ERO Legal Group developed *Hearing Body Manual – Guidance for Conducting Hearings at the Regional Entities* (Hearing Body Manual) to provide practical guidance to hearing body members at the eight Regional Entities regarding the hearing process. The Hearing Body Manual outlines the specific duties of the hearing officer and the hearing body and discusses the standard of review that should govern the hearing body's consideration of the hearing officer's decisions throughout the hearing process. The particulars of the hearing process, including the roles of the hearing officer and the hearing body, are set forth in Attachment 2 to the CMEP. To the extent that there is a conflict between the Hearing Body Manual and the CMEP, the CMEP, as applicable, prevails.

The remainder of this discussion of NERC's compliance with criterion 4 addresses NERC's rules and procedures for the determination and imposition of penalties for violations of Reliability Standards.

Section 215(e)(6) of the FPA, and §39.7(g) of the Commission's regulations,[98] requires that any penalty imposed for violation of a Reliability Standard shall (a) bear a reasonable relation to the seriousness of the violation; and (b) take into consideration the efforts of the user, owner or

[96] *Order Addressing Revised Delegation Agreements*, 122 FERC ¶61,245 (2008); *Order Accepting Compliance Filings, Subject to Conditions*, 125 FERC ¶61,330 (2008).

[97] 18 C.F.R. Part 385.

[98] 18 C.F.R. §39.7(g).

operator to remedy the violation in a timely manner.[99] This fundamental requirement is embodied in §401.7 of the NERC ROP and in §3.8 of the NERC *Sanction Guidelines*, Appendix 4B to the ROP. Section 39.7(c) of the Commission's regulations[100] requires that NERC or a Regional Entity may, after notice and opportunity for hearing, impose a penalty on a user, owner or operator of the BPS for a violation of a Reliability Standard if NERC files a notice of penalty and record of the proceedings with the Commission and serves a copy on the user, owner or operator. The notice of penalty must contain: (i) the name of the entity on whom the penalty is imposed; (ii) identification of each Reliability Standard violated; (iii) findings of fact with respect to any act or practice resulting in violation of the standard; (iv) a description of the penalty imposed; (v) the record of the proceeding; and (vi) any other matters NERC or the Regional Entity may find relevant.[101] The penalty may not take effect earlier than the 31st day after NERC files the notice of penalty and record of proceeding with the Commission,[102] and it is subject to review by the Commission on its own motion or on application of the user, owner or operator.[103] Section 5.9 of the NERC CMEP provides for the filing of a notice of penalty with the Commission, and for a 30-day period to run before the penalty becomes effective, in accordance with 18 C.F.R. §39.7(d) through (e).[104]

Section 39.7(g) of the Commission's regulations[105] requires the ERO to submit for Commission approval penalty guidelines that set forth a range of penalties for violations of Reliability Standards, and specifies that a penalty imposed by the ERO or a Regional Entity must be within the range set forth in the penalty guidelines. The NERC *Sanction Guidelines* comprise the penalty guidelines established by NERC, which the Commission has approved pursuant to §39.7(g).

---

[99] 18 C.F.R. §39.7(g)(1) also specifies that a penalty may be monetary or non-monetary, and may include, but is not limited to, a limitation on an activity, function, operation, or other appropriate sanction, including being added to a reliability watch list composed of major violators that is established by the ERO, a Regional Entity or the Commission.

[100] 18 C.F.R. §39.7(c).

[101] 18 C.F.R. §39.7(d).

[102] 18 C.F.R. §39.7(e).

[103] 18 C.F.R. §39.7(e).

[104] Certain instances of noncompliance with the Reliability Standards may be resolved outside of the notice of penalty process set forth in the NERC CMEP. Beginning in September 2011, NERC began tracking certain lesser-risk remediated possible violations in the FFT program. Following the Commission's *Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing*, 138 FERC ¶ 61,193 (2012), the Commission considered all FFT matters closed sixty days after the FFT informational filing was submitted to the Commission unless the Commission sought to review a specific matter. In June 2013, the Commission approved expanding the scope of the FFT Program to include a limited pool of moderate risk issues (in addition to the minimal risk issues already permitted under the program), as well as issues with ongoing mitigation activities, provided the mitigation would be completed within 90 days. In addition, the Commission approved the practice of publicly posting FFT matters on a common website in lieu of a monthly informational filing to the Commission. The Commission indicated that it would consider an FFT matter closed 60 days following the public posting. *Order on Compliance Filing*, 143 FERC ¶ 61,253 (2013).

[105] 18 C.F.R. §39.7(g)(2).

Under the *Sanction Guidelines*, penalties are to be commensurate to the reliability impact of the violation and to those levied for similar violations, while still reflecting unique facts and circumstances related to the violation or the violator. NERC is charged with ensuring "acceptable similarity" in penalties for comparable violations.[106]

Significantly, however, the *Sanction Guidelines* also state, "Any provisions within a settlement regarding Penalties or sanctions can supersede any corresponding Penalties or sanctions that would otherwise be determined pursuant to these Sanction Guidelines."[107] As such, the negotiation of settlements and determination of penalties involve compromise and the weighing of multiple considerations to arrive at a penalty agreeable to the Regional Entity and the registered entity. Even with this available flexibility, NERC still evaluates the facts and circumstances of every violation that is part of a settlement to ensure that the penalty for that violation, and for the group of violations in the settlement, is within a range of reasonableness that displays consistency.

When evaluating every violation, NERC starts with a base penalty amount that is provided by the VRF/VSL matrix. If the registered entity has a previous violation of a same or similar Reliability Standard Requirement, then the penalty may be aggravated.[108] NERC next considers the violation time horizon for the violation, with multipliers applied to the penalty based on the effect on operations. The highest multiplier applies to real-time operations, while long-term planning is on the opposite end of the spectrum. The registered entity's ability to impact reliability determines the next multiplier, with small facilities or entities having their penalty reduced by a significant amount. A multiplier can be applied based on the condition of the BPS at the time of the violation, with aggravation for a violation occurring during stressed conditions.[109] Among the mitigating factors in penalty determination are the quality of the registered entity's internal compliance program, the degree of the registered entity's cooperation in resolution of the violation, and whether the registered entity self-reported the violation.[110]

NERC will aggregate the results of the violation-by-violation analysis for comparison with the penalty included in the settlement submitted by the Regional Entity. NERC also evaluates how the penalty for the violations in the instant settlement compares to penalties for similar violations included in settlements that have already been approved by NERC and subject to review by the Commission. The evaluation of settlements provides an evolving store of knowledge to use when considering new settlements submitted to NERC. In the end, if the penalty included in the settlement falls within a range of reasonableness for penalties associated with violations involving similar reliability risks, similar entities, and similar facts and circumstances, then the penalty is deemed consistent enough for approval by NERC.

---

[106] *Sanction Guidelines* §1.

[107] *Sanction Guidelines* §2.1.

[108] *Sanction Guidelines* §§3.1 and 3.2.

[109] *Sanction Guidelines* §2.7; *see also* §3.2.

[110] *Sanction Guidelines* §3.3.

E. Criterion 5 - The ERO has established rules that provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards, and otherwise exercising its duties.

NERC has established rules that provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards, and otherwise exercising its duties. With respect to the development of Reliability Standards, NERC's Bylaws require that:

> The Corporation shall develop Reliability Standards pursuant to procedures and processes that shall be specified in the Rules of Procedure of the Corporation. The Rules of Procedure shall provide for the development of Reliability Standards through an open, transparent, and public process that provides for reasonable notice and opportunity for public comment, due process, and balancing of interests and is designed to result in Reliability Standards that are technically sound. Participation in the process for developing Reliability Standards shall not be limited to members of the Corporation but rather shall be open to all persons and entities with an interest in the reliable operation of the BPS.[111]

NERC's process for developing and modifying Reliability Standards, which the Commission accepted as meeting the criteria for certifying NERC as the ERO pursuant to §215 of the FPA and §39.3(b) of the Commission's regulations,[112] is embodied in §300 of the NERC ROP and the SPM, Appendix 3A to the ROP. Section 304 of the ROP states that NERC shall develop Reliability Standards in accordance with the NERC SPM. The SPM sets forth the detailed process steps for development and approval of a new Reliability Standards or revision to a Reliability Standard.

Section 304 of the NERC ROP sets forth NERC's "Essential Principles for the Development of Reliability Standards," which include openness, transparency, consensus-building, fair balance of interests, due process, and timeliness:

> 1. **Openness** — Participation shall be open to all persons who are directly and materially affected by the reliability of the North American BPS. 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.

[111] NERC Bylaws Article IX, §2.

[112] *ERO Certification Order*, 116 FERC ¶61,062, at PP 239, 241, 250.

3. **Consensus-building** — The process shall build and document consensus for each standard, both with regard to the need and justification for the Reliability Standard and the content of the Reliability Standard.

4. **Fair Balance of Interests** — The process shall fairly balance interests of all stakeholders and shall not be dominated by any two segments as defined in Appendix 3D, *Development of the Registered Ballot Body*, of these Rules of Procedure, and no single segment, individual or organization shall be able to defeat a matter.

5. **Due Process** — Development of Reliability Standards shall provide reasonable notice and opportunity for any Person with a direct and material interest to express views on a proposed Reliability Standard and the basis for those views, and to have that position considered in the development of the Reliability Standards.

6. **Timeliness** — Development of Reliability Standards shall be timely and responsive to new and changing priorities for reliability of the BPS.

Section 305 of the NERC ROP specifies that "NERC Reliability Standards shall be approved by a Registered Ballot Body prior to submittal to the [NERC] Board and then to [a]pplicable [g]overnmental [a]uthorities for their approval," and that "[a]ny person or entity may join the Registered Ballot Body to vote on Reliability Standards." The RBB is organized on an industry segment basis, and persons or organizations joining the RBB must select membership in the appropriate segment (subject to periodic review by NERC).[113] The RBB segments and the criteria for membership in each segment are set forth as follows:[114]

- 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

[113] ROP §305.

[114] ROP Appendix 3D at 2-3. The segments of the RBB are different from the NERC membership segments established by Article II, §4 of the NERC Bylaws (discussed above under criterion 2). The Commission approved the use of segments for the RBB that are different from the NERC membership segments. *North American Electric Reliability Corporation, Order on Petitions for Rehearing and Clarification, Order on Compliance Filing*, 117 FERC ¶ 61,126 (2006), at P 30.

- 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
- Segment 10: Regional Entities

Section 306 of the ROP provides for the standards development process to be overseen by a Standards Committee, which is an elected body comprised of two members of each segment of the RBB and two officers elected to represent the interests of the industry as a whole.[115] The Standards Committee is to ensure stakeholder interests are fairly represented in the Reliability Standards development process. Section 308.2 of the ROP specifies that proposed Reliability Standards or revisions to Reliability Standards shall be submitted to the NERC Board of Trustees for approval after being approved by the RBB pool voting on the standard.

The NERC SPM sets out the detailed steps in the process for developing and approving Reliability Standards or revisions to Reliability Standards. The process is based on the procedures of the ANSI and other standards-setting organizations in the United States and Canada.[116] The standards development process is intended to develop consensus on both the need for and content of a proposed standard.[117] As detailed in the SPM, the process includes the following key elements:

- Nomination of a proposed standard, revision to a standard, or withdrawal of a standard, using a SAR, which may entail appointing a SAR drafting team.[118]
- Public posting of the SAR to allow interested persons and entities to review and comment on the need for the proposed standard and the expected outcomes and impacts from implementing it, and to identify if there is stakeholder consensus on the need, scope and applicability of the standard proposed by the SAR.[119]

[115] Election of the members of the Standards Committee is governed by the *Procedures for Election of Members of the Standards Committee*, Appendix 3B to the ROP.

[116] SPM §§1.4, 10.0, 13.0, and 16.0. ANSI accredited NERC's Reliability Standards development process in 2003.

[117] SPM §§1.4. 3.8, 3.10, and 4.0.

[118] SPM §§4.0, 4.2, and 4.3.

[119] SPM §§4.0, 4.1, and 4.2.

- Review of the public comments in response to the SAR and prioritization of proposed standards, leading to authorization to develop standards for which there is a stakeholder consensus-based need.[120]

- Appointment of a standard drafting team to draft the new or revised standard. The appointed standard drafting team is to have the expertise, competencies and diversity of views needed to develop the standard. The appointment process includes a public solicitation for nominees.[121]

- Drafting the new or revised standard. The standard will be drafted by the standard drafting team with the assistance and administrative support of the NERC standards process manager (a NERC professional staff member), who will review the draft standard for consistency of quality and completeness and to ensure the standard is within the scope and purpose identified in the SAR.[122]

- Public posting of the draft standard to allow interested parties to review and comment on it, to receive specific comments from interested parties on the text of the standard, to assess stakeholder consensus on the draft standard, and to determine if the draft standard should be modified to increase consensus.[123]

- Field testing (if any) of the draft standard and its measures.[124]

- Analysis of public comments and field test results (if any) by the standard drafting team, giving consideration to the written views and objections of all participants, to determine if there is consensus the proposed standard should go to ballot, or requires further work.[125]

- Balloting of the standard by the industry stakeholder ballot pool formed from the RBB for purposes of balloting the new or revised standard.[126] (The voting process is described below.)

---

[120] SPM §§4.0, 4.1, 4.2, and 4.3.

[121] SPM §§4.0, 4.3, and 4.4.

[122] SPM §§4.0 and 4.4.

[123] SPM §§4.0, 4.5, and 4.7.

[124] SPM §§4.0 and 6.0.

[125] SPM §§4.0, 4.5, 4.6, 4.7, 4.12, and 6.0.

[126] SPM §§4.0, 4.7, 4.8, and 4.9.

- Re-balloting of the standard to consider specific comments by those submitting negative votes with comments.[127]

- Vote by the NERC Board of Trustees to approve or reject the standard that has been approved by the ballot pool. The NERC Board of Trustees may adopt or reject a Reliability Standard that has been approved by the ballot pool, but may not modify the standard; however, if the NERC Board of Trustees chooses not to adopt a proposed standard, the board shall provide its reasons.[128]

- Submission of the RBB-approved and board-approved Reliability Standard to the Commission and other applicable governmental authorities for approval.[129]

As provided in the SPM, voting on a proposed Reliability Standard or revision to a standard is done by the RBB ballot pool formed for that standard, and is tallied on a weighted segment basis. At least 30 days prior to the start of a ballot, the NERC standards process manager issues a notice to the entities in the RBB advising them of the upcoming ballot on the new or revised standard, so that entities may elect to join the ballot pool for balloting the standard. Any member of the RBB may join (or leave) the ballot pool for the standard until the ballot period begins.[130] The balloting is conducted electronically with voting allowed during a specified ballot period, typically 10 days.[131] Approval of a proposed standard or revision to a standard requires both (i) a quorum, which is established by at least 75 percent of the members of the ballot pool submitting a response with an affirmative vote, a negative vote, or an abstention,[132] and (ii) affirmative votes by a two-thirds majority of the weighted segment votes.[133] The calculation of the weighted segment voting results is described in detail in the SPM.[134]

The foregoing demonstrates that NERC's rules provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in the development of

[127] SPM §§4.0, 4.13, and 4.14. Voters on the first ballot are allowed to submit comments with affirmative ballots and reasons for their votes with negative ballots (although inclusion of a statement of reasons with a negative ballot is not required).

[128] SPM §§4.0, 4.15, and 4.16.

[129] SPM §§4.0, 4.16, and 4.17.

[130] SPM §4.8.

[131] SPM §§4.0 and 4.9.

[132] SPM §4.10.

[133] SPM §§4.10 and 4.11. For this purpose the number of votes cast is the sum of the affirmative and negative votes cast by the ballot pool, excluding abstentions, non-responses and negative votes without comments.

[134] SPM §§4.10 and 4.11.

Reliability Standards. In finding that NERC met the statutory and regulatory criteria to be certified as the ERO, the Commission found NERC's Reliability Standards development process met the ERO certification requirement that the ERO candidate have rules providing for reasonable notice and opportunity for public comment, due process, openness, and balancing of interests in developing Reliability Standards.[135]

Other NERC rules provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in the exercise of NERC's duties other than developing Reliability Standards. As discussed under criterion 2 above, NERC's Bylaws provide for its trustees to be elected by the MRC, which (again per the NERC Bylaws) is comprised of representatives of the sectors of the NERC membership as defined in the Bylaws. The Bylaws also provide that amendments to the Bylaws must be adopted by majority vote of both the Board of Trustees and the MRC, conducted after at least 10 days and no more than 60 days' notice of the vote on the proposed amendment. Additionally, the NERC membership may adopt new Bylaws, or alter, amend, or repeal amendments adopted by vote of the board and the MRC, by vote of two-thirds of the sectors voting on the alteration, amendment, repeal or adoption.[136]

The Bylaws further provide that revisions to the NERC ROP may be proposed by: (i) any 50 members of NERC, which must include members from at least three membership sectors; (ii) the MRC; (iii) a committee of NERC to whose function and purpose the ROP to be amended pertains; or (iv) an officer of NERC. A proposed revision to the NERC ROP must be posted on the NERC website for public comment for a minimum of 45 days prior to the NERC Board of Trustees vote on the proposed revision.[137]

The NERC Bylaws require that notice of meetings of the NERC Board of Trustees and of the MRC, and notice of calls for action without a meeting by the board or the MRC, along with all non-confidential materials to be considered by the board or MRC at a meeting or in an action without a meeting, shall be posted on the NERC website at least 24 hours prior to the meeting or within 24 hours after the call for action without a meeting.[138] The ROP provide that notice of meetings of NERC committees, and all non-confidential materials relating to the meeting, shall be posted on the NERC website at approximately the same time(s) the notice and materials are provided to the committee members.[139] Additionally, the Bylaws require that, except for discussions of certain specified non-public topics, meetings of the NERC Board of Trustees and of the MRC shall be open to the public (subject to reasonable space limitations).[140] Similarly, the

[135] *ERO Certification Order* at P 250.

[136] NERC Bylaws Article XIV, §1.

[137] NERC Bylaws Article XI, §2.

[138] NERC Bylaws Article V, §§4 and 6; Article VIII, §§10 and 12.

[139] ROP §1304.1.

[140] NERC Bylaws Article V, §4; Article VIII, §10.

NERC ROP require that, except for discussions of certain specified non-public topics, meetings of NERC standing committees shall be open to the public (subject to reasonable space limitations).[141]

With respect to the preparation of NERC's annual business plan and budget, the NERC Bylaws provide that NERC shall post a draft business plan and budget for comment by the NERC membership, the MRC, and the NERC standing committees for at least 30 days prior to the board meeting at which the annual business plan, budget and funding requirement is to be approved for submission to the Commission. The Board shall also consult with the members of the MRC on the proposed business plan and budget before it is adopted.[142] Should a supplemental or modified budget or assessment be considered for adoption during the course of the year, the Bylaws require that the procedures for posting, receipt of comments, and consultation with the MRC shall be followed to the extent possible in the board's judgment in light of the exigency of the circumstances necessitating preparation and approval of the supplemental or modified budget, funding and assessment.[143]

With respect to compliance monitoring and enforcement, as discussed above under criteria 1 and 4, the NERC CMEP and Regional Entity CMEPs, the NERC *Hearing Procedures* (Attachment 2 to the CMEP), and the NERC *Sanction Guidelines*, provide for reasonable notice to and due process for users, owners, and operators of the BPS in the conduct of compliance monitoring and enforcement activities of NERC and the Regional Entities. These activities include the implementation of the compliance monitoring processes, the conduct of hearings on disputed notices of alleged violations, proposed penalties, disputed mitigation plan components and disputed remedial action directives, and the imposition of penalties and sanctions for violations of Reliability Standards.

Finally, as discussed above under criterion 2, the NERC Bylaws and ROP require members to be selected for NERC standing committees and other committees and subgroups so as to (subject to specified exceptions) provide for balanced decision making, such that no two stakeholder sectors can control the voting on the committee and no single stakeholder sector is able to defeat a matter; and to provide the opportunity for an equitable number of members from the United States and Canada.

F. Criterion 6 - The ERO has established rules that provide appropriate steps to gain recognition in Canada and Mexico.

As stated in its Certificate of Incorporation, one of the corporate purposes of NERC is "to act as the electric reliability organization for the United States as certified by the Federal Energy Regulatory Commission and for Canada and Mexico as recognized by applicable government and regulatory authorities in such countries, all pursuant to law." The efforts of NERC to seek recognition in Canada and Mexico are described below.

---

[141] ROP §1304.1.

[142] NERC Bylaws Article XIII, §4; *see also* ROP §1103.1.

[143] NERC Bylaws Article XIII, §5.

Canada

Under the Constitution of Canada, regulation of electricity is primarily within the jurisdiction of each province. Canada does not have a 'FERC-equivalent' with plenary jurisdiction over electricity matters, although the National Energy Board (NEB) does have jurisdiction over international power lines. Accordingly, beginning before its certification as the ERO for the United States and continuing to the present time, NERC has devoted significant efforts to developing relationships with each of the relevant provincial authorities, as well as the NEB. Where possible, NERC has devoted efforts attempting to obtain recognition as the electric reliability organization. NERC's progress in this regard is described below.

Alberta

Reliability Standards

The Alberta Electric System Operator (AESO) is the independent system operator, a statutory corporation pursuant to Alberta's *Electric Utilities Act*, *2003* (EUA).[144] AESO's statutory mandate requires that it direct the operation of the Alberta interconnected electric system, plan for the future of the transmission system, and operate the wholesale electricity market in the province.

Pursuant to the Alberta *Transmission Regulation* (made pursuant to the EUA),[145] Alberta Reliability Standards include reliability standards[146] enacted by WECC, NERC, or any similar entity that is recognized by the AESO, to the extent that these reliability standards are adopted by the AESO in accordance with the *Transmission Regulation*. The AESO also has the authority under the *Transmission Regulation* to adopt other reliability standards subject to certain process requirements.

In order for a reliability standard to be adopted in Alberta, the *Transmission Regulation* requires that the AESO consult with those market participants that it considers likely to be directly affected by one or more reliability standards and make a recommendation to the Alberta Utilities Commission to approve or reject the reliability standards being considered for approval. The Alberta Utilities Commission must follow the AESO's recommendation unless an interested person satisfies the Alberta Utilities Commission that the recommendation of the AESO is either "technically deficient" or "not in the public interest." When the AESO considers NERC Reliability Standards for adoption in Alberta, the AESO is required to determine whether the NERC

[144] Alberta's EUA is available at: http://www.qp.alberta.ca/documents/Acts/E05P1.pdf.

[145] Alberta's *Transmission Regulation* is available at: http://www.qp.alberta.ca/documents/Regs/2007_086.pdf.

[146] In this context, where not capitalized, the phrase "reliability standards" refers to standards relating to reliability generally, whether or not they were developed or approved by NERC.

Reliability Standards can be applied in Alberta, including whether approval would be appropriate for the Alberta electric energy market framework.[147]

The AESO's *Alberta Reliability Standards Program Work Plan* is intended to help manage and track the adoption of NERC Reliability Standards in Alberta. It was last revised in June 2014, and it reflects a risk-based prioritization approach.[148] The Alberta Reliability Standards, as approved, bear the same identifiers as the original NERC Reliability Standards (COM, BAL, FAC, etc.), but have an "AB" added to the name.[149]

An Alberta Reliability Standard may incorporate modifications from the original NERC Reliability Standard to recognize the physical characteristics of the Alberta system or for other reasons.[150]

When presented to the Alberta Utilities Commission by the AESO for approval, a proposed Alberta Reliability Standard will contain an explanation for any proposed modifications, which are not intended to change the intent or substance of the NERC Reliability Standards. Where there have been changes from a NERC Reliability Standard to an Alberta Reliability standard, it is noted in a quarterly update report that is provided to WECC and to NERC.

Effective January 1, 2014, the AESO assumed all responsibilities related to the functions of a Reliability Coordinator, effective January 1, 2014. The AESO has indicated that it remains an active member and supporter of the WECC (the former Reliability Coordinator for the AESO), and it looks forward to a strong working relationship with the proposed independent WECC RC, Peak Reliability. Additional Alberta Reliability Standards will be adopted, and this work is underway.

Data Sharing

Under §8.4 of the WECC/AESO membership and operating agreement (MOA), if WECC determines that the AESO is not in compliance with an Alberta Reliability Standard, WECC must promptly refer the matter to the Market Surveillance Administrator (MSA). Pursuant to the

---

[147] Alberta has developed an Alberta Functional Model that integrates with the Alberta regulatory and market framework. The Alberta Functional Model defines entity types that perform functions that impact the reliability of the transmission system. Functional entity types are used to identify if an Alberta Reliability Standard is applicable to that functional type.

[148] The *Alberta Reliability Standards Program Work Plan* can be found at: http://www.aeso.ca/rulesprocedures/25052.html. Alberta Reliability Standards currently in effect and their effective dates are listed on the AESO website at: http://www.aeso.ca/rulesprocedures/17006.html. A number of NERC Reliability Standards have been rejected as not being applicable to entities in Alberta. These are listed at: http://www.aeso.ca/rulesprocedures/16426.html.

[149] An example of a current Alberta Reliability Standard is BAL-001-AB-0a, Real Power Balancing Control Performance.

[150] *See* Project Charter for Alberta Reliability Standards Implementation at p.1, available at: http://www.aeso.ca/downloads/ARS_Project_Charter_2011-12-05_final.pdf.

WECC/MSA services agreement, WECC, on behalf of the MSA, will monitor AESO's compliance with Alberta Reliability Standards and report its findings to the MSA.

Sections 2.13, 6.1, and 6.5 of the WECC/MSA services agreement address WECC's ability to report possible violations[151] to NERC. Under §2.13, NERC and FERC are not allowed to participate in or observe WECC's actions taken according to the WECC/MSA services agreement, without the express approval of the MSA. Section 6.1 establishes that all records pertaining to WECC's services will be considered confidential and should be treated as strictly confidential at all times.[152]

Based on its agreement with the MSA, WECC is prohibited from disclosing information related to the AESO's compliance with Alberta Reliability Standards without the permission of the MSA. However, as noted in the NERC/WECC/AESO memorandum of understanding (MOU),[153] disclosing information related to confirmed contraventions would occur as such information is made public by the Alberta Utilities Commission. In addition, as there is value to the North American electric industry of receiving information on lessons learned from such contraventions, the AESO will work with NERC and WECC to provide information on lessons learned as made public by the Commission.

Compliance

The NERC/WECC/AESO MOU commits the AESO to appropriate compliance monitoring and enforcement "in a manner determined in Alberta." With regard to entities (other than the AESO) that are subject to Alberta Reliability Standards, the AESO carries out its mandate to monitor compliance according to a compliance monitoring plan. Matters of noncompliance with an Alberta Reliability Standard must be referred by the AESO to the MSA for consideration and possible action.

The Alberta Utilities Commission adopted specified penalties for contraventions of Alberta Reliability Standards effective November 2010. If warranted, the MSA is empowered by §52 of the *Alberta Utilities Commission Act* to issue a notice of specified penalty for contravention of an Alberta Reliability Standard. Specified penalties are defined in AUC Rule 027 and range from $500 to $25,000, depending upon the severity of the contravention and the applicable Alberta

[151] The terms "possible violation," confirmed violation," and "violation" are not defined in Alberta. Rather, Alberta uses the terms "suspected contravention" and "contravention."

[152] Section 6.5 is even more explicit with respect to WECC's authority to share information with NERC and mandates the following:

> WECC further acknowledges that this Agreement clearly stipulates that in no event will Confidential Records received or generated by WECC in respect of the Services or this Agreement be disclosed or made available to persons outside WECC, including to any representative of FERC, NERC or any other person, without the express written approval of the MSA.

[153] MOU between NERC, WECC, and AESO, effective July 15, 2010, at p. 7, available at: http://www.nerc.com/files/NERC-WECC-AESO_MOU_Executed%20Version_071510.pdf.

Reliability Standard.[154] Specified penalties can be appealed to the Alberta Utilities Commission. Alternatively, the MSA can pursue an administrative penalty before the Alberta Utilities Commission. The maximum administrative penalty amount is $1 million per day on which a contravention occurs or continues.

British Columbia

Reliability Standards

The British Columbia Utilities Commission (BCUC) is an independent, quasi-judicial regulatory agency that operates under and administers the *Utilities Commission Act*.[155] The BCUC adopts or rejects reliability standards in British Columbia and is responsible for the administration of the Mandatory Reliability Standards Program. The British Columbia Hydro and Power Authority (BC Hydro), a provincial crown corporation, is a regulated integrated utility and transmission provider that acts as a balancing authority and applicant for Reliability Standards to the BCUC.

To provide the necessary information required for determinations and in accordance with the *Utilities Commission Act*, BC Hydro submits a *Mandatory Reliability Standard Assessment Report* to the BCUC assessing the new and revised reliability standards adopted in the United States by FERC within the annual assessment period (December 1 to November 30). The assessment report is developed in consultation with Registered Entities in the Mandatory Reliability Standards Program. Further, in consultation with stakeholders regarding the estimated time required for the entities to implement and come into compliance with the reliability standards, BC Hydro suggests effective dates for each of the Reliability Standards assessed. After a public comment process, the BCUC reviews BC Hydro's analysis and then may either approve or reject Reliability Standards. The BCUC does not have authority to alter or amend a standard. To date no standards have been rejected, although the provincial process can lead to delays before a FERC-approved Reliability Standard is adopted.

In Order G-171-10, issued on November 25, 2010, the BCUC approved an annual Implementation Plan created by WECC for 2011 that includes "a list of minimum [R]eliability [S]tandards to be actively monitored, methods to be used for monitoring, an Audit Plan, Self-Certification Program and Schedule, Periodic Information Submittal requirements and Exception Reporting process."[156] The BCUC has also issued orders approving annual Implementation Plans for subsequent years.[157]

---

[154] The specified penalties for contravention of Alberta Reliability Standards are available at: http://www.auc.ab.ca/rule-development/rule-027-specified-penalties-for-reliability-standards/Pages/default.aspx.

[155] The *Utilities Commission Act* is available at: http://www.bclaws.ca/Recon/document/ID/freeside/00_96473_01.

[156] Order No. G-171-10, issued by the BCUC, at p. 1, available at: http://www.bcuc.com/Documents/Orders/2010/DOC_26511_G-171-10_MRS-2011-Implementation-Plan.pdf.

[157] *See*, e.g., Order No. R-39-13, available at: http://www.bcuc.com/Documents/Orders/2013/DOC_38047_R-39-13_BC-Reliability_2014-Implementation-Plan.pdf (approving the Implementation Plan for the 2014 calendar year).

The standards in effect in British Columbia are generally listed in an attachment to the most recent order approving new or amended standards. NERC Reliability Standards and WECC regional Reliability Standards effective in British Columbia are also listed on the WECC website.[158] British Columbia has vested the BCUC with authority to levy monetary penalties for violations.

Data Sharing

WECC's relationship with the BCUC is governed by the Administration Agreement between the parties (dated October 8, 2009), the BCUC's *Rules of Procedure for Reliability Standards in British Columbia* (BCUC ROP), and BCUC's compliance monitoring program.[159] Under §3.2 of the Administration Agreement, WECC is required to immediately advise the BCUC and an applicable entity who has provided information to WECC if that information has been requested by NERC or a foreign government agency, unless disclosure of the request is prohibited by law. Therefore, WECC can only disclose confidential information related to possible violations if the BCUC approves the disclosure or by compulsion of law.

Under §6.3.1 of the BCUC ROP, the BCUC, in its discretion and upon request, may designate information as restricted.[160] If such designation is made, §3.6 of the Administration Agreement and the BCUC ROP prohibit WECC from transmitting the information outside of British Columbia. WECC can review the restricted information only at the offices of the applicable entity or at the BCUC. The applicable entity is not required to give WECC a copy of the restricted documents.

Under §3.1 of the Administration Agreement, WECC shall maintain the confidentiality of the confidential information and shall not disclose it even under conditions of confidence, except as provided in the Rules of Procedure, namely with BCUC approval. Section 3.1.1(ii) also prohibits WECC from disclosing documents or portion of documents that would potentially identify the source of the information. Finally, WECC cannot disclose any information if the BCUC directs WECC to keep it confidential.

Compliance

Under a contract with the BCUC, WECC performs compliance oversight for the province, including registration, monitoring and auditing functions and activities. However, the violations, enforcement, and penalty assessment functions remain with BCUC. Until recently, the BCUC had no monetary sanctions authority. BCUC now has authority to assess fines of up to $1 million per day. The process for imposing penalties for confirmed violations of reliability standards is under development.

---

[158] *See* http://www.wecc.biz/Standards/BCApproved%20Standards/Forms/AllItems.aspx.

[159] *See* Attachments 1 and 2 to Order No. G-123-09, issued by the BCUC, available at: http://www.bcuc.com/Documents/Orders/2009/DOC_23219_G-123-09_BCUC%20MRS.pdf.

[160] *See* http://www.bcuc.com/Documents/MRS/Rules-of-Procedure.pdf.

Manitoba

Reliability Standards

The *Manitoba Hydro Act* establishes the framework for Manitoba Hydro to adopt NERC Reliability Standards by authorizing Manitoba Hydro, subject to Lieutenant Governor in Council approval, to adopt:

> in whole or in part, any standards, rules, terms, conditions, guidelines or schedules, which are related to the planning, design or operation of generation or transmission facilities within an integrated regional power grid, established by [the North American Electric Reliability Council, Mid-Continent Area Power Pool or…] an industry organization, regional transmission group, regulatory body or other association or group or any other person.[161]

The *Manitoba Hydro Amendment and Public Utilities Board Amendment Act (Electricity Reliability)*[162] and its implementing regulations, which came into force on April 1, 2012, set the basis for the adoption of mandatory and enforceable NERC Reliability Standards in Manitoba. This legislation gives the Public Utilities Board of Manitoba (PUB) the authority to make determinations of noncompliance with Reliability Standards, to impose sanctions, and to remand a standard to NERC for reconsideration.

On April 1, 2012, all then-current NERC Reliability Standards became mandatory and enforceable in Manitoba. These standards are listed in Schedule 1 to the *Reliability Standards Regulation*.[163] The province reserved the right to adopt new or amended standards by regulation. The government is consulting with stakeholders as to the best process for considering and approving standards for application in Manitoba.

Compliance

The *Compliance Monitoring and Enforcement Program Province of Manitoba*, based on the NERC CMEP, was adopted as Schedule 2 to the *Reliability Standards Regulation*. MRO and NERC, as compliance bodies, will monitor Manitoba Hydro's compliance with NERC Reliability Standards. If a compliance body alleges that a violation of standards has occurred in Manitoba, it must apply to the PUB with a recommended enforcement action for a determination on whether a standard has been violated. MRO also makes recommendations to PUB regarding the imposition

---

[161] *See The Manitoba Hydro Act*, C.C.S.M. c.H190, s.16.3(1)(a), available at: http://web2.gov.mb.ca/laws/statutes/ccsm/h190e.php. The bracketed language above was stricken in *The Manitoba Hydro Amendment and Public Utilities Board Amendment Ac*t (dated June 11, 2009), and replaced with "an industry organization."

[162] Statutes of Manitoba 2009, c. 17.

[163] Available at: http://web2.gov.mb.ca/laws/regs/annual/2014/098.pdf.

of associated penalties or sanctions. The PUB will decide whether a violation of a standard has taken place and the penalty, if any, which should apply for noncompliance. The PUB can impose a penalty, with enforcement through a board order. When the PUB issues an order confirming a violation, NERC may make this fact and any attached penalties public.

NERC or MRO, in advising the PUB that they believe a violation has occurred, is also to advise on appropriate remedial actions, sanctions, or penalties.

Data Sharing

The compliance program requires timely data from registered entities to effectively monitor compliance with Reliability Standards.

All findings by PUB related to electricity reliability proceedings are made public through the issuance of orders. These orders will include the name of the registered entity, the Reliability Standard(s) and requirements(s) violated, whether the PUB agrees with MRO's findings and recommendations, and any penalties or sanctions imposed.

When the PUB issues an order confirming a violation, NERC may make this fact and any attached penalties public. The mitigation plan will not be made public until there is a confirmed violation. Similarly, final audit reports will be released to the public, but only after any alleged violations have become confirmed violations. Lastly, while compliance investigations are confidential, confirmed violations resulting from a compliance investigation will be made public.

New Brunswick

Reliability Standards

On October 3, 2008, NERC, the Minister of Energy of the Province of New Brunswick, and the New Brunswick System Operator (NBSO) signed a MOU that recognized NERC's role as the ERO and found that NERC is a "standards authority" within the meaning of the *New Brunswick Electricity Act*. NERC, NPCC, and NBSO have signed an MOU under which NERC and NPCC would monitor compliance and carry out enforcement as to NBSO. Under the MOU, NBSO was to monitor and enforce compliance with Reliability Standards by those entities within New Brunswick as a part of its market rules.

In October 2013, New Brunswick's legislation that amends how Reliability Standards are approved, monitored, and enforced received Royal Assent and was proclaimed (i.e., became effective). The *New Brunswick Electricity Act*[164] led to the amalgamation of NBSO with the NB Power Group of Companies. The system operation functions performed by NBSO are now performed within the vertically integrated New Brunswick Power Corporation (NBPC). In addition to its responsibility to comply with reliability standards applicable to its function, NBPC is also responsible for making filings to the New Brunswick Energy and Utilities Board (NBEUB) to update Reliability Standards, maintain a list of BPS elements, and to make recommendations on

[164] The *New Brunswick Electricity Act* is available at: http://laws.gnb.ca/en/ShowPdf/cs/2013-c.7.pdf.

compliance registrations. The NBSO's role in the adoption, monitoring, and enforcement of North American Reliability Standards has been transferred to the NBEUB.

The NBEUB may adopt FERC-approved NERC Reliability Standards that have been filed by NBPC. NERC Reliability Standards are filed and adopted with an accompanying NB Appendix to describe the specific application of the standard in New Brunswick. The NBEUB posts proposed Reliability Standards on its website for a 60-day review period prior to adoption. If the proposed Reliability Standard contains substantive revisions to the FERC-approved version, or if there are substantive comments received during the review period, the NBEUB may hold a hearing and may determine to approve, not approve, or remand the proposed Reliability Standard back to NBPC. A list of enforceable Reliability Standards is available on the NBEUB's website.[165]

Data Sharing

Confidentiality and public disclosure is governed by Part 7 of the *New Brunswick Compliance Monitoring and Enforcement Program* (NB CMEP) – Schedule A to the *Reliability Standards Regulation – Electricity Act*.[166] Any information that a registered entity provides to the NBEUB, NPCC, or NERC may be marked as confidential and may not be released to a third party without the written consent of the registered entity. The regulation provides for the public disclosure of finalized audit reports, confirmed violations, penalties, sanctions, and settlement agreements, including the name of the registered entity. The NBEUB is required to keep all CIP information confidential in accordance with §1500 of the NERC ROP.

Pursuant to the MOU, NERC provides information relevant to New Brunswick on issues relating to reliability, Reliability Standards, and compliance with Reliability Standards.

Compliance

The NBEUB implements a compliance monitoring system for reliability standards that is based on the requirements of the NERC compliance program. The NB program is documented as the NB CMEP – Schedule A to the *Reliability Standards Regulation – Electricity Act*. As a recognized compliance body under the regulations, NPCC assists the NBEUB with compliance monitoring activities according to a service agreement the NBEUB has executed with NPCC. The NBEUB will initiate enforcement action if it has reason to believe that a violation of a reliability standard has occurred. NBEUB requires that the entity take action to remove the risk the violation poses to the reliability of the BPS and to implement a plan that will prevent a future occurrence of the violation. Registered entities are subject to financial penalties and sanctions for violations of adopted reliability standards. A penalty matrix, provides ranges for penalties corresponding to VRFs and VSLs, is provided in the *Reliability Standards Regulation*.

[165] *See* http://www.nbeub.ca/index.php/en/electricity/reliability-compliance/118.

[166] New Brunswick's *Reliability Standards Regulation – Electricity Act* is available at: http://laws.gnb.ca/en/ShowPdF/cr/2013-66.pdf.

Nova Scotia

Reliability Standards

The Nova Scotia Utility and Review Board (NSUARB) is an independent, quasi-judicial body which exercises general supervision over all electric utilities operating as public utilities within the Province of Nova Scotia, pursuant to the *Nova Scotia Public Utilities Act*.[167] Nova Scotia Power Incorporated (NPSI) is a public utility in Nova Scotia and is a member of NERC and NPCC. The Nova Scotia Department of Energy is responsible for energy and electricity policy in the province.

NERC has signed two separate MOUs with entities in Nova Scotia: one with NSUARB, and one with NSPI.[168]

NERC submits standards to NSUARB and NSPI for approval; each organization may approve, modify, remand or dismiss the standard as not applicable, though final approval authority rests with NSUARB. NSUARB has a quarterly review process allowing the submission, by NERC, of standards already approved by FERC. NSUARB will only process an application after FERC has approved or remanded the Reliability Standard in the United States.[169] NERC made an initial filing of Reliability Standards on June 30, 2010 along with the *Glossary of Terms Used in NERC Reliability Standards*. Nova Scotia approved this filing on July 20, 2011. None of the proposed standards were changed or rejected.

On September 2, 2011, NERC made its first quarterly filing to Nova Scotia that included a list of Standards approved by FERC in the period of time since the June 30, 2011 filing. This filing was approved.

In June 2012, the NSUARB proposed an expedited process for its review of NERC quarterly filings. This was approved for implementation in August 2012. With respect to the quarterly filing, NSPI and NPCC have 10 days to comment if they wish. At the end of the comment period, the NSUARB will decide if, based on any comments, a more rigorous review is required. If a more rigorous review is deemed required it will be undertaken; otherwise, the NSUARB will issue its decision. To date, all filings have been approved without additional review.

Under the MOU with NPSI, NSPI agrees to comply with NERC's Reliability Standards. NPSI also committed to review and provide recommendations on the adoption of Reliability Standards.

---

[167] The *Nova Scotia Public Utilities Act* is available at: http://nslegislature.ca/legc/statutes/public%20utilities.pdf.

[168] The NSUARB and NERC signed an MOU on December 22, 2006, in which NERC and the NSUARB agreed to a cooperative relationship to improve the reliability of the North American BPS. On May 11, 2010, NERC, NPCC, and NSPI signed an MOU which memorializes the working relationship between the three entities to improve reliability of the grid in Nova Scotia and North America. Both MOUs are available at: http://www.nerc.com/filingsorders/ca/pages/canadian-mous.aspx.

[169] The date of the order is considered the effective date for the adopted Reliability Standards.

Data Sharing

The MOU states that NSPI will provide NPCC all information respecting reporting requirements in the CMEP for NERC Reliability Standards.

Under the MOU, NERC has agreed to share relevant information on issues related to reliability compliance with the NSUARB. Examples of such information include:

(1) Compliance audits and spot checks;

(2) Readiness evaluations;

(3) Disturbance reports;

(4) Reliability assessments and benchmarking information; and

(5) Reports by regional reliability organizations, where applicable.[170]

There is also a data sharing requirement relevant to the Reliability Standards process. The MOU with NSUARB calls for NERC to submit all NERC Board of Trustees-approved Reliability Standards to the NSUARB. NERC also agreed to notify NSUARB immediately if a Reliability Standard has been remanded in another jurisdiction.

With respect to enforcement matters, the MOU states that the NSUARB and NERC will work together to establish a system for disclosure by NERC of violations to provide for assessment and reporting by NERC of inter-region reliability risks to or from entities outside of Nova Scotia where coordinated action is required to address those risks.

Compliance

Compliance is mandatory in Nova Scotia. NPCC as the regional Entity maintains the list of all market participants of the BES who must comply with approved reliability standards. NPCC provides recommendations to NSPI and may also identify organizations that may be candidates for registration and assign them to the compliance registry. The registry is based on the NERC functional model and registry criteria. The NSUARB will monitor compliance and accept compliance information and recommendations from NERC. NERC, NPCC and NSUARB may all suggest compliance violation; proceedings shall be conducted under the NSUARB's direction and control. NERC may recommend a particular penalty for any violation, but NSUARB will be responsible for determining if a violation occurred and what penalties should be imposed.

NSPI is subject to NERC's CMEP as implemented by NPCC.

[170] *See* MOU between the NSUARB and NERC at pp. 2-3.

Ontario

Reliability Standards

The Ontario Minister of Energy is responsible for the legislation that governs the Ontario Energy Board (OEB) and the Independent Electricity System Operator (IESO) and for energy and electricity policy in the province. The IESO of Ontario is a not-for-profit corporate entity established under the *[Ontario] Electricity Act, 1998*,[171] and is subject to the oversight authority of the OEB. The OEB is responsible for regulating the electricity sector, and it has the legislative authority to stay or revoke the operation of a reliability standard in Ontario and refer it back to NERC or NPCC for further consideration.

On October 25, 2006, the OEB and NERC signed an MOU[172] setting forth the mutual understanding of each party's responsibilities with respect to reliability in the Province of Ontario. The MOU states that Ontario's legislative framework does not expressly contemplate approval of NERC Reliability Standards, By-laws or Rules of Procedure. The MOU recognizes that, under the Ontario Electricity Act, one of the IESO's objectives is to participate in the development of standards relating to the transmission system and to enforce those standards. The MOU confirms that NERC Reliability Standards are referenced generically in the Market Rules written and administered by the IESO, and they are considered in effect in Ontario upon expiration of the remand period. On November 28, 2006, the Ontario Ministry of Energy formally recognized NERC as the entity named as a "standards authority" in the *Electricity Act, 1998*. Subsequently, in 2008, the *Electricity Act, 1998* was amended, allowing for NPCC to be recognized as a standards authority.

An MOU between the IESO, NPCC, and NERC was signed on November 29, 2006 and amended on February 5, 2010. This MOU documents the roles of the parties in conformance with the Ontario reliability framework and commits the IESO to carry out a compliance enforcement program for Ontario entities. The MOU also acknowledges that the NERC Rules of Procedure have effect in Ontario, provided they do not conflict with the established reliability and compliance framework in Ontario. The amended MOU includes provisions for investigations, organization registration, and NERC certification.[173] The IESO is subject to NERC's CMEP processes in accordance with the MOU. Monitoring and enforcement activities, with the exception of financial sanctions, are performed by NPCC.

While there continues to be no formal approval of NERC Reliability Standards in Ontario, there is a process for a Reliability Standard to be rejected or remanded. This process provides for market participants, the IESO, or the OEB itself to initiate a review that could result in a standard

[171] Ontario's *Electricity Act, 1998* is available at: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_98e15_e.htm.

[172] Both the 2006 MOU and the 2010 MOU described in the following paragraph are available at: http://www.nerc.com/filingsorders/ca/pages/canadian-mous.aspx.

[173] In general, such NERC compliance processes do not involve direct participation by Ontario market participants.

being remanded or revoked for application in the province. Only Reliability Standards approved by the NERC Board of Trustees on or after May 14, 2008 are subject to this process.

Ontario was the first jurisdiction in North America to adopt NERC Reliability Standards as mandatory and enforceable. Until July 2011, a NERC Reliability Standard became effective on the date specified by the NERC Board of Trustees when it approved the standard. Because of the uncertainties in the timing of FERC approvals, a standard typically came into effect earlier in Ontario than in adjoining U.S. jurisdictions. An Ontario Market Rule amendment effective July 8, 2011 addressed this mismatch. Under this Market Rule,[174] a NERC Reliability Standard will become effective when it is declared mandatory and enforceable in the U.S., unless the OEB remands the Reliability Standard or otherwise stays its enforceability. In addition, any Reliability Standard approved by the NERC Board of Trustees under NERC Rule 321 (i.e., a standard responsive to a regulatory directive that has not been approved by the NERC RBB) must be approved by IESO before it can comes into effect in Ontario.

To date, Ontario has neither remanded nor modified any NERC Reliability Standards. Information regarding Reliability Standards in Ontario can be found on the IESO's website.[175]

Data Sharing

Under the MOU, NERC will provide the OEB with information relevant to Ontario on issues related to compliance with NERC Reliability Standards, including reports on:

(1) Compliance audits and spot checks;

(2) Readiness audits;

(3) Disturbance reports;

(4) Reliability assessments and benchmarking information; and

(5) Reports by regional reliability organizations, where applicable.

The MOU also calls for NERC to inform the OEB of Reliability Standards approved by NERC and submitted to appropriate regulatory authorities, and to notify the OEB of NERC Reliability Standards that are remanded to NERC in any jurisdiction outside of Ontario. The MOU states that the IESO is the only Ontario entity directly accountable to NERC for its own compliance and will be accountable to NERC for compliance by all Ontario entities with NERC Reliability Standards.

In the MOU, there is also an undertaking that, subject to confidentiality requirements, the IESO will advise NERC of the functional responsibilities of Ontario entities.

---

[174] *See Market Rules for the Ontario Electricity Market*, ch. 5, Bulk Power System Reliability, available at: http://ieso-public.sharepoint.com/Documents/marketRules/mr_marketRules.pdf.

[175] *See* https://www.ieso.ca/imoweb/ircp/reliabilityStandards.asp.

Compliance

The IESO is subject to NERC's CMEP, with the exception that the IESO is not subject to financial sanctions.

Compliance enforcement within Ontario, i.e., of Ontario market participants, is conducted by the IESO's Market Assessment and Compliance Division, which is "ring-fenced" from the rest of the organization. The IESO is subject to assessments of compliance with NERC Reliability Standards, including audits performed by NPCC. The MOU provides NPCC and NERC the right to draw their own conclusions with respect to a compliance investigation of Ontario entities, but with limited authority to impose financial sanctions on the IESO only.

The IESO carries out a compliance enforcement program and can issue a monetary order, finding, or remedial action with respect to a violation of a Reliability Standard in Ontario, subject to appeal to the OEB. The IESO has delegated enforcement accountability to the Market Assessment and Compliance Division, which exercises independent discretion in terms of enforcement decision-making.

The Market Assessment and Compliance Division establishes and executes procedures and programs for monitoring, investigating, and imposing sanctions, including financial penalties, against market participants and the IESO itself. The MOU acknowledges the Market Assessment and Compliance Division as the enforcement body in Ontario for Reliability Standards with full sanctioning powers as afforded under the Market Rules for breaches committed by the IESO and Ontario market participants.

In the event that a violation is confirmed under the Market Rules, the name of the responsible entity is made public. The Market Assessment and Compliance Division has the authority to levy sanctions for reliability violations. These sanctions may include financial penalties and are subject to appeal to the OEB. The Market Assessment and Compliance Division has established sanctions guidelines similar to those of NERC using severity/impact criteria. It has authority for "Extraordinary Financial Penalties" under certain circumstances to assess penalties of up to $1 million per occurrence. The OEB can impose administrative penalties of up to $20,000 per day.

Québec

Reliability Standards

The Régie de l'énergie du Québec (Régie) is an independent agency established under the *Act Respecting the Régie de L'Énergie* (Régie Act) to regulate the province's electricity and natural gas sectors. On December 8, 2006, NERC and the Régie signed an MOU that contemplated a future amendment to Québec's reliability legislation to grant the Régie the power to adopt and enforce NERC standards and allow for NERC funding and oversight in the province of Québec.[176]

[176] NERC-Canadian MOUs are available at: http://www.nerc.com/filingsorders/ca/pages/canadian-mous.aspx.

The MOU noted that §73.1 of the Régie Act provides that the "electric power carrier," or Hydro-Québec, will establish reliability standards for its electric power transmission system and submit them to the Régie for approval. According to the MOU, the standards will become mandatory after approval by the Régie.

On December 13, 2006, Québec implemented *An Act Respecting the Implementation of the Québec Energy Strategy and Amending Various Legislative Provisions*,[177] which grants the Régie jurisdiction over a mandatory reliability standards framework in the Province of Québec. This act formalizes the ability of the Régie to approve reliability standards after reviewing an evaluation of the relevance and impact of the proposed standards. Under the act, the Régie may request that the Reliability Coordinator modify a standard or submit a new one. Further, the Reliability Coordinator must submit guidelines to the Régie describing criteria to be taken into account in determining sanctions for noncompliance with reliability standards and identify owners or operators that will be subject to the standards approved by the Régie.

On June 2, 2009, the RC filed an application seeking the adoption of 95 NERC Reliability Standards applicable in Québec, in French and English, along with an evaluation of the relevance and impacts of standards filed with the Régie. The filing also called for the approval of Registers of Entities and of Facilities, and approval of a *Glossary of Terms Used in NERC Reliability Standards*, among other things. The entities' and facilities' registers, as filed for approval, also provide interpretations regarding standard applications within Québec, and among other matters, a BES definition for the Québec Interconnection that is more stringent than NPCC's BPS definition.

In a partial decision issued on May 13, 2011, the Régie approved the content of the submitted NERC Reliability Standards.[178] In addition, the Régie accepted the Main Transmission System to be the system that defines the transmission and generation facilities to which Reliability Standards are applicable (TO, GO, GOP, TOP). The partial decision also called for a number of changes in how the standards and appendices are presented and for a review of the translation of the standards into French. The Régie is working to ensure the French version of the standards is as close in meaning to the English version as possible. The Régie will establish a timetable for filing of revised versions of the standards in English and French for final adoption. Accordingly, no NERC Reliability Standards have been formally adopted nor made effective in Québec.

The second agreement among NERC, the Régie, and NPCC regarding implementation of mandatory Reliability Standards in Québec has been developed, and the agreement is under consideration by the Québec provincial government. The Régie has issued a decision to adopt a second group of Reliability Standards for Québec, which brings the total number of adopted standards in Québec to 35. Following public hearings which took place in October 2013, it is expected that the Régie will issue a decision concerning a third group of standards. Hydro-Québec

[177] Available at: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2006C46A.PDF.

[178] A list of these approved Reliability Standards is available at: http://www.regie-energie.qc.ca/audiences/3699-09/Demande_3699-09/B-1_HQCME-2Doc1_3699_02juin09.pdf.

TransÉnergie, the Québec RC, has initiated a consultation process on 18 NERC Reliability Standards that will be filed with the Régie once its decision on the third group of standards is issued. This filing is expected before the end of 2014. The review of the Sanction Guide proposed by Hydro-Québec TransÉnergie and the determination of Reliability Standards enforcement dates remains pending.

Data Sharing

Under the MOU, NERC has agreed to share relevant information on issues related to reliability compliance with the Régie. The MOU further states NERC will be invited to participate in compliance audits and readiness evaluations done in Québec. Under the MOU, NERC and the Régie also agreed to discuss issues relating to: (i) Reliability Standard approval and remand; (ii) penalties for noncompliance with standards; and (iii) funding. For instance, NERC has agreed to notify the Régie when a new or modified standard is approved in the U.S. or remanded by any other jurisdiction outside of Québec. Additionally, although it is recognized that NERC cannot impose financial penalties for violations of Reliability Standards in Québec, NERC has agreed to inform the Régie of any violations and of the corresponding amount of penalties associated with such a violation in the United States.

Compliance

The Régie is responsible for compliance and enforcement. If NERC or NPCC determines that an entity subject to a Reliability Standard is not in compliance with the Reliability Standard, it shall report to the Régie on its findings and may recommend the application of a sanction. Ultimately, the Régie will determine if there has been a violation and will determine any appropriate penalty.

The RC must submit guidelines to the Régie describing criteria to be taken into account in determining sanctions for noncompliance with Reliability Standards and identify owners or operators that will be subject to the standards approved by the Régie. The intent, once all agreements are in place, is that NPCC and NERC will act as the Régie's agents in developing and delivering a comprehensive CMEP, subject to the approval of the Régie. As the first limited list of mandatory standards have only recently come into effect, and as the governmental authorities have not approved the agreement covering compliance arrangements, there has been limited compliance activity under the formal Québec regime.

The agreements note that NERC cannot impose financial penalties, but should recommend to the Régie what would be an appropriate sanction for a particular violation. The RC did submit a sanctions guide to the Régie as required. However, the regulator decided to postpone considering this until the second agreement covering compliance monitoring is approved by the governmental authorities. Under the provincial regime, the Régie may impose, if appropriate, a sanction that may not exceed $500,000 per day and set a deadline for payment.

Saskatchewan

Reliability Standards

Pursuant to *The Power Corporation Act*,[179] Saskatchewan Power Corporation (SaskPower) has the authority to adopt, set, and administer standards for the planning, design, or operation of transmission lines, equipment, or other facilities within the Saskatchewan integrated regional power grid, and to maintain a membership in an integrated regional power organization. NERC, MRO, and SaskPower entered into an MOU that became effective on February 3, 2009 and was amended on January 15, 2012.[180] The MOU reflects the intent of Saskatchewan to support common North American BPS standards and to describe the protocols to achieve such a goal. For purposes of the MOU, NERC, and MRO are recognized to be Saskatchewan's electric Reliability Standard setting bodies.

Reliability Standards approved by the NERC Board of Trustees are automatically adopted in Saskatchewan, unless one of the following two conditions applies. First, if a particular standard has been remanded by any jurisdiction, the Reliability Standard will not be applicable in Saskatchewan. Second, a Reliability Standard will not be applicable in Saskatchewan if is remanded, set aside, or a variance has been requested. Under the MOU, once the Reliability Standard is adopted, compliance with the standard is required in Saskatchewan.

Data Sharing

The MOU between MRO, SaskPower, and NERC does not have an explicit provision regarding public disclosure of violations.

Compliance

Under SaskPower's legislative authority, the oversight unit within SaskPower serves as the monitoring, compliance, and enforcement authority for the province. MRO currently performs on-site compliance audits for SaskPower. While not delegating its reliability authority, SaskPower aligns its compliance program, to the degree reasonable, to the compliance and monitoring processes established by NERC and MRO.

The process includes, but is not limited to, the following three functions:

(1) Oversight (including remand, set aside, and compliance findings);

(2) Standards development (including the coordination of assessments, communication, and internal education); and

[179] Available at: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/P19.pdf.

[180] NERC-Canadian MOUs are available at: http://www.nerc.com/filingsorders/ca/pages/canadian-mous.aspx.

(3) Compliance and enforcement (including management of an internal and external auditing function, which will give Saskatchewan the ability to make formal findings of compliance and noncompliance and to order and enforce mitigation plans to be implemented).

The oversight unit within SaskPower would make any determination of a violation. There is no provision for financial or other sanction. The oversight unit can impose a mitigation plan on a noncompliant entity.

National Energy Board

Reliability Standards

NERC and the NEB signed an MOU in 2006. The MOU recognizes NERC as the ERO. In the MOU, NERC and the NEB commit to coordinate in the promotion of a reliable North American BPS.

The NEB regulates the construction and operation of international power lines in accordance with, among other things, the *National Energy Board Act* and the *National Energy Board Electricity Regulations*.[181] The NEB has authority under its legislative framework to take certain enforcement measures in the case of noncompliance to the conditions of a permit or a certificate that was issued for an international power line.

While initially the NEB did not have an authority to make Reliability Standards mandatory and enforceable on international power lines, this was changed with the passage of NEB's *General Order MO-036-2012 for Electricity Reliability Standards* and five amending orders for Electricity Reliability Standards in December 2012 (NEB General Order).[182]

The provisions of the NEB General Order contain twelve Reliability Standards requirements that correspond to the main categories of Reliability Standards developed by NERC. The requirements are defined broadly so that they may include regional variations and can be harmonized with provincial regulatory frameworks as they relate to Reliability Standards.

In the NEB General Order, the NEB did not itself adopt any NERC Reliability Standards. Rather, the NEB General Order requires that international power line owners file with the NEB a list of Reliability Standards adopted by the provincial system to which the international power line connects. The NEB General Order requires international power line owners or permit holders to identify these Reliability Standards and to keep the NEB advised of any changes. Accordingly, there is no list of the NEB-approved Reliability Standards, nor does the NEB make determinations of effective dates. The NEB also committed to working with the provinces, utilities and other reliability authorities including NERC to avoid, to the extent possible, the generation of duplicate

[181] NEB maintains a list of acts and regulations that set forth its mandate, responsibilities, and powers at: http://www.neb-one.gc.ca/clf-nsi/rpblctn/ctsndrgltn/lstctsndrgltn-eng.html.

[182] The NEB General Order is available at: http://www.neb-one.gc.ca/clf-nsi/rpblctn/ctsndrgltn/rrggnmgpnb/lctrcty/lctrcty-eng.html.

reporting requirements. However, international power line owners are required to submit to the NEB reports of noncompliance with Reliability Standards.

Data Sharing

NERC and the NEB have committed to exchange of experience, information and data relating to the development and compliance with Reliability Standards as applicable to international power lines. The MOU commits NERC to informing and seeking input from the NEB on proposed changes to NERC's Bylaws or ROP. The MOU also commits NERC to inform the NEB when a SAR has been approved and assigned to a drafting team, and to notify NEB when a Reliability Standard is approved.

Under the MOU, NERC commits to notify the NEB at the stage of its development process where the Standards Committee approves a SAR and assigns it for development by a drafting team. The NEB agrees to inform NERC about any changes in its regulatory processes to allow formal approval of NERC Reliability Standards.

Compliance

Consistent with its approach to adopting standards, the NEB has not imposed its own additional compliance monitoring and enforcement regime. The NEB General Order requires international power line permit holders to provide the NEB with certain compliance information, based on the compliance program of the jurisdiction where the international power line is located. In 2012, legislation was passed to provide the NEB with authority to establish a system of Administrative Monetary Penalties (AMP) through regulations in order to promote compliance with the *National Energy Board Act*. The penalties can be up to $100,000 per day for violations levied on companies. Lesser amounts can be levied on individuals. The NEB's regulations on how the AMP would be applied came into force in mid-2013.

There currently is no specific provision that violations would be made public.

Mexico

Baja California

Reliability Standards

The Comisión Federal de Electricidad (CFE), through the Centro Nacional de Control de Energia (CENACE), and the Area de Control Baja California (ACBC) have entered into a MOA with WECC. The MOA provides that WECC assist CENACE and ACBC in monitoring compliance with Mexico Reliability Standards for Baja California, Mexico. CENACE has approved the following Mexico Reliability Standards:

- BAL-001-MX-0 (Real Power Balancing Control Performance)
- BAL-006-MX-0 (Inadvertent Interchange)

- CIP-001-MX-0 (Sabotage Reporting)
- INT-001-MX-0 (Interchange Information)
- INT-003-MX-0 (Interchange Transaction Implementation)
- PER-001-MX-0 (Operating Personnel Responsibility and Authority)
- PER-002-MX-0 (Operating Personnel Training)
- PER-003-MX-0 (Operating Personnel Credentials)
- VAR-002-WECC-MX-0 (Automatic Voltage Regulators (AVR))
- VAR-501-WECC-MX-0 (Power System Stabilizer (PSS))

CFE participates in the NERC Reliability Standards and WECC regional standards development process to develop standards.

Compliance

WECC uses a compliance monitoring program[183] to monitor and assess compliance with Mexico Reliability Standards applicable to Designated Entities,[184] consistent with the applicable law of Mexico and relevant agreements. If there is any conflict between the MOA and the CMP, the MOA prevails.

WECC does not have enforcement or registration/designation authority for CFE. WECC provides compliance monitoring, reviews mitigation plans and completed mitigation plans, and provides assessment recommendations with respect to alleged violations.

[183] The 2014 implementation plan for Mexico Reliability Standards, together with other CFE-related documents and compliance information, is available at: http://www.wecc.biz/compliance/Baja_CFE/Pages/Baja-English.aspx.

[184] "Designated Entities" are the Mexican equivalent of registered entities in the United States.

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 2

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

JOINT REGIONAL ENTITY SELF-ASSESSMENT

JULY 21, 2014

Attachment 2

TABLE OF CONTENTS

INTRODUCTION 1

A. Satisfaction of Statutory and Regulatory Criteria 1

B. Achievements 4

C. Improvement Opportunities 5

D. Regional Reliability Standards 7

1. Regional Reliability Standards Processes 7
2. Regional Fill-in-the-Blank Standards and Regional Criteria 10
3. Prioritization of Standards Work 11

E. Organization Registration and Certification 12

1. Organization Registration 12

a. The Scope of the Registration Criteria 18
b. Re-examination of Functional Model Definitions 19
c. Oversight of Multi-Regional Entities 20
d. Transfer of Registered Entities between Regional Entities 20
e. Applicability of Reliability Standards to Federal Entities 21

2. Organization Certification 21

F. Compliance Monitoring and Enforcement Program 22

1. Development and Status of the Compliance Monitoring Enforcement Program 22

a. Development of Single ERO-Wide Audit Process Checklist and Associated Auditor Handbook 30
b. Implementation of FFT Enhancements 31
c. Improvements in the Self-Reporting Process 31

2. Updates to the 2009 Joint Regional Entity Self-Assessment 32

a. Consistency 33
b. Compliance Monitoring 35
c. Enforcement 38
d. Hearings and Appeals 42

3. Additional Statutory Functions 44

a. Reliability Assessment 44
b. Event Analysis 45
c. Situation Awareness 46
d. Critical Infrastructure Protection 47

4. Budget 49

CONCLUSION 50

Appendix A: Description of Regional Entities

Appendix B: Regional Entity Responses to Specific Concerns Raised in the Commission's September 16, 2010 Order on the Three-Year ERO Performance Assessment

Appendix C: Regional Entities' Satisfaction of Statutory and Regulatory Criteria

INTRODUCTION

The Regional Entities are pleased to have the opportunity to submit jointly a self-assessment of their performance for 2009 through 2013, to the Federal Energy Regulatory Commission (Commission or FERC), as part of the *Five-Year Electric Reliability Organization (ERO) Performance Assessment Report* prepared by the North American Electric Reliability Corporation (NERC).[1] While their corporate structures may vary, the Regional Entities are uniformly committed to working together and with the ERO to ensure the reliability of the bulk power system (BPS) in the U.S., and, where applicable, in Canada and Mexico. They are likewise dedicated to create seamless implementation of the law and policies administered by the Commission and the ERO. In light of the commonality of these overarching objectives, under the leadership of the Regional Entity Management Group (REMG), the Regional Entities prepared this 2014 Joint Regional Entity Self-Assessment (JRESA), which they respectfully request that the Commission accept.

The main purpose of this self-assessment is to demonstrate that the Regional Entities continued during the assessment period to satisfy the statutory and regulatory criteria for certification as part of the ERO. In this regard, in its order accepting the ERO's Three-Year Performance Assessment, the Commission explicitly directed that future assessments of the Regional Entities include a separate section assessing each Regional Entity's satisfaction of those criteria.[2] This self-assessment also provides an update on issues and concerns raised in the 2009 JRESA, specifically with respect to regional Reliability Standards, organization registration and certification, the compliance monitoring and enforcement program, and additional statutory functions.[3]

A. Satisfaction of Statutory and Regulatory Criteria

Section 215(e)(4) of the Federal Power Act (FPA), 16 U.S.C. §824o(e)(4), as reiterated in §39.8 of the Commission's regulations, 18 C.F.R. §39.8 (2013), provides that a Regional Entity must satisfy the following criteria to be delegated "authority for the purpose of proposing reliability standards to the ERO and enforcing reliability standards:"

---

[1] The eight Regional Entities are: (i) Florida Reliability Coordinating Council, Inc. (FRCC); (ii) Midwest Reliability Organization (MRO); (iii) Northeast Power Coordinating Council, Inc. (NPCC); (iv) ReliabilityFirst Corporation (ReliabilityFirst or RF); (v) SERC Reliability Corporation (SERC); (vi) Southwest Power Pool Regional Entity (SPP RE) — an independent and functionally separate division of Southwest Power Pool, Inc. (SPP); (vii) Texas Reliability Entity, Inc. (Texas RE or TRE); (viii) and Western Electricity Coordinating Council (WECC). A description of each of the individual Regional Entities can be found at Appendix A.

[2] *See North American Electric Reliability Corporation*, Order on the Electric Reliability Organization's Three-Year Performance Assessment, 132 FERC ¶ 61,217 (2010), at P 36. The Commission also discussed specific concerns regarding each of the individual Regional Entities in the order on the three year assessment. *Id*. PP 198-244. The responses of the individual Regional Entities to those concerns can be found at Appendix B.

[3] The instant self-assessment will not repeat the discussion on the framework of self-regulation and delegation, found at pp. 12-18 of the 2009 JRESA, as that discussion was more appropriate for an assessment of the initiation of the reliability paradigm; however, opportunities to improve that structure are discussed *infra* pp. 6-8.

(1) The Regional Entity is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board.

(2) The Regional Entity meets the requirements otherwise applicable to the ERO in FPA §215(c)(1)(2), 16 U.S.C. §824o(c)(1)(2), namely that it (a) has the ability to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk-power system; and (b) has established rules that (i) assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure, (ii) allocate equitably reasonable dues, fees, and other charges among end users for all activities, (iii) provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties, (iv) provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties, and (v) provide for taking appropriate steps to gain recognition in Canada and Mexico.

(3) The Regional Entity operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability.

Each of the eight Regional Entities continued to satisfy the statutory and regulatory criteria during the assessment period, as demonstrated with specificity on Appendix C and summarized briefly here.

The Regional Entities met the first criterion by being governed by an independent board (SPP RE and WECC (as of January 1, 2014)), a balanced stakeholder board (FRCC and SERC), or a combination independent and balanced stakeholder board (MRO (as of January 1, 2013), NPCC, RF, TRE, and WECC (during the assessment period)).

The Regional Entities fulfilled the next requirement to develop and enforce Reliability Standards that provide an adequate level of reliability of the BPS by working closely with NERC and stakeholders in the development of continent-wide standards and in the implementation and improvement of the Compliance Monitoring and Enforcement Program (CMEP). In particular, although each Regional Entity had a regional Reliability Standards Development Procedure (RRSDP), with the exception of WECC, they developed few regional Reliability Standards during the assessment period. They preferred to support NERC's efforts to develop continent-wide standards and focus their resources primarily on monitoring compliance with, and enforcement of, the mandatory Reliability Standards. Illustratively, during the assessment period, the Regional Entities conducted 2,358 compliance audits and 1,612 compliance spot checks, and processed 4,740 self-reports. They discovered nearly 6,900 violations or possible violations of the mandatory Reliability Standards, and submitted through NERC 5,128 confirmed violations in 633 Notices of Penalty (NOPs) to the Commission. They also explored ways to approach their compliance and enforcement responsibilities with a greater emphasis on

measuring the risk of noncompliance on the reliability of the BPS. In this regard, in collaboration with NERC, they developed the Reliability Assurance Initiative (RAI).[4]

The Regional Entities also established rules to ensure impartiality in the conduct of their business and due process in the performance of their compliance and enforcement functions, and, where applicable, took the appropriate steps to gain recognition in and otherwise work with entities in Canada and Mexico. To start with, they followed the NERC Rules of Procedure (ROP), as approved by the Commission, and adopted additional procedures and policies for their own areas. Thus, for example, they all relied on NERC ROP *Sanction Guidelines*, Appendix 4B, CMEP, Appendix 4C, and *Hearing Procedures,* Attachment 2 to Appendix 4C to carry out their compliance, enforcement, and hearing responsibilities fairly and impartially. They augmented those rules with policies and procedures to prevent conflicts of interest in the operation of their boards of directors or trustees, the exercise of their statutory duties, and the activities of their employees and contractors. They also followed NERC's lead, again as approved by the Commission, in equitably recovering their funding from end users through a formula based on net energy for load (NEL), and developed annual business plans and budgets for Commission approval to assure that they properly and adequately accounted for those funds. As noted, while they generally forwent the development of regional Reliability Standards during the assessment period, the Regional Entities participated in the development and improvement of the NERC Reliability Standards while maintaining their RRSDPs in the event they were needed. Finally, three of the Regional Entities with international footprints—MRO, NPCC, and WECC—made appropriate arrangements with Canadian border provincial authorities and utilities to coordinate the oversight of Canadian and U.S. reliability efforts, and WECC entered into a memorandum of understanding with the Mexican energy regulator under which WECC acts as a compliance monitor for certain activities in Baja California, Mexico.

Finally, the Regional Entities satisfied the statutory and regulatory criterion for maintaining their delegated authority by operating under agreements with NERC that promoted effective and efficient administration of BPS reliability. As described by the Commission when it first approved NERC's delegation agreements with the Regional Entities (RDAs) in 2007, NERC delegated authority under those agreements to the Regional Entities to audit, investigate, and otherwise ensure that users, owners, and operators of the BPS comply with NERC's mandatory Reliability Standards, subject to ERO oversight.[5] The RDAs further addressed regional Reliability Standards development, registration of entities that must comply with Reliability Standards, and other services supporting NERC's functions, including reliability assessments, event analysis, and training and education. In October 2010, the Commission again approved (revised) RDAs between NERC and each of the eight Regional Entities.[6]

[4] Regional activity and actions in regard to standards development and the CMEP, in particular RAI, are discussed later in greater detail under those headings.

[5] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,060, *order on reh'g,* 120 FERC ¶ 61,260 (2007).

[6] *See North American Electric Reliability Corporation*, 133 FERC ¶ 61,061 (2010), *order on reh'g*, 134 FERC ¶ 61,179, *order on compliance filing*, 137 FERC ¶ 61,028 (2011).

Subsequently, the Commission also approved other changes to specific regional agreements.[7] In brief, the Regional Entities functioned during the assessment period under RDAs with NERC that were comprehensively reviewed and ultimately approved by the Commission to promote effective and efficient administration of BPS reliability.

As a separate but related matter, each of the Regional Entities underwent at least one extensive audit by the Commission staff during the assessment period. Most of these audits evaluated the Regional Entities' budget formulation, administration, and execution, and focused on the costs and resources used to achieve program objectives in fulfilling the duties delegated to them by the ERO under FPA §215.[8] The final audit reports concluded that the Regional Entities had policies, procedures, and controls that facilitated their carrying out, in an effective and efficient manner, their responsibilities under their RDAs and bylaws, as well as their budget obligations. Several other audits more closely examined the structures of the regional organizations, and made recommendations in particular with respect to separation of functions.[9] In all of these proceedings, during the assessment period, the Regional Entities completed or were in the process of completing the corrective actions suggested by the Commission or its staff. The Regional Entities believe that the overall conclusions and recommendations in the Regional Entity audits underscore that they satisfied the statutory and regulatory criteria for maintaining the authority delegated to them by the ERO.[10]

B. Achievements

Closely intertwined in the Regional Entities' satisfaction of the statutory and regulatory certification criteria during the assessment period were their achievements as individual organizations and as a group united by common goals. Their individual achievements are partly set forth in Appendix C, and discussed or referenced throughout this document. Their joint achievements are, by definition, likewise discussed throughout this document. These achievements in particular reflect the work and oversight of the REMG, an organization composed of the executives of the eight Regional Entities to provide strategic guidance in the execution of their RDAs, consistent with maintaining and enhancing reliability across North

[7] *See*, e.g. *North American Electric Reliability Corporation*, Docket Nos. RR13-7-000 (Aug. 19, 2013) (TRE), RR13-5-000 (June 12, 2013) (MRO), RR12-12-000 (Oct. 24, 2012) (RF), RR12-4-000 (June 12, 2012) (FRCC), and RR12-2-000 (March 1, 2012) (WECC) (unpublished delegated letter orders).

[8] *See* delegated letter orders and final audit reports issued in *North American Electric Reliability Corporation*, Docket Nos. FA12-14-000 (May 9, 2013) (MRO), FA12-7-000 (May 9, 2013) (RF), PA12-10-000 (June 28, 2013) (NPCC), FA12-6-000 (June 11, 2013) (SERC), PA11-2-000 (October 5, 2011) (SPP RE), and PA12-9-000 (July 10, 2013) (WECC) (unpublished delegated letter orders).

[9] *See Florida Reliability Coordinating Council, Inc*., 131 FERC ¶ 61,262 (2010); *Western Electricity Coordination Council*, 132 FERC ¶ 61,149 (2010); *Texas Regional Entity*, 130 FERC ¶ 61,025 (2010).

[10] NERC also audited the Regional Entities during the assessment period, in accordance with the Commission's direction in Order No. 672. *See 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 (2006), at P 773. Specifically, NERC developed a program to audit the Regional Entities' adherence to the NERC ROP, the CMEP, and the requirements of the Regional Delegation Agreements. *See* generally http://www.nerc.com/pa/comp/Audits%20of%20Regional%20Entities%20DL/Forms/AllItems.aspx.

America for the benefit of all BPS users, owners, and operators. The REMG aims to attain that objective by promoting information sharing, transparency, and consistency with and among the Regional Entities while assuring efficient and effective use of resources to execute their delegated functions. In addition, the REMG combines the Regional Entities' efforts with the ERO Executive Management Group (ERO EMG), which was chartered originally in April 2010, and likewise dedicated to provide guidance and direction in the execution of the RDAs.

As particularly relevant to the rest of this self-assessment, in the summer of 2012, the REMG held its first strategic retreat, and decided upon three priorities: (i) to ensure that their work, especially in the audit area, follows professional standards and as a result fosters consistency among the Regional Entities; (ii) to reserve enforcement for serious matters, rather than using enforcement for every corrective action resulting from a violation; and (iii) to scale their work towards risk to reliability and move away from a prescriptive, mechanical approach. Soon after this retreat, as discussed in greater detail below, the Regional Entities took steps to make these priorities a reality. With NERC's participation, they engaged a third-party consulting firm to perform a review of the Regional Entities' auditing practices, to identify areas to improve consistency among the Regional Entities, and to increase the rigor in the conduct of their work. Within a relatively short time, by the end of the assessment period, NERC and the Regional Entities made substantial progress on implementing the consulting firm's major recommendations to develop a standardized audit process checklist, to publish an auditor handbook, and to create an audit training program around these tools. The Regional Entities also worked closely with NERC and the registered entities to pursue the related second and third priorities of reserving enforcement for serious matters and directing their compliance and enforcement efforts to identifying risk to the BPS. In this regard, they continued to examine ways to improve the timeliness and effectiveness of their CMEP processes, including improvements in self-reporting and enhancements to the Find, Fix, Track and Report (FFT) program, and prepared analyses and initiated pilot programs to find better ways to gauge the risk that registered entities posed to reliability, and to scale their monitoring and enforcement efforts accordingly. As a result, the Regional Entities believe that a solid foundation was laid during the assessment period to advance to the next phase of the ERO Enterprise's maturation as captured conceptually in RAI.[11]

C. Improvement Opportunities

Notwithstanding the solid foundation for the continued effective functioning of the ERO Enterprise, the Regional Entities, in tandem with NERC, are committed to exploring ways to improve their operations and their contribution to the reliability of the BPS. In this regard, they have identified certain elements essential to improved operations of the ERO Enterprise on which they plan to focus in the months ahead. Specifically, they plan to pursue: (i) clarifying and refining roles and responsibilities; (ii) coordinating strategic planning and operational decision-making; (iii) continuing to improve consistency; (iv) sharing tools and infrastructure for delegated functions; and (v) coordinating communications.

[11] Toward the end of the assessment period, the reliability community began to use the expression "ERO Enterprise" to represent the combined efforts of NERC and the Regional Entities.

The undertaking to clarify and refine roles and responsibilities is especially important to the Regional Entities as it is critical to the smooth operation of the self-regulated model. At its core, the ERO Enterprise must exercise effective and well-coordinated reliability oversight that mitigates reliability risks to the BPS. Accordingly, NERC and the Regional Entities have identified objectives on which they will concentrate to clarify and refine roles and responsibilities within the ERO Enterprise. For example, NERC will consider including in its review of Regional Entity business plans adequacy of resources and alignment of the plans for achieving delegated function objectives and outcomes described in the three-year plan. For their part, the Regional Entities will work in a coordinated fashion to support NERC in the development of comprehensive functional program designs and controls; adapt existing regional programs for delegated functions to conform to emerging program designs provided by NERC; and ensure Regional Entity staffs meet qualification and training requirements.

In addition, NERC and the Regional Entities will strive to better coordinate their strategic and business planning, e.g., by developing and maintaining a joint three-year strategic plan for the ERO Enterprise describing the goals and deliverables for statutory functions, a plan that should guide the development of each Regional Entity's annual business plans. Along the same lines, NERC and Regional Entities intend to develop and transparently report results based on a common set of performance measures focused on BPS reliability outcomes and effectiveness of the statutory programs. Furthermore, they hope to better coordinate operational decision-making within the ERO Enterprise.

Lastly, at this time, NERC and the Regional Entities plan to focus on better achieving consistency, sharing tools and infrastructure for delegated functions, and coordinating external and cross-ERO Enterprise communications. Specifically, with NERC leading, the ERO Enterprise will explore developing a core set of methods, practices, procedures, and tools to support unified implementation of the major statutory functions of NERC. The Regional Entities and NERC will also examine developing ERO Enterprise IT applications, where appropriate, to support common processes, to enhance the efficiency and effectiveness of Regional Entities' practices, to increase the consistency of the interface with registered entities, and to facilitate NERC's oversight function. Finally, all parties of the ERO Enterprise plan to continue the joint board coordination to ensure oversight and accountability of all elements of the enterprise, and to continue refining and expanding coordinated outreach to government entities in the U.S. and Canada, stakeholders, and media.

The Regional Entities believe that this coordinated effort with NERC to improve the self-regulation model will result in more clarity around the roles and responsibilities between them and among them which in turn will lead to better coordination of goals, more uniform work processes and tools, and performance measures across the enterprise, along with an understanding that all parties comprising the ERO Enterprise must be vested in each other's success. These improvements will also create higher levels of productivity, less duplication, and greater efficiency in the oversight and execution of statutory functions and mitigation of BPS reliability risks. The Regional Entities look forward to working with NERC and the stakeholders in their continual pursuit of opportunities to improve their operations that will promote the reliability of the nation's BPS.

D. Regional Reliability Standards

The 2009 JRESA provided a brief overview of the regional Reliability Standards process and scope, and reviewed what had been achieved to date.[12] The following provides an update on that overview and review and additional information on the Regional Entities' progress in developing regional Reliability Standards.

1. Regional Reliability Standards Processes

FPA §215(d), 16 U.S.C. §824o(d), requires the ERO to develop mandatory and enforceable Reliability Standards that are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by NERC, subject to Commission oversight, or by the Commission independently. A Regional Entity may also develop a Reliability Standard for Commission approval to be effective in that region only. In Order No. 672, the Commission stated that:

> As a general matter, we will accept the following two types of regional differences, provided they are otherwise just, reasonable, not unduly discriminatory or preferential and in the public interest, as required under the statute: (1) a regional difference that is more stringent than the continent-wide Reliability Standard, including a regional difference that addresses matters that the continent-wide Reliability Standard does not; and (2) a regional Reliability Standard that is necessitated by a physical difference in the Bulk-Power System.[13]

In addition, FPA §215(d)(3), 16 U.S.C. §824o(d)(3), provides that the ERO "shall rebuttably presume that a proposal from a Regional Entity organized on an interconnection-wide basis for a reliability standard or modification to a reliability standard to be applicable on an interconnection-wide basis is just, reasonable, and not unduly discriminatory or preferential, and in the public interest."[14]

In October 2010, as noted earlier, the Commission approved revised RDAs between NERC and each of the eight Regional Entities.[15] As relevant here, Exhibit C to the revised RDAs includes each Regional Entity's current RRSDP.[16] These procedures provide the process that each Regional Entity uses to develop regional Reliability Standards that are proposed to NERC for adoption, and, where applicable, regional variances if the Regional Entity is organized

---

[12] *See* 2009 JRESA, at pp. 19-20.

[13] *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, at P 291, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[14] *See also* 18 C.F.R. §39.5(b) (2013).

[15] *See North American Electric Reliability Corporation*, 133 FERC ¶ 61,061 (2010).

[16] *See* http://www.nerc.com/AboutNERC/Pages/Regional-Entity-Delegation-Agreements.aspx.

on an interconnect-wide basis. While the RRSDP's are not identical, each contains important common attributes that advance the development of regional Reliability Standards consistent with the objective of a uniform reliability program.[17] Illustratively, participation in the development of a regional Reliability Standard must be open to all organizations that are directly and materially affected by the Regional Entity's system, with no constraints based on financial capability, technical expertise or membership in the organization. The RRSDP must strive to have an appropriate balance of interests and may not be dominated by any two interest categories and no single interest category can defeat a matter. All entities with a direct and material interest in the BPS in the region may participate by expressing a position and its basis, having that position considered, and having the right to appeal. The RRSDP must also provide for reasonable notice and opportunity for public comment, and provide that all actions material to the development of any standards be transparent.[18] Under these circumstances, it can be fairly stated that during the assessment period, each of the Regional Entities fulfilled the obligation to provide an open, fair, balanced, and inclusive process for the development of regional Reliability Standards as demonstrated by the approval of those processes at the Commission, NERC, and regional levels.

NERC understandably focuses on the development of continent-wide standards as consistent with the goal of a reliable BPS, and, from the inception of the program, the Commission, NERC, and the Regional Entities anticipated that the Regional Entities would develop relatively few regional Reliability Standards to address unique situations with specific or more stringent requirements in a particular interconnection or geographic region which the continent-wide standards may not address. In fact, that has been proven to be the case. Since the Commission issued Order No. 693 in 2007, outside of WECC, the Commission has approved only seven regional Reliability Standards.[19] The regional Reliability Standards in effect as of the end of the assessment period are listed in Table 1.

[17] The Regional Entities regularly review their RRSDPs to ensure they are adequate to develop regional Reliability Standards consistent with Commission's directives and NERC's ROP *Standard Processes Manual* at Appendix 3A. *See,* e.g., *North American Electric Reliability Corporation*, Docket Nos. RR13-5-000 (June 12, 2013) (MRO), RR12-12-000 (Oct. 24, 2012) (RF), RR14-1-000 (Jan. 31, 2014) (SPP RE) , RR12-2-000 (March 1, 2012) (WECC) (unpublished delegated letter orders).

[18] In this regard, NERC maintains on its website a current overview of regional Reliability Standards under development, with detailed information on the status of the proceeding. *See* http://www.nerc.com/pa/Stand/Pages/RegionalReliabilityStandardsUnderDevelopment.aspx.

[19] WECC developed the most regional Reliability Standards because of a mandatory program it had in place prior to the approval of NERC as the ERO and the delegation to WECC. Under this program, called the Reliability Management System (RMS), WECC was required to translate existing reliability criteria into regional mandatory standards. *See,* e.g., *North American Electric Reliability Corporation*, 119 FERC ¶ 61,260 (2007) (describing the RMS and approving WECC-BAL-STD-002-0,WECC-IRO-STD-006-0, WECC-PRC-STD-001-1, WECC-PRC-STD-003-1, WECC-PRC-STD-005-1, WECC-TOP-STD-007-0,WECC-VAR-STD-002a-1,and WECC-VAR-STD-002b-1).

Regional Reliability Standards – Table 1	
Regional Entity	**Regional Reliability Standards (Description)** **FERC Docket Number, Citation**
FRCC	None
MRO	None
NPCC	**PRC-002-NPCC-01** (Disturbance Monitoring Equipment) RD11-8-000, 137 FERC ¶ 61,043 (2011). **PRC-006-NPCC-01** (Automatic Underfrequency Load Shedding) RM12-12-000, Order No. 775, 142 FERC ¶ 61,128 (2013).
RF	**BAL-502-RFC-02** (Planning Resource Adequacy Analysis, Assessment and Documentation) RM10-10-000, Order No. 747, 134 FERC ¶ 61,212 (2011).
SERC	**PRC-006-SERC-01** (Automatic Underfrequency Load Shedding Requirements) RM12-9-000, Order No. 772, 141 FERC ¶ 61,243 (2012).
SPP RE	None
TRE	**CIP-001-2a** (Regional Variance) (Cyber Security – Sabotage Reporting) RD11-6-000, Delegated Letter Order, August 2, 2011. **IRO-006-TRE-1** (Transmission Loading Relief) RD12-1-000, 139 FERC ¶ 61,169 (2012). **BAL-001-TRE-1** (Real Power Balancing Control) RD13-12-000, 146 FERC ¶ 61,025 (2014).
WECC	**FAC-501-WECC-1** (Transmission Maintenance) **VAR-002-WECC-1** (Automatic Voltage Regulators) **VAR-501-WECC-1** (Power System Stabilizer) **PRC-004-WECC-1** (Protection System and Remedial Action Scheme Misoperation) RM09-9-000, Order No. 751, 135 FERC ¶ 61,061 (2011). **IRO-006-WECC-1** (Qualified Transfer Path Unscheduled Flow Relief) RM09-19-000, Order No. 746, 134 FERC ¶ 61,199 (2011). **BAL-004-WECC-02** (Automatic Time Error Correction) (replacing BAL-004-WECC-1) RD13-11-000k, Delegated Letter Order (Oct. 16. 2013). **TOP-007-WECC-1** (System Operating Limits) RM09-14-000, Order No. 752, 135 FERC ¶ 61,062 (2011). **BAL-002-WECC-2** (Contingence Reserve) (replacing BAL-STD-002-2) RM13-13-000, Order No. 789, 145 FERC ¶ 61,141 (2013).

Indeed, while the Regional Entities believe that they should still have the authority to develop regional Reliability Standards under the conditions laid out by the Commission and

maintain their RRSDP's accordingly, with the exception of WECC, they are no longer actively engaged in developing regional standards.[20] Rather, they prefer to avoid duplicating NERC efforts, and concentrate their relevant resources on working with NERC and stakeholders to develop clear, reasonable, and technically sound continent-wide standards in a timely and efficient manner, and to ensure that regional concerns are addressed in the continent-wide standards. To this end, and as further discussed later under §D.3 below, Prioritization of Standards Work, the Regional Entities are actively encouraging awareness and participation in the NERC standards process by stakeholders in their areas, by educational outreach efforts, and through participation in the NERC Standards Committee and related subcommittees. They also have standards committees or groups that analyze the draft ERO standards to determine their quality and effectiveness, and to ensure the reliability objective is adequate and cost effective.

2. Regional Fill-in-the-Blank Standards and Regional Criteria

The 2009 JRESA agreed with stakeholders' concerns about the effect on reliability of the outstanding and incomplete "fill-in-the-blank" reliability standards projects.[21] During the assessment period, the ERO Enterprise made considerable progress to respond to the Commission's directives on those standards. This was accomplished in large part by greater collaboration and cooperation between NERC and the Regional Entities. Furthermore, the Regional Entities believe now that the appropriate resolution to the issue of fill-in-the-blank standards is the timely development of continent-wide NERC Reliability Standards.[22] Accordingly, as a general matter, the Regional Entities are no longer planning to develop Regional Reliability Standards to address the "fill-in-the blank" standards; however, they may pursue any unaddressed reliability gaps that new continent-wide standards may not cover.

---

[20] Illustratively, during the assessment period, FRCC stayed work on four regional Reliability Standards (PRC-003-FRCC-01, PRC-002-FRCC-01, PRC-006-FRCC-01, and PRC-024-FRCC-01) in large part because of related activities at the national level. MRO developed four regional Reliability Standards, but found them unnecessary before even submitting them to the board. RF worked on a number of regional Reliability Standards (e.g., MOD-024-RFC-01, MOD-025-RFC-01, EOP-007-RFC-01, and PRC-002-RFC-01) that it subsequently, using its RRSDP, converted to Regional Criteria, which are essentially RF board-approved good utility practices. In August 2012, RF also suspended work on drafting efforts for PRC-006-RFC-01 and PRC-012-RFC-01. SPP RE developed one board-approved regional Reliability Standard (PRC-006-SPP-01), but withdrew the FERC filing in August 2013, because a continent-wide standard eliminated the need for it.

In contrast, WECC maintained and continued to develop regional Reliability Standards during the assessment period for two primary reasons: (i) the Western Interconnection has some unique characteristics and concerns; and (ii) several of the current WECC regional Reliability Standards projects are required by the initial FERC orders approving the WECC regional Reliability Standards as part of the transition from the RMS program. *See supra* note 19. *See* generally http://www.wecc.biz/Standards/Development/Pages/default.aspx.

[21] As explained in the 2009 JRESA, at p. 19, when the Commission approved 83 Reliability Standards in Order No. 693, it withheld a decision on certain standards that referred to Regional requirements that were not specifically noted within the standards. These were referred to as "fill-in-the-blank," meaning the entity had to refer to a Regional document for the answer of what level of performance was required.

[22] In this regard, for example, the Commission's approval of Reliability Standard PRC-006-1 addressed an area of significant concern with respect to under-frequency load shedding. *See Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards*, Order No. 763, 139 FERC ¶ 61,098 (2012).

3. Prioritization of Standards Work

While NERC is responsible in the first instance to develop the continent-wide standards, the Regional Entities clearly have a stake in that process, because they are ultimately responsible for enforcing compliance with those standards. Accordingly, during the assessment period, the Regional Entities supported NERC in response to the Commission's concerns to increase the efficiency and effectiveness of the standards development process and to improve the quality of the resulting Reliability Standards. As now discussed, the Regional Entities are encouraged by the advances that NERC made in this regard.

First, the Regional Entities support NERC's objective to transform the current set of Reliability Standards in 2014 through 2015 to high quality, technically sound, results-based, cost-effective standards, which collectively will help ensure the reliable operation of the North American BPS. They especially appreciate NERC's piloting of the Cost Effective Analysis Process (CEAP), which is intended to evaluate the cost effectiveness of standards under development.

Second, the Regional Entities appreciate NERC's development of the *Weekly Standards Bulletin*, which helps the registered entities and other stakeholders to keep apprised of standards development. Along the same lines, the Regional Entities believe that the quarterly *Analyses of NERC Standards Process Results* were also very helpful for a better understanding of, and provides insight to, the development of continent-wide standards.[23]

Third, the Regional Entities are encouraged by the Commission's approval of revisions to the NERC *Standard Processes Manual*, ROP Appendix 3A, finding that those revisions are reasonable and allow for greater flexibility and efficiency in the process.[24] The Commission highlighted that the revisions recognize the need for highly qualified standards drafting teams that include technical writers, legal and compliance resources, and rigorous and highly trained project management.[25] The Regional Entities, which are in daily contact with the stakeholders who must deal with the intricacies of compliance with the standards, agree that well-trained personnel are needed to ensure the quality and effectiveness of the mandatory Reliability Standards, and believe that NERC has made significant strides to achieve that objective.

Fourth, the Regional Entities are encouraged by NERC's response to the Commission's March 2012 invitation to suggest retirement of requirements within standards, and the Commission's approval of NERC's proposal to withdraw 34 requirements within 19 Reliability Standards, and the additional withdrawal of 41 Commission directives that NERC develop

[23] NERC submitted these analyses pursuant to FERC directives, including the order on the three-year assessment. *See Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 (2010), at P 85.

[24] *See North American Electric Reliability Corporation*, 143 FERC ¶ 61,273 (2013), at P 18.

[25] *Id.*

modifications to Reliability Standards.[26] These actions signal a cooperative effort that will help alleviate some of the complexity and frustration that has plagued the development of standards for many years and ease compliance burdens on the registered entities. Along the same lines, the Regional Entities commend NERC's creation of the Standards Independent Experts Review project in 2012. During the assessment period, this group assessed the current non-Critical Infrastructure Protection (CIP) Reliability Standards to determine which requirements should be retired and to grade the remaining requirements for content and quality. More important, this group identified gaps where risks to reliability are not adequately addressed in the current set of standards, including outage coordination, governor frequency response, situational awareness models, and clear three-part communications.

Finally, the Regional Entities commend the NERC Board of Trustees (NERC Board) for forming the Reliability Issues Steering Committee (RISC) in August 2012. Through its efforts, RISC is helping to move the ERO Enterprise toward a more efficient standards development program and a sensible prioritization of the work to produce reasonable and effective standards and identify any emerging risks to reliability.

E. Organization Registration and Certification

The 2009 JRESA discussed the subject of compliance registry within the context of the CMEP.[27] While the topic fits there, it also lends itself to a separate discussion, as set out below.

1. Organization Registration

The Regional Entities and NERC are required to identify and register all entities that meet the criteria as laid out in the NERC ROP *Statement of Compliance Registry Criteria*, Appendix 5B.[28] The Regional Entities review and evaluate registration requests and changes and make registration recommendations to NERC when a request or change may affect the NERC Compliance Registry (NCR). NERC is responsible for registering those entities and establishing and maintaining the NCR of the BPS owners, operators, and users that are subject to approved Reliability Standards.[29]

As pointed out in the 2009 JRESA, the registration of BPS users, owners and operators has been a very successful aspect of the Regional Entities' obligation to monitor and enforce the

---

[26] *See Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, Order No. 788, 145 FERC ¶ 61,147 (2013).

[27] *See* 2009 JRESA, at pp. 21-23. The 2009 JRESA used the term "Compliance Registry" whereas this section will use the current term "Organization Registration" and also discuss Organization Certification.

[28] *See* http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_5B_RegistrationCriteria_20140701_updated_20140602.pdf. *See* generally ROP §500, http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20140701_without_Appendices.pdf.

[29] *See* http://www.nerc.com/pa/comp/Pages/Registration-and-Certification.aspx.

Reliability Standards.[30] The Regional Entities believe that continued to be the case during the assessment period, as evidenced by the acceptance by the *vast* majority of the registered entities of their inclusion in the NCR. Indeed, as of December 31, 2013, relatively few registered entities, just 47 out of over 1,850 registered entities in the U.S., appealed their registrations by the Regional Entities to the NERC Board, and only nine of those appeals were filed after January 1, 2009.[31] The NERC Board upheld the Regional Entities' decisions, except in one case, and remanded aspects of another appeal directing the Regional Entity to consider whether two entities should be jointly registered.[32] And in two instances, the NERC Board simply asked the Regional Entity to supply more information on an entity's status.[33] Most important, as of December 31, 2013, only eleven registered entities appealed the NERC Board decisions upholding the Regional Entities' registrations to the Commission.[34]

---

[30] *See* 2009 JRESA, at p. 21.

[31] The number "47" does not refer to the actual number of appeals. Twenty-two of the 47 registrants were involved in just eight appeals of FRCC registrations, five of which concerned the same types of county resource recovery facilities. (No appeal of an FRCC registration has been filed since January 1, 2009.) The other appeals to the NERC Board were filed regarding the registration decisions of MRO (1), RF (8), SERC (6), SPP RE (1), TRE (4), and WECC (5). *See* http://www.nerc.com/pa/comp/Pages/Decisions-on-Appeals.aspx.

[32] In NERC Docket RA080012, on January 16, 2013, the BOT remanded to SERC the issue of whether Louisiana Generating should be registered as a Distribution Provider. In NERC Docket RA080002, on August 19, 2008, the BOT remanded to RF an appeal of Cordova Energy Co, LLC, to consider whether Cordova and Constellation Energy Commodities Group, Inc. should be jointly registered.

[33] The NERC Board directed these requests to SERC regarding the U.S. Army Corps of Engineers-Ft. Worth District (in NERC Docket RA080011) and the North Carolina Electric Membership Corporation (in NERC Docket RA080007).

[34] The Commission denied four, granted six, and denied in part and granted in part one of those appeals.

See the following orders where the Commission denied registrants' appeals: *City of Holland, Michigan Board of Public Works*, 139 FERC ¶ 61,055 (2012), *order on reh'g*, 145 FERC ¶ 61,054 (2013 (denying appeal of RF's decision to register entity as a transmission owner and a transmission operator), *appeal pending sub. nom. City of Holland, Michigan Board of Public Works v. FERC*, No. 13-1306 (D.C. Cir. Dec. 16, 2013); *Cedar Creek Wind Energy, LLC and Milford Wind Corridor Phase I, LLC*, 135 FERC ¶ 61, 241 (2011), *order on reh'g*, 137 FERC ¶ 61,141 (2011), *order on compliance filing*, 139 FERC ¶ 61,214 (2012) (denying appeal of two entities of their registration by WECC as transmission owners and transmission operators); *Southeastern Power Administration*, 125 FERC ¶ 61,294 (2008) (affirming SERC's registration of SEPA as a transmission operator and resource planner).

See the following orders where the Commission granted registrants' appeals: *South Louisiana Electric Cooperative Association*, 144 FERC ¶ 61,050 (2013), *order on reh'g*, 145 FERC ¶ 61,232 (2013) (granting appeal of entity registered by SERC as a distribution provider and load-serving entity for lack of sufficient document); *Direct Energy Services, LLC, Sempra Energy Solutions LLC, and Strategic Energy, L.L.C*, 121 FERC ¶ 61,274 (2007), *order on compliance filing*, 123 FERC ¶ 61,016 (2008) (granting appeals of three entities which objected to their registration as load serving entities and directing NERC to submit a plan to address a possible gap in reliability because of inconsistent registration of certain types of entities); *Mosaic Fertilizer, LLC and City of Tampa, Florida*, 121 FERC ¶ 61,058 (2007) (remanding case to NERC for reconsideration of FRCC's registration or to provide further explanation for underlying decision).

See the following orders where the Commission denied in part and granted in part a registrant's appeal: *U.S. Department of Energy, Portsmouth/Paducah Project Office*, 139 FERC ¶ 61,054, *order on reh'g*, 141 FERC ¶ 61,108 (2012) (granting the appeal of DOE and finding that its Portsmouth facility should not be registered as a

While some individual registration cases were challenging, the organization registration program remained steady during the assessment period. The means by which new registered entities were discovered, for example, were similar to the original means, including self-registrations, compliance audits, public websites, independent system operator (ISO), and regional transmission organization (RTO) memberships (where relevant), information provided by other registered entities, exchange of information between Regional Entities (e.g., through the Regional Registration and Certification Functional Group), Energy Information Administration data, questionnaires, and, of course, word of mouth. The average time to process uncontested entity requests to register or de-register for a function (measured from the time the entity makes the request to the time the request is approved by NERC) likewise stayed the same, or even improved, during that period, taking as little time as three to five business days, or longer up to 90 days if complications arose, such as entity trying to change its registration during an audit. The greatest, albeit not that great, movement within the program was the changes in the number of functions (as opposed to entities) for which entities are registered, as reflected in Table 2.

Trends in the Activation and Deactivation of Functions – Table 2

Regional Entity	Registered Entities		Registered Functions		Trends in the Activation and Deactivation of Functions in the Regions during Assessment Period
	2009	2013	2009	2013	
FRCC	71	69	240	244	FRCC processed approximately 20 function activations, most of which were associated with changes to generating facility functional responsibilities such as a vendor accepting generator owner (GO) and generator operator (GOP) compliance responsibilities and new joint registration organizations (JROs); 14 function deactivations, most of which were associated with the same generation functional responsibility change and with distributor provider (DP) functional responsibilities being accepted by GO and TO; and 10 entity name changes.
MRO	118	134	435	453	MRO, which had registered 435 functions as of 1/1/09, had 453 registered functions at year-end 2013, for an increase of four percent.

load-serving entity on the basis of the evidence submitted) (Commissioner Norris dissenting); *U.S. Department of Energy, Portsmouth/Paducah Project Office*, 124 FERC ¶ 61,072 (2008) (affirming RF's registration of DOE facility as a transmission owner, transmission operator and distribution provider, but remanding to NERC the issue of whether it functions as a load-serving entity).

Trends in the Activation and Deactivation of Functions – Table 2					
Regional Entity	**Registered Entities**		**Registered Functions**		**Trends in the Activation and Deactivation of Functions in the Regions during Assessment Period**
	2009	**2013**	**2009**	**2013**	
NPCC	287	301	576	602	The number of registered entities in NPCC fluctuated slightly during the assessment period. At the end of the period, the number had risen to 301. The ultimate increase in the number of entities was due to the number of new GOs, GOPs, and purchasing-selling entities (PSEs) outpacing the delisting of GOs, GOPs, and PSEs.
RF	358	343	677	686	RF experienced very little change in the registration of new entities, and hence functions, during the assessment period. The majority of registry work involved name or ownership changes. A notable trend during the assessment period was the deactivation of GOs and GOPs that owned or operated blackstart resources. This deactivation may have occurred due to the compliance obligations and costs associated with owning and operating blackstart resources. RF is concerned by this trend, as it appears that the costs of compliance may be creating a perverse incentive for registered entities to dispose of blackstart resources, which are important to bulk electric system (BES) reliability.
SERC	227	244	643	694	SERC continued to see considerable change associated with PSE and GO/GOP functions, mostly due to changes in ownership or corporate structure. SERC also registered several new wind farms and a few new generating facilities. SERC's deactivations typically occurred when there was a change in ownership of an asset. Several BAs were deactivated in December 2013 as a result of integration into the MISO BA. Name changes occurred regularly. SERC anticipates most DPs/load serving entities (LSEs) connected via radial tie lines to request deactivation following the BES definition revisions and FERC's South Louisiana Electric Cooperative Association decision. SERC noted a particular challenge with deactivation–the inability to deactivate a registered entity that has an open enforcement action. There

Trends in the Activation and Deactivation of Functions – Table 2					
Regional Entity	**Registered Entities**		**Registered Functions**		**Trends in the Activation and Deactivation of Functions in the Regions during Assessment Period**
	2009	**2013**	**2009**	**2013**	
					appears to be no mechanism to transfer a function to an acquiring registered entity, even if the new owner has agreed to accept the compliance responsibility and mitigation of the prior issues. During the assessment period, SERC's Compliance Database Management Functional Group began seeking a solution to this limitation.
SPP RE	117	140	379	438	SPP RE registered 117 new functions and deactivated 66 functions during the assessment period. Over half of the activations were GO and GOP, due in large part (60%) to construction of new generation. A large majority of the de-activations were due to sales and mergers, which also led to some name changes.
TRE	216	224	337	440	TRE registered 37 percent of the entities in the ERCOT footprint for at least two functions. Registration deactivations occurred only for the GO, GOP, LSE, PSE, and transmission Oowner (TO) functions, the majority of which occurred during 2011 and 2012, and consisted mostly of the GO, GOP, and PSE functions.
WECC	471	474	1,258	1,250	Since January 1, 2010, WECC processed 239 registration requests, all of which were accepted and approved by NERC. WECC is forecasting that most DPs/LSEs connected via radial tie lines will request deactivation following the BES definition revisions. To help prepare for this anticipated influx, WECC introduced business process management software for the WECC Compliance Registration Process in 2013. Entities now complete a web-based registration form on the WECC.biz site that requires the entity to provide additional information and answer specific questions based on their request. The system delivers the information to a WECC engineer for review while updates are provided automatically to the applicant via template emails. Everything from the original application to the engineer's review notes and correspondence emails

Trends in the Activation and Deactivation of Functions – Table 2					
Regional Entity	**Registered Entities**		**Registered Functions**		**Trends in the Activation and Deactivation of Functions in the Regions during Assessment Period**
	2009	**2013**	**2009**	**2013**	
					are managed by the system thereby decreasing the processing time.
TOTALS	**1,865**	**1,929**	**4,545**	**4,807**	

Another important part of the Regional Entities' organization registration functions pertains to the joint registration organization (JRO) and coordinated function registration (CFR), both of which are intended to define the responsibilities and accountability among entities separately registered for the same function. Revisions to NERC ROP §507 and the addition of §508, approved by the Commission on June 10, 2010, helped to clarify the operations of both types of registrations during the assessment period.[35]

Specifically, ROP §507 allows an entity to 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. Many of the registered entities that use the §507 process are cooperatives, municipalities, and other publicly owned utilities. For example, the Illinois Municipal Electric Agency is a JRO in RF, and accordingly is registered as a DP, LSE, and TO on behalf of certain of its municipal members.[36] As of end of the assessment period, all but two (NPCC and WECC) of the Regional Entities had registered a total of 30 JROs.[37] Otherwise, after the initial implementation, the program was fairly static, with few entities registering as JROs or changing their JRO status. For example, during the assessment period, (i) FRCC processed four JRO changes; (ii) FRCC, SERC, and TRE registered a few JROs; (iii) MRO registered one new JRO; and (iv) SPP RE registered no new JROs.

NERC ROP §508 allows multiple entities to register using a CFR for one or more Reliability Standard(s) or for one or more Requirements or sub-Requirements with particular Reliability Standard(s) applicable to a specific function. The Registration of the CFR is the complete Registration for each entity, and each entity must take full compliance responsibility for those standards or requirements or sub-requirements it has registered for in the CFR. For example, in 2010, TRE registered 13 entities as TOPs through CFR agreements. Each CFR is an agreement between ERCOT ISO and one other transmission entity that allocates responsibility

[35] *See North American Electric Reliability Corporation*, Docket No. RR10-8-000 (June 10, 2010) (unpublished delegated letter order).

[36] *See* the compliance audit report at http://www.nerc.com/pa/comp/Audit%20Repots%20DL/2013_public_RFC_MRRE_IMEA.pdf.

[37] *See* the *JRO Member Listing* Excel spreadsheet at http://www.nerc.com/pa/comp/Pages/Registration-and-Certification.aspx.

for TOP requirements between ERCOT ISO and that entity. The CFRs are updated regularly to account for changes in the body of applicable NERC Reliability Standards.[38]

As of end of the assessment period, 184 registered entities took advantage of coordinating their registered functions pursuant to ROP §508.[39] This represented 44 coordination agreements in all Regional Entities but one (FRCC), some of which crossed regional lines. For example, one CFR involved 31 registered entities located in three different Regional Entities (MRO, RF, and SERC). TRE had the largest number of registered entities (73) in the CFR program with 17 CFR arrangements. As was true for the JROs, with the exception of TRE, there was little activity in the CFR program during the assessment period. For example, MRO saw only one JRO convert to a CFR; SPP RE had just one new CFR register; NPCC had two new CFRs register; RF and SERC had a few new CFRs register; and WECC had three new CFR changes. In TRE, in 2010, 60 entities were registered as LSEs in a CFR agreement, and 14 entities were certified and registered as TOPs in a CFR agreement with ERCOT ISO. Since that time, TRE accepted additional CFR registrations.

Notwithstanding the Regional Entities' overall success in registering entities to ensure sufficient coverage of the BPS, the 2009 JRESA listed five areas where improvements could be made to the process of organization registration.[40] As now discussed, in the Regional Entities' opinion, these areas were largely and appropriately resolved during the assessment period by FERC-approved changes to the NERC ROP and by other Commission actions, or were overtaken or resolved by other events or activities.

a. The Scope of the Registration Criteria

FERC-approved changes to NERC ROP Appendix 5B addressed, at least in part, the issue of whether the registration criteria appropriately capture the users, owners, and operators of the BPS to ensure reliability. The current version (effective July 1, 2014) of the *Statement of Compliance Registry Criteria* (contained in ROP Appendix 5B) reflect review by NERC and the Regional Entities, in consultation with the stakeholders. This review aimed to determine if there should be a different threshold for materiality to the reliability of the BES and to determine if the compliance resources could be better prioritized by changes to the registration criteria.[41] Along these same lines, the Regional Entities supported the efforts of the Registration and Certification Functional Group, working with the NERC Board-appointed Compliance and Certification Committee's Organization Registration and Certification Subcommittee, to develop proposed changes to the registry criteria.

---

[38] To assist in this process, each Regional Entity's website includes a link to NERC's website to access its *Requirement Applicability List for Coordinated Functional Registration*. *See* http://www.nerc.com/pa/comp/Pages/Registration-and-Certification.aspx.

[39] *See supra* note 37.

[40] *See* 2009 JRESA, at pp. 21-23.

[41] *See North American Electric Reliability Corporation*, 141 FERC ¶ 61,241 (2012) (approving revisions to NERC ROP).

Also, during the assessment period, the ERO's activities to address the scope of the registration criteria became entwined with the Order No. 773 proceeding, in which the Commission modified the BES definition to remove regional discretion, and established a bright-line threshold that includes all facilities operated at or above 100 kV.[42] Order No. 773 also approved revisions to the NERC ROP to create an exception process to add elements to, or remove elements from, the BES on a case-by-case basis, and established a process pursuant to which an entity may seek a determination by the Commission whether facilities are "used in local distribution" as set forth in the FPA. As relevant here, while recognizing that the registration criteria and the BES definition have different applications (to entities and facilities, respectively), the Regional Entities believe that Order No. 773 addresses many of the concerns that were raised in 2009. The new BES definition and exception process, for example, may resolve the issue of small entities whose facilities are not necessary for the reliable operation of the BES. Currently, the Regional Entities are working with NERC to review and offer corresponding revisions to the *Statement of Compliance Registry Criteria* in NERC ROP Appendix 5B, and develop an application and database for the BES definition exception process (BESnet) to promote efficiency and consistency in the implementation of the new definition.

b. Re-examination of Functional Model Definitions

The 2009 JRESA noted commenters' concerns about the Reliability Functional Model, namely that it is conceptual whereas registered entities have (for historical or business reasons) often aligned their operations differently.[43] To address these concerns, that self-assessment discussed increasing the granularity of registration so it would focus on the requirement level, instead of the standard level, but it also recognized that redefining the terms of various functions may be impractical as it would unlikely resolve the immense diversity of organizational structures in the industry. While NERC and the Regional Entities spent some time at first to examine these ideas, they appropriately put the exercise on hold during the assessment period in light of the significant amount of work required to create and implement the new BES definition and the exception process. Also, the Order No. 773 effort may serve the same purpose and provide an increase in granularity as contemplated by the suggestions made in 2009 to revisit the Functional Model. Finally, NERC and the Regional Entities plan to start in 2014, to review and

---

[42] *See Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236 (2012), *order on reh'g and clarification*, Order No. 773-A, 143 FERC ¶ 61,053 (2013), *order on reh'g and clarification*, 144 FERC ¶ 61,174 (2013), *appeal pending sub nom. People of the State of New York, et al. v. FERC*, No. 13-2316 (2nd Cir. filed June 12, 2013); *see also Revision to Electric Reliability Organization Definition of Bulk Electric System*, Order No. 743, 133 FERC ¶ 61,150 (2010), *order on reh'g*, Order No. 743-A, 134 FERC ¶ 61,210 (2011). On June 6, 2013, the Commission extended the effective date of the new definition, until July 1, 2014. *See Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order Granting Extension of Time, 143 FERC ¶ 61,231 (2013), *order on reh'g*, 146 FERC ¶ 61,070 (2014). On March 20, 2014, the Commission approved NERC's proposed revised definition of "bulk electric system." *See North American Electric Reliability Corporation*, Order Approving Revised Definition, 146 FERC ¶ 61,199 (2014).

[43] *See* http://www.nerc.com/pa/Stand/Functional%20Model%20Archive%201/Functional_Model_V5_Final_2009Dec1.pdf . The Reliability Functional Model is not approved by the Commission, and is not used by every Regional Entity.

clarify relationships between the functional model and the NERC ROP registration and certification directives (including Registry Criteria).

c. Oversight of Multi-Regional Entities

As pointed out in the 2009 JRESA, there are instances where an entity owns or operates BES facilities in two or more regions and thus is subject to multiple compliance programs, and there are businesses that have operations in all eight Regional Entities. To address the challenges raised by these situations, several of the Regional Entities partnered during the assessment period to coordinate more effectively their compliance and enforcement efforts with respect to multi-regional registered entities (MRREs). In particular, they developed a lead region model, in which the Regional Entities decide which one will lead the compliance and enforcement efforts for a given MRRE. For example, RF, MRO, and SERC agreed that RF would be the lead Regional Entity for Mid-continent Independent System Operator (MISO) due to the location of its headquarters and load, and the complex seams issues between the MISO and PJM Interconnection markets, while RF and MRO agreed that MRO would be the lead Regional Entity for American Transmission Company (ATC) due to the majority of ATC's transmission being located within MRO's footprint. In addition, during the assessment period, the Regional Entities worked closely with NERC to improve the coordination of compliance monitoring, mitigation, and enforcement without requiring change to the registration process. To this end, toward the end of the period, the Regional Entities developed *Recommended Guidelines for Multi-Region Entity Coordination*, which the ERO Executive Management Group approved in April 2014 for implementation across the ERO. Efforts are currently underway to develop template agreements between the affected Regional Entities and the notification to registered entities.

d. Transfer of Registered Entities between Regional Entities

Changes to NERC ROP §1208, approved by the Commission during the assessment period, on October 21, 2010, adequately addressed the issue of the appropriate conditions for the transfer of a registered entity from one Regional Entity to another.[44] In the order approving the changes, the Commission agreed with NERC that a registered entity does not have a right to choose the Regional Entity that will be its Compliance Enforcement Authority.[45] The Commission explained:

> In addition, as the Commission stated in Order No. 672, it is important that the footprint of a Regional Entity makes sense from a reliability perspective and does not overlap with another regional footprint. The Commission explained that any change in size, scope or configuration of a Regional Entity would constitute an amendment to the Delegation Agreement, and any such amendment would be

[44] *See North American Electric Reliability Corporation*, 133 FERC ¶ 61,061 (2010) (approving revised Delegation Agreements and changes to ROP, including §1208 governing Regional Entity transfer requests); *see also Nebraska Public Power District, et al*., 136 FERC ¶ 61,047, *order on reh'g*, 137 FERC ¶ 61,144 (2011) (denying NPPD's request to transfer from MRO to SPP RE).

[45] 133 FERC ¶ 61,061, at P 72.

> subject to review by the ERO and approval by the Commission. This process, under which the Commission must approve any change to the boundary of a Regional Entity to which the ERO has agreed, indicates that boundary changes should be carefully considered and should serve to improve the effectiveness or efficiency of the Regional Entities' and NERC's administration of reliability, and should not merely benefit an individual registered entity.[46]

The Regional Entities believe that ROP §1208 will assist them in maintaining a more stable structure for enforcing the reliability standards, and will therefore promote consistency of results.

e. Applicability of Reliability Standards to Federal Entities

The Commission's orders with respect to Southeastern Power Administration, the U.S. Army Corps of Engineers, and the Southwestern Power Administration generally resolved the related issues of: (i) the registration status of U.S. government agencies; (ii) compliance by those agencies with the Reliability Standards; and (iii) the application of penalties to those agencies found in violation of the Reliability Standards.[47] These decisions will greatly assist the Regional Entities in their efforts to ensure that such major users, owners and operators of the BES are held accountable for their actions regarding the reliability of that system.[48]

2. Organization Certification

Organization Certification is the process by which NERC and the Regional Entities ensure that an applicant to be a reliability coordinator (RC), balancing authority (BA), or transmission operator (TOP) has the tools, processes, training, and procedures to demonstrate its ability to meet the Requirements and sub-Requirements of all of the Reliability Standards applicable to the function(s) for which it is applying, thereby demonstrating the ability to become certified and then operational. The specific requirements for this process are found in the NERC ROP Organization Registration and Certification Programs (§500), and *Organization*

---

[46] *Id.*

[47] *See Southeastern Power Administration, 125 FERC ¶ 61,294 (2008)* (affirming SERC's registration of SEPA as a transmission operator and resource planner*); North American Electric Reliability Corporation*, 133 FERC ¶ 61,214 (2010), *order on reh'g*, 137 FERC ¶ 61,044 (2011); *North American Electric Reliability Corporation*, 129 FERC ¶ 61,033 (2009), *order dismissing reh'g*, 130 FERC ¶ 61,002 (2010) (collectively, affirming TRE's and SPP RE's decisions to register the U.S. Army Corps of Engineers and finding that any other federal entity that uses, owns or operates the BPS must comply with mandatory Reliability Standards); *North American Electric Reliability Corporation*, 140 FERC ¶ 61,048, *order on reh'g*, 141 FERC ¶ 61,242 (2012) (finding that SWPA was liable for a $19,500 penalty imposed by SPP RE for violating Reliability Standards), *appeal pending sub nom. Southwestern Power Administration, et al.* v. *FERC*, No. 13-1033 (D.C. Cir. Feb. 15, 2013).

[48] The implication of these decisions on the Regional Entities' workload is apparent from the statistics in NERC's May 8, 2013 PowerPoint presentation titled on *Key Compliance and Enforcement Metrics and Trends*. At that time, there were 419 open federal entity possible violations under review, of which 373 or 89% were "on hold" because the legal issues had not been resolved. Fortunately, the registered entities had mitigated or were in the process of mitigating 86 percent of the possible violations.

Registration and Certification Manual (Appendix 5A), and are also set out in the *ERO Certification and Review Procedure* manual (updated May 12, 2014).[49] Accordingly, the Regional Entities must organize certification teams that are subject to certain training requirements to ensure the accuracy of the certifications.[50] As is true of the registration process generally, the organization certification process ran smoothly during the assessment period. In that time, the Regional Entities certified 53 entities, conducted 68 reviews, and received only three objections to a Regional Entity's certification team's decision.[51]

F. Compliance Monitoring and Enforcement Program

The 2009 JRESA discussed the Regional Entities' implementation of the CMEP, covering ten topics: (i) compliance registry; (ii) consistency and use of discretion in application of penalties; (iii) CMEP consistency; (iv) compliance audit consistency; (v) consistency in interpretation of Reliability Standards; (vi) compliance caseload backlog; (vii) treatment of minor violations; (viii) compliance information management tools; (ix) compliance process transparency (within the ERO and the Regional Entities and between the ERO and its registrants); and (x) the hearings and appeals process.[52] The following updates that discussion, and provides additional information on the Regional Entities' progress to implement and improve the CMEP.[53]

1. Development and Status of the Compliance Monitoring and Enforcement Program

During the assessment period, the Regional Entities made significant progress and improvements in the implementation of the CMEP. This is important because the CMEP represents the Regional Entities' primary responsibility under the FPA and the Commission's regulations. FPA §215(a)(7), 16 U.S.C. §824o(a)(7), defines "regional entity" in the first instance as "an entity having enforcement authority" under the relevant statutory provisions. §39.1 of the Commission's regulations, 18 C.F.R. §39.1, repeats that definition. Accordingly, during the assessment period, the Regional Entities devoted the majority of their resources to oversee compliance with and enforcement of the mandatory Reliability Standards.

---

[49] *See* http://www.nerc.com/pa/comp/Pages/Organization-Certification.aspx.

[50] *Id.* pp. 5-6

[51] These numbers break down by Regional Entity as follows:

	FRCC	MRO	NPCC	RF	SERC	SPP RE	TRE	WECC
Number of Certifications	0	1	3	5	10	3	18	13
Number of Reviews	4	7	4	11	17	4	4	17
Number of Appeals	0	0	0	0	0	1	0	2

[52] *See* 2009 JRESA, at pp. 21-31.

[53] The update to the section on Compliance Registry, included in the CMEP discussion in the 2009 JRESA, is found in the previous section of this self-assessment.

The Commission explained NERC's and the Regional Entities' roles in regard to the CMEP in its 2007 order accepting the initial RDAs and approving the original formulation of the CMEP.[54] In brief, NERC relies on the Regional Entities to enforce the NERC Reliability Standards with BES owners, operators, and users through approved RDAs. Regional Entities are responsible for monitoring compliance of the registered entities within their regional boundaries, assuring mitigation of all violations of approved Reliability Standards, and assessing penalties and sanctions for failure to comply. For that purpose, the CMEP specifies monitoring processes, including: (i) compliance audits; (ii) self-certification; (iii) spot checking; (iv) investigations; (v) self-reporting; (vi) periodic data submittals; and (vii) complaints.[55] It also includes procedures for enforcement actions, mitigation of violations, and remedial action directives, data retention, and confidentiality matters. In addition, the CMEP obligates each Regional Entity to establish and maintain a hearing body to conduct and render hearings concerning disputes over findings of alleged violations, proposed penalties, and mitigation plans.[56]

The Regional Entities have unwaveringly taken their compliance monitoring and enforcement responsibilities very seriously. In the beginning, they especially relied on their experience in conducting audits, and worked closely with NERC and the Commission's enforcement staff to structure their enforcement activities to ensure that the registered entities complied with the reliability standards. In addition, they increased their staffs to have adequate resources. More resources were necessary in part because the Regional Entities, while recognizing that they had discretion to determine appropriate remedies, conducted their enforcement programs with the understanding that they should investigate every possible violation of a standard or one of its requirements and compile a record sufficient to support any remedy chosen for a violation.[57] This was true regardless of the severity of the violations or the risk they posed to reliability. This was true even if the violations were simply a matter of documentation deficiencies.

No one in the reliability community, including FERC and NERC staff and the personnel at the Regional Entities and the registered entities, anticipated the number of violations that the Regional Entities would ultimately discover. When the 2009 JRESA was submitted to the Commission, the Regional Entities had amassed a significant backlog of over 1,700 violations. Clearly, as NERC and the Regional Entities recognized, this was an unacceptable situation.

---

[54] *See North American Electric Reliability Corporation, et al*., Order Accepting ERO Compliance Filing, Accepting ERO/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans, 119 FERC ¶ 61,060 (2007).

[55] Early in the program, the monitoring processes also included "exception reporting," which was eliminated by a change in the NERC ROP, approved by the Commission in December 2012. *See North American Electric Reliability Corporation*, Order Conditionally Approving Revisions to North American Electric Reliability Corporation Rules of Procedure, 141 FERC ¶ 61,241 (2012).

[56] *See* 119 FERC ¶ 61,060 (2007), at P 26.

[57] *See generally Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672, 123 FERC ¶ 61,046 (2008); Guidance on Filing Reliability Notices of Penalty, 124 FERC ¶ 61,015 (2008).

Within the following year, after many discussions and meetings between and among FERC, NERC, and Regional Entity staffs, and stakeholders, NERC and the Regional Entities were on their way to figuring out how to reduce that backlog, and, more to the point, to address the overarching issue of how much discretion the Regional Entities could exercise in the implementation of the CMEP.

In Fall 2009, several months after NERC had submitted its Three-Year ERO Performance Assessment Report, the Commission took three actions that set the stage for NERC and the Regional Entities to improve their implementation of the CMEP: (i) it provided further guidance on filing proposed penalties, and stated the agency's willingness to consider an abbreviated format for submitting certain types of NOPs;[58] (ii) it issued Order No. 728, which delegated to the FERC Enforcement Director authority to allow routine NOPs to become effective and to stay the effectiveness of NOPs when it was necessary to seek further information;[59] and (iii) it issued an order allowing 564 proposed penalties (labeled the "omnibus filing") to become effective by operation of law.[60]

In 2009 through 2012, the Commission issued additional orders providing direction to the members of the reliability community on what was expected of them and what they could expect from the Commission. These orders covered a variety of issues, including the importance of a mitigation record,[61] the implications of a registered entity's repeat violations and violations by its affiliates,[62] the Regional Entities' responsibility to examine a registered entity's compliance program when determining an appropriate remedy,[63] the need for Regional Entities to consider load loss and harm to customers resulting from violations of Reliability Standards in their penalty assessments for these violations,[64] and the recovery of penalties from third-parties doing business in RTOs and ISOs.[65]

---

[58] *See* Further Guidance Order on Filing of Reliability Notices of Penalty, 129 FERC ¶ 61,069 (2009).

[59] *See* Delegations for Notices of Penalty, Order No. 728, 129 FERC ¶ 61,094 (2009). Subsequently, the Commission transferred the delegation from the Director of the Office of Enforcement to the Director of the Office of Electric Reliability. *See* Delegation of Authority Regarding Consideration of Notice of Penalty, Order No. 795, 146 FERC ¶ 61,083 (2014).

[60] *See North American Electric Reliability Corporation*, Order on Omnibus Notice of Penalty Filing, 129 FERC ¶ 61,119 (2009).

[61] *See North American Electric Reliability Corporation*, Order Accepting Notices Of Penalty, 126 FERC ¶ 61,014 (2009).

[62] *See North American Electric Reliability Corporation*, Notice of No Further Review and Guidance Order, 132 FERC ¶ 61,182 (2010).

[63] *See* Delegated Letter Order, 133 FERC ¶ 62,037 (2010). *See also North American Electric Reliability Corporation*, 134 FERC ¶ 61,146 (2011).

[64] *See Northern American Electric Reliability Corporation*, 134 FERC ¶ 61,209 (2011), *order on reh'g and clarification*, 139 FERC ¶ 61,248 (2012).

[65] *See Reliability Standard Compliance and Enforcement in Regions with Regional Transmission Organizations or Independent System Operators*, Order Providing Guidance on Recovery of Reliability Penalty Costs by Regional Transmission Organizations and Independent System Operators, 122 FERC ¶ 61,247 (2008); *see also PJM*

The omnibus filing eventually led to the Regional Entities' compiling processed violations on spreadsheets entitled Administrative Citation NOPs, an approach approved by the Commission in March 2011.[66] The Commission's statements at that time provide the status of NERC's and the Regional Entities' implementation of the CMEP:

> The Commission recognizes that NERC and the Regional Entities expend substantial efforts and resources monitoring compliance with the Reliability Standards and building adequate records to support findings of violations for Commission review. On numerous occasions, the Commission has encouraged NERC and the Regional Entities to develop flexible approaches and more streamlined processes to achieve efficiency in the enforcement process, especially with regard to more minor violations. NERC has adopted an Abbreviated Notice of Penalty format and a Deficiency Notice of Penalty format that have been successful at increasing efficiency. Based upon this filing, we believe that NERC's Administrative Citation Notice format will be a successful tool in improving efficiency of NERC's enforcement process, thereby reducing the time and resources expended by the Regional Entities, NERC, and Commission staff while still achieving transparency and consistency in penalty determinations for violations that are appropriate for this format. We also commend NERC for promptly following through with its intent to institute the Administrative Citation process.
>
> We encourage NERC's continued use of the Administrative Citation Notices of Penalty format. We also encourage, particularly in the early stages of this process, the ongoing consultation between our staff and NERC prior to filing to determine what violations are appropriate for inclusion in an Administrative Citation Notice of Penalty and the appropriate amount of detail and description necessary to ensure that the Administrative Citation process continues to be a success.[67]

Six months later, in September 2011, Administrative Citation NOPs transitioned into Spreadsheet NOPs (SNOPs). Candidates for inclusion in an SNOP are those violations that posed minimal or moderate risk to the reliability of the BPS. In all cases, the SNOP sets forth whether the violations have been mitigated, certified by the respective registered entities as mitigated, and verified by the Regional Entity as having been mitigated. During the assessment period, the Regional Entities processed and submitted through NERC 5,128 confirmed violations in NOPs to the Commission, using the Administrative Citation NOP format for 296 and the

---

Interconnection, L.L.C., Order Accepting Tariff Revisions and Requiring Compliance Filing, 124 FERC ¶ 61,260 (2008) and *Midwest Independent Transmission Operator, Inc*., Order Conditionally Accepting Proposed Tariff Revisions, 128 FERC ¶ 61,229 (2009).

[66] *See North American Electric Reliability Corporation*, Notice of No Further Review of Initial Administrative Citation Notice Of Penalty, 134 FERC ¶ 61,157 (2011).

[67] *Id.* PP 7-8 (footnotes omitted).

SNOP format for 1,428 of those violations. For the 27 months from September 30, 2011 to December 31, 2013, the use of SNOPs alone represented 58% of the total number of NOPs submitted to the Commission.[68]

The next phase in the evolution of the ERO Enterprise's implementation of the CMEP is reflected in the FFT program, which started as the centerpiece of NERC's Compliance Enforcement Initiative (CEI). Details of this program during the assessment period are found primarily in two Commission orders—one issued in March 2012 and one issued in June 2013—and the NERC filings addressed by those orders.[69] Candidates for FFT treatment are possible violations that pose minimal or moderate risk to reliability and have been fixed. A certification of completion of the mitigation activities is submitted, at least within 90 days from the date the FFT is filed or posted, by the respective registered entity for every FFT submission.[70]

Again, the Commission's statements in these FFT orders are evidence of the progress made by NERC and the Regional Entities in the implementation of the CMEP. In the March 2012 order, the Commission explained,

> While the FFT initiative represents a significant change in the paradigm for monitoring and enforcing compliance with Reliability Standards, we agree with NERC that this change is warranted at this time. After several years of experience with the current program, we agree that NERC and the Regional Entities should have the flexibility to more efficiently process and track lesser risk violations in order to focus their resources on issues that pose the greatest risk to reliability.[[71]]

In its June 2013 order, the Commission found, "[b]ased on the information provided in NERC's filing… the FFT program is improving the ability of NERC and its Regional Entities to more efficiently process lesser-risk possible violations, enabling them to reduce the backlog of pending enforcement cases and focus on issues of greater importance to bulk-power system reliability."[72] Notably, in that order, the Commission explained that its staff had reviewed a

---

[68] *See* http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

[69] *See North American Electric Reliability Corporation*, Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, 138 FERC ¶ 61,193 (2012); *North American Electric Reliability Corporation*, Order on Compliance Filing, 143 FERC ¶ 61,253 (2013).

[70] Originally, as approved by the Commission, the FFT program only pertained to possible violations with minimum risk; however, in the June 2013 order, the Commission approved NERC's proposal to expand coverage to possible violations that pose moderate risk to reliability, subject to NERC's submitting a report by June 20, 2014, justifying a continuation of the expansion of the program. The Commission likewise approved NERC's proposal to allow FFT treatment even before mitigation is completed provided it is completed within 90 days of the time when the FFT is filed or posted. *See* 143 FERC ¶ 61,253, at PP 32-34, 36-37.

[71] 138 FERC ¶ 61,193, at P 2 (footnote omitted).

[72] 143 FERC ¶ 61,253, at P 27.

sample of 100 FFT issues out of approximately 820 FFT issues filed with the Commission between September 2011 and September 2012, and determined that the Regional Entities properly treated those possible violations under the FFT program.[73]

As recognized by the Commission, the Regional Entities generally believe that the FFT program significantly improved the processing of violations of the reliability standards during the assessment period, and enabled them to focus resources and attention on more serious and complex matters.[74] During the assessment period, they processed total of 1,762 possible violations using the FFT procedures, which, in 2012 and 2013, respectively, represented 48% and 43% the total number of violations and possible violations processed by the Regional Entities. In addition, the FFT program had a positive impact on processing time, which was a major concern identified by the registered entities in 2009. In this regard, between January 1, 2012 and September 30, 2013, the average time for disposing of FFTs was 7.4 months as compared to 10.7 months for SNOPs and 13.1 months for NOPs.[75]

The Commission spoke favorably of the FFT program after its review in 2013, and encouraged NERC to continue to improve the program and report back to the Commission by June 20, 2014. Specifically, the Commission directed NERC to monitor the Regional Entities' eligibility determinations; requested more specificity regarding the FFT program's impact on BPS reliability; encouraged NERC to continue to work with the Regional Entities to improve and better coordinate their risk assessments; and stressed that NERC should continue its outreach to the Regional Entities to encourage the use of self-reports by the registered entities.[76] For their part, to a certain extent in response to the Commission's review, the Regional Entities elicited from focus groups other specific issues that they believed needed to be addressed in general or in certain Regional Entities as NERC and they continued to refine the program. These included overall processing time, the full mitigation plan requirement, insufficient information on content and process, no centralized information collection (particularly for MRREs), and inadequate communication during the process. The Regional Entities are committed to continue working closely with NERC and registered entities to address these issues and to bring about continuous improvement in the FFT program and related efforts.[77]

---

[73] *Id.* P 31. Between December 6, 2013 and December 16, 2013, in Docket No. RC11-6-000, *et al*., all eight Regional Entities responded to the Commission's annual FFT survey to collect data on the effectiveness and efficiency of the FFT program. Each response included data, correspondence, and other supporting information used by the Regional Entity staffs to evaluate and conclude that the previously submitted possible violations identified by FERC staff qualified for FFT treatment. The Commission's response to these filings was still pending at the end of the assessment period.

[74] *See* Attachment A to NERC's Report in Docket No. RC11-6-004, for information from each Regional Entity on the impact of the FFT program on its region. *See* also 143 FERC ¶ 61,253, at PP 8-9 (describing the information gleaned from Attachment A).

[75] *See* the PowerPoint presentation titled *Key Compliance and Enforcement Metrics and Trends,* Compliance Committee Meeting, November 6, 2013, at slide. 5.

[76] *See* 143 FERC ¶ 61,253, at PP 28-30.

[77] Indicative of the progress made to date is reflected in the Key Compliance Monitoring Index (KCMI) compiled by NERC, which reported that as of the end of 2012, 5,115 confirmed violations were processed for the period beginning June 18, 2007. Of these violations, 85 percent had minimal impact to reliability, 13 percent had moderate

The ERO Enterprise's next advancement in CMEP implementation is RAI. Started in late 2012, RAI is intended to transform the current compliance and enforcement program into one that is forward-looking, focuses on high reliability risk areas, simplifies compliance for registered entities, and creates alternative paths outside of enforcement to resolve minor matters. Accordingly, RAI has three main goals:

(1) Develop enforcement incentives to recognize positive behavior that contribute to higher accountability and improved performance and discourage poor performance;

(2) Design and scope compliance programs that recognize risk to reliability, including consideration of an entity's management controls and corrective action programs used to meet the reliability standards; and

(3) Reduce unnecessary compliance and enforcement activities while gaining efficiencies.

As much if not more than any CMEP project undertaken since 2007, RAI is a collaborative and coordinated effort of the ERO, the Regional Entities, and the registered entities, without regard to ownership, but rather with an objective of working on a common set of deliverables.

A statement made at the July 9, 2013 FERC Reliability Technical Conference accurately portrays the situation in which the Regional Entities find themselves daily in their efforts to enforce the reliability standards, and serves as a backdrop to RAI:

> Simply put, we know the current zero tolerance approach is not sustainable for the long term….[O]ur current processes tend to be backward-looking, and we need to move to a space where we're more forward-looking to really assess an entity's ability to stay in compliance and meet or exceed the reliability standards.[78]

As further discussed at the conference, RAI would not allow "small stuff" to be "swept under the rug." The "small stuff" matters. The expectation is that the registered entities would have management practices in place to resolve the "small stuff" before it becomes a reliability risk in the form of a material violation of a Reliability Standard. To this end, the Regional Entities would look to how well a registered entity meets the reliability objectives of the standards, and whether any identified violations rise to the level that needs enforcement. It would allow Regional Entities to, among other things, better tailor the scope of audits and other

---

impact, and 2 percent had serious impact. Furthermore, the five-year assessment of the KCMI indicated that the risk to BPS reliability based on the number of violations of NERC Reliability Standards trended lower from 2008 to 2012. *See* NERC's *State of Reliability 2013* report (May 2013), http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013_SOR_May%2015.pdf, at p. 6.

[78] Testimony of Mark Rossi, Senior Vice President and Chief Operating Officer, NERC, Transcript of Reliability Conference (July 9, 2013), Docket Nos. AD13-6-000, *et al.*, at p. 86.

compliance monitoring activities based on an entity's risk (e.g., size, complexity of operations, and effectiveness of internal controls).[79] It would also provide for the determination of the nature of enforcement actions to be based on risk and the presence of internal controls. For example, a single missing record (out of hundreds) for maintaining and testing protection systems that is proactively identified and recorded by the registered entity as part of its normal management practices might not rise to an enforcement matter. While the matter would be part of the entity's compliance record, it would likely not require an enforcement filing. Traditional methods of enforcement and application of penalties, however, would still be used in connection with matters that pose a serious or substantial risk to the BPS. For those matters, the full NOP or SNOP would remain available.[80]

Starting in March 2013, several Regional Entities and registered entities became engaged in pilot programs as the initial steps towards full RAI implementation. In this regard, the Regional Entities appreciate that the Commission has previously recognized the value of pilot projects, pointing out that "[n]o matter how good the data suggesting that a regulatory change should be made, there is no substitute for reviewing the actual results of a regulatory action."[81] With this in mind, each pilot project endeavored to further define the risk-based approach and develop effective tools, training, procedures, and policies to allow the ERO Enterprise to deploy these concepts in a consistent manner across all Regional Entities. The ERO Enterprise intends to keep the Commission apprised of the progress of the pilot projects, and will make appropriate revisions and submit any necessary filings with the Commission to establish a common framework throughout the ERO Enterprise.

In sum, in the ERO Enterprise's opinion, there are significant benefits to be gained through RAI, including better alignment to a culture of reliability. RAI would give credit to entities that demonstrate strong management practices and a culture of complying with the reliability standards. Similarly, the program would focus compliance monitoring on areas that pose the greatest risk to reliability, thereby enabling and encouraging an entity to address areas of higher risk by strengthening management practices around those risks. This in turn should result in a more effective program addressing risks to reliability consistent with internal control approaches used in other areas of the corporation.[82]

---

[79] *Id.* pp. 86-87.

[80] *See* Reliability Assurance Initiative, *White Paper [No. 5] Change State Element No. 4 - Redesign of the Enforcement Strategy* (March 13, 2013), at p. 4, located at http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

[81] Order No. 637, FERC Stats. & Regs. ¶ 31,091 (2000), at p. 31,279. The U.S. Court of Appeals for the D.C. Circuit agrees: "For at least 30 years this court has given special deference to agency development of such experiments, precisely because of the advantages of data developed in the real world." *Interstate Natural Gas Association of America v. Federal Energy Regulatory Commission*, 285 F.3d 18, 24 (D.C. Cir. 2001).

[82] *See* generally http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx. In this regard, the Regional Entities appreciate the Commission's recognition of the RAI's potential benefit. Toward the end of the assessment period, the Commission noted that "…the [RAI] process when fully developed may afford a consistent, informed approach that provides incentives for entities to develop robust internal control programs." *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), at P 73 (footnote omitted).

Along with developing the RAI toward the end of the assessment period, NERC and the Regional Entities focused on three other major areas: (i) the development of a single ERO-wide audit process checklist and associated auditor handbook to ensure the use of more consistent processes and procedures by the staff in the field; (ii) the implementation of the FFT enhancements approved by the Commission in its June 20, 2013 order in Docket No. RC11-06-004; and (iii) the improvement in the self-reporting processes, including reducing the burden and cost of self-reporting. The Regional Entities, as part of the ERO Enterprise, made the following progress in each of these areas:

a. Development of Single ERO-Wide Audit Process Checklist and Associated Auditor Handbook

As the Regional Entities recognized in 2009, work was needed to ensure the consistency of compliance audits.[83] Accordingly, as discussed below, they worked on numerous projects within their own regions and across regions to improve their major tool to ensure compliance with the mandatory Reliability Standards. As relevant here, in September 2012, the Regional Entities engaged an outside firm to assess the current state of regional compliance audit procedures and underlying processes, and make recommendations that could lead to more consistent audit practices across the Regional Entities and better position them to adapt to future regulatory changes and demands. This engagement dovetailed with the development of the white papers and other conceptual documents underlying RAI, and naturally became part of the larger effort to revisit the CMEP paradigm. The outside firm produced its assessment (referred to as the Third-Party Assessment) in February 2013, and recommended that the Regional Entities:

(1) Develop a single set of standardized audit methodology documents to be used across the ERO, after aligning their existing audit methodologies;

(2) Deploy a pilot program to assess and implement the standardized audit checklist; and

(3) Roll out a robust training program to provide the audit community with sufficient growth opportunities and ultimately guide auditors in the interpretation and optimal application of the audit guidance and checklist.

Subsequently, with NERC's support and cooperation, during the assessment period, the Regional Entities produced a standard *Compliance Auditor Checklist* and completed the first version of a common *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*.[84] Also, certain Regional Entity staffs participated in pilot or

---

[83] *See* 2009 JRESA, at p. 25.

[84] *See* http://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/ERO_Enterprise_Compliance_Auditor_Manual_version_1.pdf.

comparable programs to see how the audit process checklist worked in the field, and collaborated with their colleagues in other Regional Entities to fashion appropriate training materials. The Regional Entities firmly believe that the use of the audit process checklist and handbook will create a standardized process that will improve efficiencies and drive consistency while ensuring that audits conform to professional auditing standards, particularly the Generally Accepted Government Accounting Standards (GAGAS).

b. Implementation of FFT Enhancements

As noted earlier, in the June 2013 FFT order, the Commission approved, with conditions, four enhancements to the FFT program.[85] The Commission permitted an expansion of the program by allowing FFT treatment for a "limited pool" of possible violations involving moderate (in addition to minimal) risk, subject to NERC's filing a report by June 20, 2014, justifying the continuation of the expanded FFT program; allowed the inclusion of possible violations as FFTs even if the mitigation was not yet completed, provided the mitigation was completed within 90 days from the date the FFT is filed or posted; permitted the Regional Entities to publicly post FFTs on a common website on the last business day of each month instead of NERC submitting a monthly informational filing to the Commission; and agreed with NERC's proposal to review a representative sample of FFTs during the 60-day window following the Regional Entities' monthly posting of FFTs on NERC's website instead of reviewing each FFT before public posting. In July 2013, immediately after the issuance of the June 2013 order, the Regional Entities began implementing the approved FFT enhancement applicable to them. Specifically, they included FFTs where mitigating activities had not yet been completed, submitted monthly FFT compilations to NERC for posting on its website, and evaluated possible violations involving moderate risk for processing as FFTs.[86]

c. Improvement in the Self-Reporting Process

As NERC President and CEO Gerry Cauley pointed out at the July 9, 2013 FERC Technical Conference, two-thirds of all violations at that time were self-reported.[87] Nevertheless, at that conference and in other forums such as the FERC FFT proceedings and NERC and regional meetings with the registered entities, the need to improve the self-report process was often stressed. Accordingly, the Regional Entities took steps to meet that need. To start with, as mentioned earlier, they identified areas for potential improvements. These included a lack of sufficient information on content in self-reports both in the details of the violation and the risk assessment information. In addition, there was a perception in certain cases of a lack of centralized information collection (particularly for MRREs), and the registered entity complaints on the combination of long overall processing time and a lack of communication throughout the process.

---

[85] *See* 143 FERC ¶ 61,253 (2013). The Commission rejected one of NERC's proposals, to eliminate senior officer certification. *Id*. P 17.

[86] *See* http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx for the FFT postings.

[87] *See* Transcript of Reliability Conference (July 9, 2013), Docket Nos. AD13-6-000, *et al*., at p. 135. Self-reports in this context also includes self-certifications.

Next, the Regional Entities worked together, with NERC, and with a focus group of registered entities to start putting in place enhancements to the self-report process. These included:

(1) Additional guidance on processing and the content of self-reports;

(2) Points of contact at the Regional Entity for additional guidance;

(3) An improved intake form that has the capability of augmenting information and cross-referencing information already provided, and a centralized process for MRREs; and

(4) Aggregation of minimal risk issues by selected registered entities in selected Regional Entities to allow training on risk assessment and mitigation development.

Significantly, by the end of the self-assessment period, with input from the industry focus group, NERC and the Regional Entities completed a draft of the *ERO Self-Report User Guide*, which was posted for broader stakeholder comment in January 2014. As explained in the posting, this user guide should provide registered entities with valuable information and insight on what to do to facilitate disposition of possible noncompliance by the ERO Enterprise.[88] Subsequently, in April 2014, NERC posted a revised *ERO Self-Report User Guide* with the express purpose of enhancing the Registered Entities' understanding of the information necessary for NERC and the Regional Entities to provide efficient and timely resolution of instances of potential noncompliance.[89]

2. Updates to the 2009 Joint Regional Entity Self-Assessment

As described above, the 2009 JRESA addressed nine separate CMEP topics, in addition to the compliance registry. Four involved achieving consistency within the program (consistency and use of discretion in application of penalties, CMEP consistency, consistency in interpretation of reliability standards, and compliance audit consistency), four dealt with enforcement issues (caseload backlog, treatment of minor violations, information management tools, and process transparency), and one reviewed the hearing and appeals process. Because the previous discussion on the progress made by NERC and the Regional Entities on streamlining and improving the CMEP addresses or otherwise touches on most of these topics, the following will not repeat relevant parts of that discussion here. Rather, it will provide updates to specific topics and issues that were raised by the Commission, NERC, the Regional Entities themselves, or stakeholders, in 2009. The discussion is organized under the topics of: (i) Consistency; (ii) Compliance Monitoring; (iii) Enforcement; and (iv) Hearings and Appeals.

[88] *See* http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

[89] *See* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf.

a. Consistency

In the 2009 JRESA, the Regional Entities identified consistency as an overarching issue in their discussion of the CMEP. That discussion, of course, reflects their recognition that the Commission has repeatedly tasked NERC to ensure consistency of compliance across the Regional Entities, and the NERC ROP explicitly provide that NERC must have a program to monitor the compliance enforcement efforts of each Regional Entity to achieve that objective. Accordingly, in 2009, the Regional Entities examined the issue from several different perspectives. Taken as a whole, these examinations break down into an understanding of the concept of consistency as a general matter and the efforts of the Regional Entities to achieve consistency within their own regions and across regions. To reiterate, what is now described is in addition or complementary to the ERO Enterprise's efforts to develop the RAI.

Consistency as a General Matter

The Regional Entities are committed to working within their own areas, across regions, and with NERC to meet the Commission's expectation that their compliance monitoring and enforcement endeavors adhere to the same principles, course, and form. That said, they also are aware, and urge the Commission and NERC to recognize, that consistency does not necessarily mean exactness in results. Indeed, the adoption of a risk-based approach to the CMEP, as introduced in NERC's 2011 through 2013 annual CMEP Implementation Plan,[90] will naturally result in different treatment of different entities and different outcomes of compliance and enforcement activities. Specifically, for example, penalty consistency does not mean the same penalty for specific alleged violations across all Regional Entities, because the risk posed by a specific alleged violation varies depending on the characteristics of the Regional Entity's footprint, the registered entity and its geographical location and interconnection, as well as other pertinent facts and circumstances. Instead, in the Regional Entities' opinion, penalty consistency must focus on the need for a uniform methodology to ensure that the penalty for each violation (i) is consistent with the risk posed by that violation, and (ii) encourages the appropriate behavior to improve the reliability of the BES.

Consistency of Remedies <u>Within</u> the Regions

While sensitive to consistency in their work generally, the Regional Entities expended considerable resources and paid special attention during the assessment period to ensure that their determinations on appropriate remedies for violations of the mandatory reliability standards were consistent within their own regions. For that purpose, they all used internal case management systems, which were similar in that they involved methodical comparisons of the violations to actual penalties assessed for violations of the same or similar standards or requirements within the Regional Entity; directed their staffs to coordinate and otherwise participate in regular meetings of the regional stakeholder compliance committees; required review or "sign off" by senior regional managers; and stressed internal training and regular

[90] *See*, e.g., *ERO Compliance Monitoring and Enforcement Program 2013 Implementation Plan* (revised December 27, 2012) at http://www.nerc.com/pa/comp/Resources/Pages/default.aspx?View={cb5b1d3f-f5b7-421d-8266-0bcf6a06fc08}&SortField=Date&SortDir=A.

communications with and outreach to their registered entities. They also developed other specific means for achieving the objective of consistent remedial determinations, such as compiling and posting frequently asked questions (FAQs), using surveys, involving technical experts to address risk and harm, assigning a single point of contact for each registered entity, and separating their compliance and enforcement staffs.

Consistency of Remedies and Other Matters Across the Regions

The Regional Entities made substantial progress during the assessment period to improve CMEP consistency by increasing their interaction with each other. Notable accomplishments in this regard were made by the REMG, which proactively and persistently stressed the importance of information sharing, transparency, and consistency within and among Regional Entities, and working collaboratively with NERC. In addition, as mentioned earlier, several of the Regional Entities partnered to coordinate more effectively their compliance and enforcement efforts with respect to MRRE. In this regard, they developed a lead region model, in which the Regional Entities decide which one will lead the compliance and enforcement efforts for a given MRRE.[91] Further, the Regional Entity staffs regularly met with each other to promote consistency with CMEP processes and provide subject matter experts, as needed, to the same end, and conducted compliance workshops to which the registered entities from other regions were welcomed. They also collaborated on improving data management tools and the various forms used by the Regional Entities and the registered entities, including the self-report and the self-certification forms and, as discussed in greater detail below, the reliability standards audit worksheets (RSAWs).

Finally, and as apparent from the previous discussion of the developments in the CMEP during the assessment period, the Regional Entity staffs actively participated in NERC-led committees, task forces, and working groups. For example, the Regional Entities actively participated during the assessment period is the Enforcement Sanctions and Mitigation Working Group (ESMWG). This group reviews one or two Regional Entity enforcement processes during an in-person meeting, and then shares its review to help identify best practices and highlight areas where consistency could be improved. NERC Enforcement staff also participates in these meetings and is present for discussions regarding variations in approach to enforcement and mitigation responsibilities. Additionally, the ESMWG conducts periodic "risk assessment" exercises whereby each Regional Entity is asked to review particular fact patterns and descriptions of mitigating activities and assign the appropriate level of risk. Regional Entities are further asked to highlight any assumptions that are made or to identify additional information that would assist in the assignment of the risk posed by the particular facts and circumstances. Not only do these exercises provide value in driving consistency in assessment of risk, they highlight areas of improvement in the drafting of descriptions of violations, mitigating activities, and risk assessments. By becoming involved in in-depth analyses and discussions of potential and actual risk, the Regional Entities aim to continuously improve the final enforcement product.

[91] For example, RF, MRO, and SERC agreed that RF would be the lead Regional Entity for MISO", while RF and MRO agreed that MRO would be the lead Regional Entity for ATC".

b. Compliance Monitoring

During the assessment period, the Regional Entities steadfastly used their major tool to monitor compliance with the mandatory Reliability Standards—compliance audits of the registered entities. They also used other compliance monitoring tools, including: (i) spot checks; (ii) self-reports; (iii) self-certifications; and (v) periodic data submittals. The Regional Entities' extensive compliance monitoring efforts, specifically with respect to compliance audits, spot checks, and self-reports, can be seen in Table 3.[92]

Compliance Monitoring Activities – Table 3									
		FRCC	**MRO**	**NPCC**	**RF**	**SERC**	**SPP RE**	**TRE**	**WECC**
Compliance Audits	2009	22	25	66	49	55	46	24	90
	2010	19	20	56	52	49	47	50	92
	2011	20	18	68	84	79	92	53	101
	2012	34	18	56	99	73	72	74	150
	2013	22	21	78	90	55	42	64	165
Total		**117**	**102**	**324**	**374**	**279**	**299**	**265**	**598**
Spot Checks	2009	40	64	40	147	45	90	1	8
	2010	12	27	51	57	24	14	53	32
	2011	61	8	30	30	11	17	45	16
	2012	5	1	120	3	0	6	43	0
	2013	5	0	483	2	0	3	12	6
Total		**123**	**100**	**724**	**239**	**80**	**130**	**154**	**62**
Self-Reports	2009	73	12	31	56	92	54	8	313
	2010	63	44	75	264	194	106	88	140
	2011	80	90	120	262	208	154	105	220
	2012	30	50	90	325	211	83	76	184
	2013	21	60	78	240	216	109	73	162
Total		**267**	**256**	**344**	**1,147**	**852**	**505**	**350**	**1,019**

The 2009 JRESA primarily focused on compliance audits, and the following discussion will be tailored accordingly. Importantly, during the assessment period, the Regional Entities completed the first three-year cycle of such audits for registered entities (registered in 2007 or 2008) performing the RC, BA, and TOP functions on schedule in 2010, and the six-year cycle for those registered entities not performing one of the three certified functions on schedule in 2013. Some Regional Entities also completed a portion of the second 3-year audits during the assessment period.

[92] The CMEP also once included Exception Reporting, which was removed by the revisions to the NERC ROP, approved by the Commission on December 20, 2012. *See* 141 FERC ¶ 61,241 (2102). The Regional Entities review self-certifications for all registered entities at least once annually. Some Regional Entities also require monthly self-certifications for certain Reliability Standards and Requirements. Periodic data submittals happen continuously, with certain information due to the Regional Entities on a monthly basis, other data on a quarterly basis.

The 2009 JRESA touched mainly on three topics related to Compliance Audits—the effectiveness of the RSAWs, the adequacy of audit training, and the status of NERC and FERC observers in regional audits. These will be taken up in turn.

Reliability Standards Audit Worksheets

As a general matter, the Regional Entities believe that RSAWs are helpful in their conduct of compliance audits. For example, they provide a means for recording the conduct of the audit, including detailed auditor notes and findings, and can be linked to the registered entity's evidence that can then be more easily reviewed. Registered entities appear to appreciate them, and use them extensively to prepare for an audit. Nevertheless, all of the Regional Entities believe that the RSAWs could be improved, and are pleased that their staffs are involved in the task force for that purpose. They are concerned, among other things, that the RSAWs attempt to meet multiple diverse needs, with the result being that no need is met fully or effectively; lack sufficient detail or granularity to be effective in guiding the conduct of the audit; constitute nothing more at times than a restatement of the requirement and provide little meaningful guidance to the auditor or the audited entity; and are generally cumbersome to use. As a consequence, some of the Regional Entities have developed alternate or supplemental tools to augment the RSAWs, e.g., with detailed data requests and inventory workbooks. Of course, in the Regional Entities' opinion, the audit process checklist and auditor handbook, described earlier, will help alleviate many of the Regional Entities' current concerns.

Adequacy of Audit Training

Without question, the Regional Entities are mindful of the importance of adequate audit training, both of their own staffs and for their registered entities. Accordingly, during the assessment period, they routinely encouraged, if not required, their staffs to attend or otherwise participate in relevant training sponsored by NERC (e.g., semi-annual ERO auditor workshops, GAGAS performance audit training, fundamentals of audits training, audit team leader training, compliance investigations training, *Crucial Conversations* training, and gathering quality evidence online training) or provided by third-party vendors; conducted their own in-house training; and regularly held compliance workshops for their registered entities.[93] In addition, they stressed the importance of their staffs continuing their education in specialized areas, such as cybersecurity, and maintaining or adding to their professional accreditations. As a result, the Regional Entities are confident that during the assessment period they assembled highly trained and professional audit staffs, which some of them supplemented with outside consultants with corresponding qualifications and credentials and with industry subject matter experts, to carry out their compliance monitoring obligations.[94]

[93] A good overview of NERC's training can be found in its filing submitted in compliance with the Commission's initial order on the FFT program in Docket No. RC11-6-003, on October 12, 2012, and accepted by Delegated Letter Order, on February 25, 2013.

[94] The Regional Entities' Cyber Infrastructure Protection auditor qualifications are discussed in greater detail below under §F.3, Additional Statutory Functions.

The Regional Entities will steadfastly continue these efforts, which complement and otherwise support the development of RAI. In this regard, the Third-Party Assessment suggested ways for improving auditor training, which are currently under active consideration by the ERO Enterprise. These suggestions include:

(1) Understanding and inventorying audit training over the past 2 to 3 years;

(2) Identifying initial pockets of excellence that could be leveraged;

(3) Preparing an initial listing and profile of known trainings and certifications that should be embedded within an on-going training program;

(4) Reconfirming and defining key trainings that include content related to auditing and understanding the technical aspects of the NERC requirements;

(5) Determining which professional certifications are best suited for audit professionals;

(6) Developing a program that includes all desired training and certifications;

(7) Assigning a target audience, delivery method, importance, approximate course length and frequency for each item in the training program;

(8) Establishing a method to track employee completion which will report data on progress per employee, office and region;

(9) Developing a process for proactive monitoring and continued improvements in the current training program;

(10) Creating individual annual training requirements for each employee based on gaps in their current skill sets and their expressed interests; and

(11) Tracking training and certification completion status and periodically reporting progress.

Status of NERC and FERC Observers in Regional Audits

The final compliance audit topic addressed in the 2009 JRESA concerned the uncertainty of the scope of participation by NERC and FERC observers in regional audits, even though as a general matter the Regional Entities found benefit in the observers' feedback. The Regional Entities believe that this uncertainty was largely resolved during the assessment period by Commission-approved changes to the NERC ROP Appendix 4C, §3.1.5.3, which clearly sets forth the role of audit observers, stating that "[c]ompliance Audit observers and attendees are not

Compliance Audit team members and do not participate in conducting the Compliance Audit or in making Compliance Audit findings and determinations."[95]

c. Enforcement

The 2009 JRESA touched on four specific enforcement-related topics in addition to issues of consistency—caseload backlog, treatment of minor violations, process transparency, and information management tools. As these topics overlap with each other and previously discussed topics, the following will combine the updates. As an initial matter, the Regional Entities want to stress that they continue to view communication and transparency in the enforcement process to be imperative to ensure a fair and effective implementation of the CMEP. They also believe that RAI is a positive step in that direction, and are committed to working with NERC and other members of the reliability community to make RAI a reality to advance BES reliability. In particular, RAI will support the goal of approaching the enforcement of the reliability standards on the basis of risk, as the initiative calls for evaluating registered entities' internal controls and processes, an evaluation that will enable the Regional Entities to create risk profiles. Once known, those risk profiles will assist the Regional Entities in both their compliance monitoring and enforcement activities, and eventually help reduce the time to final resolution of compliance issues.

The Regional Entities experienced a significant increase in the number of new violations discovered during the assessment period, in large part because of the introduction of the CIP mandatory Reliability Standards in 2010. Indeed, with the exception of the last year, NERC reported that the number of violations consistently trended upward during the assessment period, generally for all Regional Entities. This trend can be seen by Regional Entity on Table 4. NERC also reported that the CIP Reliability Standards were consistently the most frequently violated since 2010.[96]

New Violations during Assessment Period – Table 4						
	2009	**2010**	**2011**	**2012**	**2013**	**Total**
FRCC[97]	184	103	135	68	61	**551**
MRO	60	103	196	166	139	**664**
NPCC	43	99	130	213	66	**551**
RF	123	469	565	505	240	**1,902**
SERC	187	312	309	300	285	**1,393**
SPP RE	132	254	291	173	191	**1,041**
TRE	14	51	430	197	169	**861**

[95] *See* 141 FERC ¶ 61,241 (2012).

[96] *See* the PowerPoint presentation titled *Key Compliance and Enforcement Metrics and Trends* (February 2014), http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Presentations%20--%20February%205,%202014.pdf, at slide 15.

[97] There is a slight difference between the FRCC number of violations in Table 4 and those found in NERC's assessment of the Regional Entities. FRCC's numbers here reflect the year in which the violations were discovered whereas the other numbers reflect the year the violations were reported to NERC.

New Violations during Assessment Period – Table 4						
	2009	**2010**	**2011**	**2012**	**2013**	**Total**
WECC	571	550	807	818	437	**3,183**
TOTALS	**1,314**	**1,941**	**2,863**	**2,440**	**1,588**	**10,146**

Notwithstanding the generally steady increase in new violations during the assessment period, the Regional Entities were able to meet their objectives, stated in the 2009 JRESA, to clear out what was described there as a backlog of violations, improve the time of processing violations (especially minor violations), and, generally speaking, establish stable workloads of enforcement cases. In particular, the Regional Entities' significant reduction in their pre-2012 caseload by the end of the assessment period can be seen on Table 5.[98]

[98] As NERC reported in its 2014 business plan and budget proposal:

> As of June 30, 2013, approximately 85% of the active non-CIP violations and 72% of the active CIP violations were discovered since January 1, 2012 (i.e., were discovered in the preceding 18 months). At June 30, 2013, there were no active non-CIP violations that were discovered prior to January 1, 2010 and only 12 active non-CIP violations that were discovered in 2010. There were only 16 active violations that were discovered in 2009 and 91 active CIP violations that were discovered in 2010. Further, for the 12 months ended June 30, 2013, the number of violations dismissed or filed with the Commission exceeded the number of new violations opened by 680 violations.

Request for Acceptance of 2013 Business Plans and Budgets of NERC and Regional Entities and for Approval of Proposed Assessments to Fund Budgets, Docket No. RR13-9-000 (submitted on August 23, 2013), at p. 104.

Reduction in Pre-2012 Violations Caseload – Table 5			
	Total violations open at the end of 2011	**Total violations open at the end of 2011 still open at end of 2013**	**Percentage of Reduction**
FRCC	95	0	100%
MRO	151	14	93%
NPCC	221	0	100%
RF	429	21[99]	95%
SERC	575	25	96%
SPP RE	233	6	97.4%
TRE	283	0[100]	100%
WECC	65	0	100%

The Regional Entities accomplished these objectives in the first instance by gaining more experience, expanding their enforcement staffs, increasing their outreach to registered entities, and focusing on improved efficiency. They also accomplished this by working with Commission staff, NERC, and the stakeholders in the development of the CEI, in particular the Administrative Citation NOPs, the SNOPs, and the FFTs.[101] As mentioned above, in 2012 and 2013, respectively, the use of SNOPs represented 48% and 43% of the total number of violations and possible violations submitted to the Commission. For the same years, the use of FFTs represented 38% and 43% of the total number of violations and possible violations processed by the Regional Entities.[102] Moreover, for violations and possible violations discovered after January 1, 2012 and filed by September 30, 2013, the average processing time for SNOPs and FFTs was 10.7 months and 7.4 months, respectively.[103] As the Commission can appreciate from the management of its own enforcement cases, as reported in its Enforcement staffs' annual reports, this represents a very respectable and acceptable time to process violations of the law.

[99] This number excludes Federal entity violations which are on hold due to legal issues.

[100] This number excludes one case involving two violations that is on appeal.

[101] The Regional Entities also credit the registered entities in the improvement in the processing of violations, namely that as they also gained experience through compliance and enforcement activities, they obtained a better understanding of how to comply with the standards and thereby were able to facilitate both activities.

[102] *See* the PowerPoint presentation titled *Key Compliance and Enforcement Metrics and Trends* (February 2014), http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Presentations%20--%20February%205,%202014.pdf, at slide 10. For the period July 1, 2012 to June 28, 2013, this breaks down by region as follows:

	WECC	TRE	SPP RE	SERC	RF	NPCC	MRO	FRCC
FFT	25%	54%	44%	43%	41%	60%	57%	45%
SNOP	37%	23%	28%	38%	28%	39%	39%	40%
NOP	38%	23%	28%	19%	32%	1%	4%	15%

[103] *See* the PowerPoint presentation titled *Key Compliance and Enforcement Metrics and Trends* (November 2013), http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/CC_Presentations_Nov_2013_Complete.pdf, at slide 5.

At the same time as they were working to reduce their pre-2012 caseload and otherwise improve their processing of violations of the mandatory Reliability Standards, the Regional Entities endeavored to strictly oversee the completion of plans to mitigate those violations, because, axiomatically, timely mitigation is imperative for BPS reliability. Toward the end of the assessment period, they were able to improve the average times of two major milestones to less than a year, or significantly less than a year—the time from discovery of the violation to the registered entity's submittal of mitigation activities and the time from the discovery of a violation to the registered entity's completion of mitigation activities. This can be seen by Regional Entity for September 2012 through September 2013 in Table 6.

Average Times for Submittal and Completion of Mitigation Plans – Table 6		
	Average time from discovery of a violation to the registered entity's submittal of mitigating activities	**Average time from discovery of a violation to the registered entity's completion of mitigating activities**
FRCC	5.6 months	10.2 months
MRO	5 months	9 months
NPCC	3 months	3.4 months
RF	5.6 months	6.4 months
SERC	11 months	9 months
SPP RE	6.4 months	10.2 months
TRE	8 months	6 months
WECC	4.6 months	5.6 months

The Regional Entities achieved another 2009 enforcement goal during the assessment period by compiling and sharing with each other and the reliability community "lessons learned" from their enforcement proceedings. Accordingly, they were able to improve their own operations and help the registered entities to understand better how to comply with the mandatory Reliability Standards. They did this by: (i) creating webpages;[104] (ii) producing training videos; (iii) issuing newsletters with information on frequently violated standards and violation processing metrics;[105] (iv) publishing cases and dismissal notes;[106] (v) developing and sharing compliance guidance statements;[107] (vi) compiling other relevant written materials such as FAQs;[108] (vii) holding frequent compliance calls with registered entities; (viii) conducting

[104] *See*, e.g., http://www.texasre.org/StakeholderOutreach/LessonsLearned/Pages/Default.aspx; and http://www.serc1.org/Documents/Compliance/Statistics%20and%20Lessons%20Learned/2012/SERC%20Lessons%20Learned%20July%202012.pdf.

[105] *See*, e.g., https://rfirst.org/Pages/Newsletter.aspx.

[106] *See*, e.g., http://www.midwestreliability.org/02_compliance/Enforcement%20Case%20Notes/2013%20Case%20Notes/MRO%20Case%20Notes%202nd%20Quarter%202013.pdf.

[107] *See*, e.g., https://www.npcc.org/Compliance/Compliance%20Guidance%20Statements/Forms/Public%20List.aspx.

[108] *See*, e.g., https://www.frcc.com/FAQ/default.aspx.

numerous workshops, seminars, conferences, webinars, and open forums;[109] (ix) including detailed discussions in their compliance committee meetings; and (x) participating in trade and other industry conferences and conventions. Indeed, in the last three years of the assessment period (2011 through 2013), the Regional Entities' workshops and equivalent training programs attracted more than 30,000 attendees.[110]

Critical in the Regional Entities' enforcement activities is their use of information management tools. During the assessment period, they all changed or significantly improved or enhanced those tools. They did not, however, use the same tools (and there was no single, integrated compliance information system approach in place for them and NERC). Rather, they used one of two different integrated systems to manage compliance information received from registered entities. Five of the Regional Entities (RF, MRO, SPP RE, TRE, and WECC) used the web-based Compliance Data Management System (webCDMS), and three of the Regional Entities (SERC, NPCC, and FRCC) used the Compliance Issue Tracking System (CITS).[111] NERC used the Compliance Reporting and Tracking System (CRATS) to aggregate regional compliance data from webCDMS and CITS. While each system has its advantages, NERC and the Regional Entities plan to look to the feasibility of a common platform in the near future.

d. Hearings and Appeals

From the inception of the CMEP, the Regional Entities recognized the importance of providing sufficient process to registered entities which allegedly violated the mandatory Reliability Standards. Indeed, the Commission stressed more than once that the Regional Entities must have procedures in place to enable a registered entity to be heard in a trial-type hearing, and that NERC must have procedures in place to allow a registered entity to appeal a regional decision to the NERC Board and ultimately to the Commission.[112] Accordingly, the ERO Enterprise spent considerable time during the assessment period in developing and refining the *Hearing Procedures* laid out in Attachment 2 to NERC ROP Appendix 4C, and each Regional Entity issued its own CMEP hearing procedures, either incorporating or adopting by reference the procedures in Attachment 2. Many of the Regional Entities also provided training on the hearing procedures, including conducting a mock hearing, for their staffs, hearing bodies, or stakeholders.

---

[109] *See*, e.g., http://www.wecc.biz/Training/Pages/default.aspx.

[110] This broke down by Regional Entity as follows: FRCC (2,176), MRO (1,219), NPCC (1,650), RF (1,260), SERC (4,019), SPP RE (2,451), TRE (2,924), and WECC (14,658). WECC had almost half of the attendees because it held routine open WebEx calls with pre-set agendas with the time dedicated for questions and answers.

[111] The Regional Entities also used a variety of other programs, such as SharePoint document management system and MK Insight materials repository system.

[112] *See*, e.g., *North American Electric Reliability Corporation, et al*., Order Accepting ERO Compliance Filing, Accepting ERO/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans, 119 FERC ¶ 61,060 (2007), at PP 134-165*; North American Electric Reliability Corporation, et al.*, Order Addressing Revised Delegation Agreements, 122 FERC ¶ 61,245, at PP 74-138, *order on compliance filing*, 125 FERC ¶ 61,330 (2008), at PP 58-60.

Toward the end of the assessment period, with active participation by the Regional Entities, NERC proposed changes to *Hearing Procedures*, which the Commission approved on December 20, 2012.[113] Among other things, the Commission agreed with NERC's proposal to allow third-party interventions under a strict standard, namely that the intervener must have a direct and substantial interest in the outcome of the alleged violation, proposed penalty or sanction, mitigation plan, or remedial action directive.[114] The Regional Entities agree that the codification of this standard will facilitate the resolution of enforcement proceedings, especially in those regions with RTOs or ISOs, where a third-party may be allocated all or a portion of a penalty and where the Commission's objective of getting to the "root cause" of the violation is critical to such allocation.[115]

Even though all of the Regional Entities established hearing procedures and organized their resources to accommodate hearings, just three of them conducted a total of only five hearings during the assessment period.[116] RF conducted one regular hearing and one fast-tracked hearing, both of which were ultimately resolved by settlement. SPP RE conducted two regular hearings, one of which is pending resolution in the U.S. Court of Appeals for the D.C. Circuit,[117] and one for which a settlement was pending before the NERC Board of Trustees Compliance Committee as of December 31, 2013. TRE conducted one hearing, at the end of which its board of directors issued a confidential decision, in January 2013, and submitted the matter to the NERC Board where it was pending as of December 31, 2013. At this time, in light of the relatively little activity under the current ROP, the Regional Entities believe that they should

[113] *See North American Electric Reliability Corporation*, Order Conditionally Approving Revisions to North American Electric Reliability Corporation Rules of Procedure, 141 FERC ¶ 61,241 (2012), at PP 108-110.

[114] *Id*. P 110. *See also Monongahela Power Co., et al*., 135 FERC ¶ 61,226 (2011) (authorizing FirstEnergy to intervene in an RF hearing).

[115] *See generally Reliability Standard Compliance and Enforcement in Regions with Regional Transmission Organizations or Independent System Operators,* Order Providing Guidance on Recovery of Reliability Penalty Costs by Regional Transmission Organizations and Independent System Operators, 122 FERC ¶ 61,247 (2008); *see also PJM Interconnection, L.L.C.,* Order Accepting Tariff Revisions and Requiring Compliance Filing, 124 FERC ¶ 61,260 (2008) and *Midwest Independent Transmission Operator, Inc.,* Order Conditionally Accepting Proposed Tariff Revisions, 128 FERC ¶ 61,229 (2009).

[116] The Regional Entities also received very few complaints and conducted very few investigations (as that term is defined in the CMEP) during the assessment period as follows:

	FRCC	MRO	NPCC	RF	SERC	SPP RE	TRE	WECC
Complaints	2	1	6	4	4	1	3	0
Investigations	0	3	3	3	3	3	3*	1

*One of TRE's investigations involved a 2011 winter event that led to a FERC/NERC staff report, *Report on Outages and Curtailments During the Southwest Cold Weather Event on February 1-5, 2011*. *See* http://www.ferc.gov/legal/staff-reports/08-16-11-report.pdf.

[117] *See Southwestern Power Administration, et al. v. FERC*, No. 13-1033 (D.C. Cir. Feb. 15, 2013).

obtain more experience with hearings and appeals before any significant changes are made to Attachment 2.[118]

3. Additional Statutory Functions

The 2009 JRESA identified four other functions which are primarily the ERO's responsibility but which require the active involvement, cooperation, and assistance of the Regional Entities—Reliability Assessment, Event Analysis, Situation Awareness, and Critical Infrastructure Protection.[119] In regard to Reliability Assessment, Event Analysis, and Situation Awareness, NERC and some industry members expressed concerns about the Regional Entities' performance. In regard to Critical Infrastructure Protection, the Regional Entities noted a concern they had. As now demonstrated, during the assessment period, the Regional Entities successfully took steps to address and otherwise allay the concerns of NERC and the industry members, and had its own concern satisfactorily addressed as well.[120]

a. Reliability Assessment

FPA §215(g), 16 U.S.C. §824o(g), provides that "[t[he ERO shall conduct periodic assessments of the reliability and adequacy of the bulk-power system in North America." Section 39.11 of the Commission's regulations, 18 C.F.R. §39.11 (2013), additionally directs the ERO to conduct such assessments and provide reports to the Commission and other designated entities. Accordingly, NERC prepares the annual *Long-Term Reliability Assessment*, *Summer Assessment*, *Winter Assessment*, and special assessments as needed. To this end, as can be gleaned from the NERC's *Reliability Assessment Guidebook* (version 3.1), NERC relies heavily on the Regional Entities to prepare these reports.[121] Indeed, as anticipated in the 2009 JRESA, the finalization of this guidebook during the assessment period adequately responded to the issues raised during the preparation of the Regional Entities' first performance assessment.[122] Nonetheless, the Regional Entities are committed to continue working with NERC to improve data collection and validation, and to foster greater alignment across the regions in the conduct of high quality, timely, and independent assessments that support the ERO Enterprise's valuation of reliability.

---

[118] Notably, the Commission approved a major change to the TRE hearing procedures in August 2013, allowing TRE to change its hearing process, which previously provided for the Texas Public Utility Commission to serve as the hearing body, to be the same as used by the other seven Regional Entities. *See North American Electric Reliability Corporation*, Docket No. RR13-7-000 (August 19, 2013) (unpublished delegated letter order).

[119] *See* 2009 JRESA, at pp. 32-33.

[120] Additionally, as budget matters were discussed at various places in the 2009 JRESA, this section concludes with a brief overview of Regional business plans and budget activities during the assessment period.

[121] *See* http://www.nerc.com/pa/RAPA/rg/ReliabilityGuidelines/Reliability_Assess_Guidebook_3_1Final.pdf.

[122] Concerns at that time included data checking and validation, process and procedures, stakeholder/member involvement, and overall quality and timeliness.

b. Event Analysis

In the 2009 JRESA, the Regional Entities agreed with industry members that work needed to be done on the process of timely conducting, and disseminating information gathered from, event analyses performed by NERC and the Regional Entities.[123] Without question, the ERO Enterprise made tremendous strides during assessment period to address these concerns and otherwise improve the very critical reliability function of analyzing events and distributing lessons learned to the entire reliability community. For their part, the Regional Entities significantly contributed to this effort by helping to organize and actively participating in the voluntary ERO event analysis program.

By way of background, following the creation of the NERC Event Analysis Working Group (EAWG) and two industry trials in 2010, NERC approved an industry-wide event analysis program in February 2012, and revised it in 2013.[124] This voluntary program recognizes the need to establish an appropriate level of review for the events which occur on the BPS based on their varying levels of significance, while still providing otherwise unrealized lessons to be learned from both major and minor occurrences. To complete this effort, the registered entity, the Regional Entity, and NERC staff collaborate to prepare an event analysis report, identify root cause and contributing causes, perform a formal "cause-coding" analysis, and publish lessons learned gathered from the disturbance. The process also encourages registered entities to establish a liaison between their internal event analysis and compliance functions for development of a registered entity compliance self-assessment report separate from the event analysis report. During the assessment period, this integration of industry engagement and the collaborative review of disturbances greatly improved the effectiveness, consistency, and timeliness of event analyses performed by NERC and the Regional Entities.

The following shows the progress made by the voluntary ERO event analysis program, developed by NERC, the Regional Entities, and stakeholders. Between October 2010 and December 31, 2013, registered entities submitted 469 event reports through the program, two-thirds of which were classified as Category 1.[125] Generally, the registered entities were very

---

[123] The *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011, Causes and Recommendations* (August 2011) (2011 Southwest Cold Weather Event) neatly summarizes the event analysis process:

> Registered entities are required to report the occurrence of defined bulk power system disturbances and unusual occurrences to the appropriate Regional Entity and to NERC. The Regional Entity and/or NERC in turn undertakes various levels of analysis to determine the causes of the events, assure tracking of corrective actions to prevent recurrence, gather information needed to assess compliance, and provide lessons learned to the industry. The event analysis process also provides input for training and education, reliability trend analysis efforts and Reliability Standards development, all of which support continued reliability improvement.

http://www.ferc.gov/legal/staff-reports/08-16-11-report.pdf, at p. 23.

[124] *See* http://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/Final_ERO_EA_Process_V2.1.pdf. The EAWG eventually transitioned to the NERC Event Analysis Subcommittee.

[125] A Category 1 event includes, among other things, an unexpected outage, contrary to design, of three or more BPS elements caused by a common disturbance. *See* generally *Electric Reliability Organization Event Analysis Process*,

supportive of the process and worked with the Regional Entities' staffs to improve the quality of the reports, even providing subject matter experts to participate in calls to ensure that the reports were completely understood to more effectively assign categories and cause codes. The Regional Entities' staffs, in turn, were fully committed to the success of the lessons learned aspect of the program, and attempted to keep the registered entities up to date on the program and to help develop meaningful lessons learned. As is well known, during the assessment period, the two most notable event analyses were performed by NERC and FERC staffs with respect to the 2011 Southwest Cold Weather Event and the 2011 Arizona-Southern California Outages.[126] In both matters, the reports provided valuable information and recommendations that were closely examined by the other Regional Entities for application in their areas.[127]

c. Situation Awareness

The 2009 JRESA touched briefly on situation awareness, and took note that NERC and the Regional Entities were actively participating with FERC to enhance situation awareness by having RCs provide near-real-time operating information for their respective footprints to the Commission, NERC and the Regional Entities in order to permit the Commission to "measure the health" of the Interconnections and to monitor parameters which might warn of a developing crisis. The Regional Entities cautioned in 2009 that the communication protocols should be followed in order to prevent this effort from exposing system operators to distracting inquiries during emergency situations. Since then, as now explained, the efforts underway in 2009 were largely successful and the Regional Entities' concerns were satisfactorily addressed.

During the assessment period, FERC, NERC, and Regional Entity staffs worked together to develop a near-real time situation awareness visualization tool called SAFNR (**S**ituation **A**wareness for **F**ERC, **N**ERC, and the **R**egional Entities). SAFNR version 1 was implemented in June 2009. SAFNR version 2, which provides enhanced situation awareness with increased

---

Appendix E: Categorization of Events (February 2012) at http://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/ERO_Event_Analysis_Process_Document_Version_1_Feb_2012.pdf. There was only one Category 5 event during the assessment period—Hurricane Sandy in 2012.

The events covered by the reports break down by Regional Entity as follows:

FRCC	MRO	NPCC	RF	SERC	SPP RE	TRE	WECC
25	41	69	47	42	13	69	163

[126] *See* n. 125 and *Arizona-Southern California Outages on September 8, 2011, Causes and Recommendation*s (April 2012) (2011 Arizona-Southern California Outages) http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf. *See also Arizona Public Service Company*, Order Approving Stipulation and Consent Agreement, 148 FERC ¶ 61,009 (2014) (approving first settlement in 2011 Southwest Blackout case between FERC's Office of Enforcement, NERC, and Arizona Public Service Company).

[127] For example, in light of the recommendations in the Arizona-Southern California Outages report, SPP RE staff conducted a survey of entities regarding operational planning and real-time situational awareness, and worked with the SPP RTO and the SPP Event Analysis Working Group to craft training materials. In addition, the SPP RTO implemented a daily benchmark process of the "next day" models to validate load forecasting and generation dispatch assumptions as well as voltage performance. Also in consideration of the recommendations in that report, WECC launched an initiative to improve modeling of remedial action schemes and relays.

trending capability, was completed in late 2012. As contemplated in the 2009 JRESA, SAFNR calls for U.S. RCs to provide system conditions via the internet to FERC, NERC, and the Regional Entities thereby allowing them to monitor continuously operating conditions and emerging reliability events on the BPS. In addition to the near-real time monitoring capabilities of SAFNR, the RCs send situation awareness reports every morning to the Commission, NERC, and the Regional Entities. These reports include an overview of weather conditions, transmission line and generation outages, and operating reserves. Furthermore, the Regional Entities participate in weekly situation awareness and event analysis conference calls with NERC. From the Regional Entities' perspective, the combination of SAFNR, the daily situation awareness reports, and the weekly calls with the ERO, give them a good overview of what is happening on the BES. And, of course, they are in regular communication with the registered entities within their footprints, in particular the RCs, and provide those entities with the means to contact them or receive pertinent information from them at all times with respect to any incidents or events on the grid.[128]

d. Critical Infrastructure Protection

The 2009 JRESA posited only one issue with respect to CIP, namely that the Commission should approve a pending proposal to amend the NERC ROP to provide that any Technical Feasibility Exception (TFE) requests (from the coverage of the CIP Reliability Standards) be submitted in the first instance to the Regional Entities, rather than to NERC.[129] Early in the assessment period, the Commission approved the proposed amendment, thus mooting the issue raised in 2009.[130] More recently, in September 2013, the Commission approved what NERC described as the first comprehensive review of the TFE process since it was originally developed and approved.[131] The Commission explained that NERC and the Regional Entities had processed by that time over 3,800 TFE requests in the past three years, including over 1,300 TFE requests in 2011, experience that supported NERC's proposal to streamline the process for submitting, reviewing, and approving or disapproving TFE requests, and for modifying approved TFEs.[132] The Regional Entities are pleased that the Commission

[128] For example, WECC established a web portal to allow BAs and TOPs access to actual RC real-time state estimator, contingency analysis, and other situational awareness-enhancing tools. NPCC introduced the *Emergency Preparedness Conference Call Procedures* to enable the RCs in its footprint, and, as circumstances may require, their counterparts in neighboring Regional Entities, to rapidly communicate the status of current operating conditions, facilitate the procurement of assistance during emergency conditions, and identify potential physical or cyber threats to the system.

[129] TFE requests primarily arise with respect to long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern. *See Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 (2008), at P 180.

[130] *See North American Electric Reliability Corporation*, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 FERC ¶ 61,050 (2010).

[131] *See North American Electric Reliability Corporation,* Order Approving Revisions to Electric Reliability Organization's Rules of Procedure and Directing Compliance Filing, 144 FERC ¶ 61,180 (2013), *order on compliance*, Docket No. RR13-3-001 (January 30, 2014) (unpublished letter order).

[132] *Id.* P 12.

approved NERC's proposed amendments, which will help reduce TFE processing times while maintaining the integrity of the CIP mandatory Reliability Standards.

In addition, during the assessment period, the Regional Entities significantly expanded the number and the expertise of their staffs, in particular their auditors, to verify compliance with the CIP mandatory Reliability Standards. They uniformly hired personnel with relevant credentials and experience. For example, SPP RE's audit team (as of mid-2013) had over 94 years of information technology, cybersecurity, and IT audit experience, including 52 years of experience in the electricity sector, and FRCC required (as of mid-2013), as a condition of employment, five years of experience in cybersecurity practices, information technology, auditing practices, implementation of NERC Reliability Standards, or other equivalent experience. Moreover, by the end of the assessment period, many of the Regional Entities' employees held active certifications recognized by the U.S. Department of Defense Directive 8570 (e.g., Certified Information Systems Auditor (CISA), Certified Information Systems Security Specialists (CISSP), Certified Ethical Hacker (CEH), and Network +). They also sought out personnel who understood energy management systems (EMS) and supervisory control and data acquisition (SCADA) systems and several of them augmented their staffs' expertise with contractors who held similar credentials and experience.

Needless to say, the Regional Entities recognize the incredibly important role that cybersecurity plays in the fulfillment of their statutory responsibilities.[133] Accordingly, during the assessment period, they uniformly expended considerable resources and effort to organize their CIP programs and to enforce the mandatory CIP Reliability Standards. Several also initiated on-site visits at their registered entities to assess their physical security, to discuss with those entities the intricacies of complying with the CIP Reliability Standards, and to explore best industry practices with respect to cybersecurity. In addition, the Regional Entities improved their own technology to be able to handle the transport and storage of the especially sensitive information that they collect in CIP compliance audits and investigations.

Finally, during the assessment period, Regional Entities participated in two NERC Grid Security Exercises (GridEx), which use best practices from the Department of Homeland Security, the Federal Emergency Management Agency, and the National Institute of Standards and Technology. Six Regional Entities (MRO, NPCC, RF, SERC, TRE, and WECC) joined 70 industry and government organizations in the 2011 GridEx, on November 16, 2011 through November 17, 2011, and six Regional Entities (FRCC, MRO, NPCC, RF, SERC, and TRE) joined more than 200 industry and government organizations, either as full participants or as observers, in the 2013 GridEx on November 13, 2013 through November 14, 2013. The 2011 GridEx was designed to validate the readiness of the Electricity Sub-sector to respond to a cybersecurity incident, strengthen registered entities' crisis response functions, and provide input for internal security program improvements. Overall, the exercise was widely regarded across industry and government as a critical imperative in preparing the BPS for a disruptive cyber event.[134] The 2013 GridEx gave participants the opportunity to check the readiness of their crisis

[133] *See* 16 U.S.C. §§824o(a)(3) and (4).

[134] *See 2011 NERC Grid Security Exercise After Action Report* (March 2012) at http://www.nerc.com/pa/CI/CIPOutreach/Documents/NERC%20GridEx%20AAR%2016Mar2012%20Final.pdf.

action plans through a simulated security exercise to self-assess response and recovery capabilities, and to adjust actions and plans as needed, while communicating with industry and government information sharing organizations.[135]

4. Budget

The 2009 JRESA mentioned various budget matters but did not include a separate section on the topic. The significant progress made in this area during the assessment period by the Regional Entities under NERC leadership calls for at least a brief discussion here. Also, as related generally in the Introduction and specifically by each Regional Entity in Appendix C, the Regional Entities are required by FPA §215 to establish rules that "allocate equitably reasonable dues, fees, and other charges among end users for all activities," an obligation that obviously necessitates that they function under a business plan and a budget. The Regional Entities first approached these budget responsibilities during the assessment period by developing, in collaboration with NERC, and proposing annual business plans and budgets, in accordance with Commission orders, ERO rules, and NERC business planning and budgeting policies and instructions. For this purpose, they used NERC forms for business plan and budget submittal and adhered to NERC's schedule for preparation of the business plan and budget and related financial statements. They likewise followed NERC's prescribed system of accounts (except to the extent that NERC permitted a departure from the prescribed system of accounts).

The Regional Entities made significant progress in the development and submission of their annual business plans and budgets partly as a result of their active participation in the Regional Entity Budget Group (REBG), which transitioned during the assessment period to the ERO Finance Group (EROFG). This group reviewed templates, budget processes, schedules and deadlines, account classifications, financial reporting, and accounting changes. Members of the group were able to share information concerning benefits, salaries, policies, and procedures that are used in the day-to-day accounting activities in the regions. The Regional Entities also took advantage of the opportunity to preview their preliminary annual budgets for Commission staff, and receive feedback generally and with respect to staffing needs and extraordinary items. They further worked with NERC to develop long term resource and financial planning, and to formulate a set of "common assumptions," which helped to clarify expectations. As a consequence of the concerted efforts made by NERC, the Regional Entities, and the EROFG, the regional budget process significantly improved during the assessment period, progressing from a level of some uncertainty to a level of considerable predictability regarding needed resources and anticipated expenses.[136]

---

[135] *See Grid Security Exercise (GridExII) After-Action Report* (March 2014) available at: http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf. The Regional Entities were also represented at the "tabletop" of executives from government, industry, and NERC, which took place after the 2013 exercise.

[136] An excellent overview of the progress made by the ERO Enterprise during the last year of the assessment period in preparing the Regional Entities' 2014 business plans and budgets can be found in NERC's *Request for Acceptance of 2014 Business Plans and Budgets of NERC and Regional Entities and for Approval of Proposed Assessments to Fund Budgets*, Docket No. RR13-9-000 (submitted on August 23, 2013), at pp. 24-30. *See also*

CONCLUSION

The ERO Enterprise significantly matured during the assessment period, building on the foundation of the first three years of the program in which the ERO and the Regional Entities had to set up and organize their operations to implement a sweeping new set of Federal laws, regulations, policies and practices under the oversight of the Commission. Those first three years were truly a time of learning and adjusting to the new paradigm. The next five years, the current assessment period, were a time to learn from experience and explore ways to improve, refine, and stabilize the program. The Regional Entities successfully contributed to those objectives in several ways. They worked more closely and productively with the ERO and with each other. They reached out to and trained their registered entities and other stakeholders. They actively participated in FERC proceedings to keep the Commission informed and to help craft orders and policies that appropriately advance reliability. They continuously examined ways to be more efficient and effective in exercising their compliance enforcement authority and to better gauge the risk that noncompliance posed to reliability. Finally, at all times, they met their statutory obligations to be impartial, develop reasonable and technically sound standards, enforce those standards with due process, operate within sound business plans and budgets, coordinate their efforts in North America, where applicable, and function under RDAs that promote effective and efficient administration of BPS reliability.

North American Electric Reliability Corporation, Order on 2014 Business Plan and Budget of the North American Electric Reliability Corporation and Ordering Compliance Filing, 145 FERC ¶ 61,097 (2013).

Appendix A
Description of Regional Entities

A Regional Entity is an organization that has been delegated certain statutory functions of the Electric Reliability Organization (ERO). The ERO and each Regional Entity consummate the delegation through the execution of a Delegation Agreement, which must be approved by the Federal Energy Regulatory Commission (Commission or FERC) in the U.S. By entering into such an agreement, the Regional Entity becomes subject to the jurisdiction of the FERC and the rules of procedure of the ERO.

In July 2006, when the Commission certified the North American Electric Reliability Corporation (NERC) as the ERO, it also accepted NERC's proposal to delegate certain ERO functions to designated Regional Entities, as well as NERC's proposed *pro forma* Delegation Agreement.[137] In April 2007, NERC entered into separate Delegation Agreements with eight Regional Entities, through which NERC delegated certain ERO functions. Specifically, NERC delegated authority to the Regional Entities to audit, investigate, and otherwise ensure that users, owners, and operators of the BPS comply with NERC's mandatory Reliability Standards, subject to ERO oversight.[138] Further, the Delegation Agreements addressed: (i) Regional Reliability Standards development; (ii) registration of entities that must comply with Reliability Standards; and (iii) other services supporting NERC's functions, including reliability assessments, event analysis, and training and education. In October 2010, the Commission approved a revised *pro forma* Delegation Agreement, and revised Delegation Agreements between NERC and each of the eight Regional Entities.[139] Subsequently, the Commission also approved other changes to specific Delegation Agreements.[140]

As shown in Figure 1, the existing eight Regional Entities provide full geographic coverage for the jurisdictional scope of NERC as the international ERO.

---

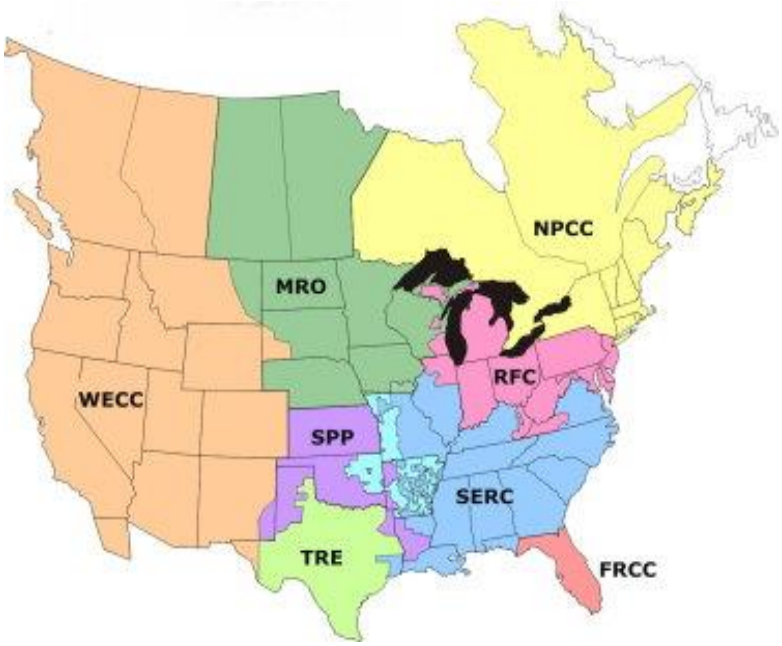
[137] *See North American Electric Reliability Corporation*, Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing, 116 FERC ¶ 61,062, *order on reh'g*, 117 FERC ¶ 61,126 (2006).

[138] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,060, *order on reh'g,* 120 FERC ¶ 61,260 (2007).

[139] *See North American Electric Reliability Corporation*, 133 FERC ¶ 61,061 (2010), *order on reh'g*, 134 FERC ¶ 61,179, *order on compliance filing*, 137 FERC ¶ 61,028 (2011).

[140] *See*, e.g. *North American Electric Reliability Corporation*, Docket Nos. RR13-7-000 (Aug. 19, 2013) (TRE), RR13-5-000 (June 12, 2013) (MRO), RR12-12-000 (Oct. 24, 2012) (RF), RR12-4-000 (June 12, 2012) (FRCC), and RR12-2-000 (March 1, 2012) (WECC) (unpublished delegated letter orders).

Figure 1 — Map of Regional Entities within NERC



Each of the Regional Entities is briefly described below.

Florida Reliability Coordinating Council, Inc. (FRCC) was formed in 1996. Its sole purpose is to ensure and enhance the reliability and adequacy of the BPS in Florida. Since becoming a Regional Entity, FRCC has made significant changes in its governance and organizational structure. FRCC amended its bylaws to create two membership divisions — Regional Entity Division (statutory functions) and Member Services Division (non-statutory functions), added a new General Sector to its membership sectors, added new employees strictly dedicated to the compliance and standards functions, and made changes in its organizational reporting structure. All staff members are independent of registered entities, and the organization is governed by a balanced stakeholder board. FRCC has also implemented internal controls in its accounting procedures to ensure there is no cross subsidization of funds between statutory and non-statutory activities.

Midwest Reliability Organization (MRO) was formed from the former Mid-Continent Area Power Pool (MAPP) Regional council and a portion of Mid-America Interpool Network (MAIN) as a new corporation for the purpose of becoming a Regional Entity under the Energy Policy Act of 2005 and the Bilateral Principles. The region spans eight states and two Canadian provinces. MRO's bylaws provide for members from the following industry sectors: municipal utilities, cooperatives, investor-owned utilities, federal power marketing agency, Canadian Crown Corporations, and independent power producers. MRO's bylaws also allow for adjunct members that are not eligible to belong to an industry sector and have a material interest in reliability issues in the MRO region. Membership is at no cost. MRO is independent of all BPS owners, operators, and users, and has no shared employees with any third party. MRO performs only responsibilities delegated from the ERO and similar functions in the Canadian provinces of Saskatchewan and Manitoba. MRO's board of directors (MRO Board) represents a hybrid

governance structure with both independent and stakeholder directors. The stakeholder directors represent the industry sectors noted above; two independent directors are elected by the entire membership. MRO's hybrid board is structured so that no two sectors can control a vote. The MRO Board has adopted procedures to ensure that it carries out its responsibilities in a non-discriminatory manner, free of conflicts.

Northeast Power Coordinating Council, Inc. (NPCC) was established as the voluntary, international regional reliability organization for Northeastern North America in January 1966. NPCC is a not-for-profit corporation with a Regional Entity division that performs the statutory functions delegated by NERC and a Criteria Services division that establishes, monitors, and enforces compliance with regionally-specific criteria. The NPCC geographic region includes the State of New York and the six New England states as well as the Canadian provinces of Ontario, Québec and the Maritime provinces of New Brunswick and Nova Scotia. Overall, NPCC covers an area of nearly 1.2 million square miles, populated by more than 55 million people. In total, from a NEL perspective, NPCC is approximately 45% U.S. and 55% Canadian. With regard to Canada, approximately 70% of Canadian NEL is within the NPCC region. NPCC's board of directors consists of seven stakeholder voting sectors that each consist of a maximum of two directors per sector, an independent sector consisting of two independent directors, an independent board chair with voting rights to preclude board deadlocks, and the President and CEO. Within NPCC, no two sectors can control and no one sector can block action.

ReliabilityFirst Corporation (RF) was formed from parts of the former East Central Area Reliability Council (ECAR), MAIN, and the Mid-Atlantic Area Council (MAAC) Regional reliability councils on January 1, 2006. The organization was specifically designed to address changes required by the Energy Policy Act of 2005 and to support the ERO in a self-regulating model by which the industry participants establish their own standards and independent Regional Entities determine compliance to those standards. The organization was modified from top to bottom compared to the legacy reliability councils it replaced, and exists solely to serve as a FERC-approved Regional Entity performing only those functions delegated to it by NERC as the ERO. All ReliabilityFirst staff are independent of registered entities, the organization is governed by a hybrid board of directors, which includes both independent and balanced industry sector directors, and the organization is funded (through the ERO) by all load-serving entities in the footprint as opposed to members (membership is free.)

SERC Reliability Corporation (SERC) was incorporated in April 2005, replacing the Regional reliability council previously in existence since 1969. The new organization was redesigned to meet FPA §215 and FERC criteria for delegating statutory authorities and responsibilities. SERC's scope includes only statutory functions delegated by NERC. The organization does not perform any registered entity functions and has no business affiliations with any registered entities. SERC adopted new bylaws, approved by FERC in April 2007, that provide for a balanced stakeholder board with seven sectors. All SERC staff are independent of registered entities. The organization is funded through the ERO. Membership is free and open to all owners, operators, and users in the SERC region.

Southwest Power Pool Regional Entity (SPP RE) has made fundamental governance and organizational changes necessary to carry out its delegated responsibilities. In response to

the Energy Policy Act of 2005, Southwest Power Pool, Inc. (SPP), created a new department to perform all compliance activities over SPP registered entities. SPP RE began engaging NERC to lead SPP audits in 2007. In April 2007, FERC approved changes to the SPP bylaws creating three independent trustees to manage all SPP RE delegated activities. These trustees, initially elected in June 2007, are required to be independent of SPP members and customers, and registered entities in the region. In March 2009, SPP RE hired a general manager, reporting directly to the three independent trustees, to oversee the execution of the Regional Entity strategic direction and direct the day-to-day operations, including all compliance and enforcement activities. The general manager oversees only delegated statutory functions. All reporting relationships between SPP RE employees and SPP employees have been terminated.

Texas Reliability Entity, Inc. (Texas RE or TRE) is a non-profit Texas corporation that was formed to serve as the Regional Entity for the Electric Reliability Council of Texas, Inc. (ERCOT) region, and to preserve and enhance reliability in the region. Effective July 1, 2010, Texas RE took over the duties of the previous Regional Entity, the Texas Regional Entity, an independent division of ERCOT. Texas RE also performs non-statutory activities as the Reliability Monitor for the ERCOT region pursuant to its July 1, 2010, agreement with the Public Utility Commission of Texas (PUCT) and ERCOT (the ISO in the region). As Reliability Monitor, Texas RE monitors and reports to the PUCT regarding market participants' compliance with electric reliability-related ERCOT Protocols, Operating Guides, and Texas rules (ERCOT Regional Rules). The ERCOT region is the geographic area located within the state of Texas that operates under the jurisdiction of the PUCT and is not synchronously interconnected with any electric utilities operating outside of Texas. The ERCOT region includes approximately 85 percent of Texas load and 75 percent of the Texas land area.

Western Electricity Coordinating Council (WECC) is the successor to the Western Systems Coordinating Council (WSCC), which was formed in 1967. WECC, established in April 2002, continues to be responsible for promoting and coordinating electric system reliability among industry stakeholders as had been done by WSCC since its formation. On July 20, 2006, pursuant to FPA §215, NERC was certified as the ERO in the U.S. Included in this certification was a provision for the ERO to delegate authority for the creation and enforcement reliability to Regional Entities such as WECC. WECC is geographically the largest and most diverse of the eight Regional Entities that have Delegation Agreements with NERC. WECC's service territory extends from Canada to Mexico. It includes the provinces of Alberta and British Columbia, the northern portion of Baja California, Mexico, and all or portions of the 14 Western states between. Due to the size and diverse characteristics of the region, WECC and its members face unique challenges in coordinating the day-to-day interconnected system operation and the long-range planning needed to provide reliable electric service across nearly 1.8 million square miles. Membership in WECC is open to all entities with an interest in the operation of the BPS in the Western Interconnection. All meetings are open and anyone may participate in WECC's standards development process.

On June 27, 2013, the WECC board of directors (WECC Board) approved the bifurcation of the company into a Regional Entity (WECC) and a Reliability Coordination Company (Peak Reliability). This decision—which is the culmination of a year of work by various WECC board committees, staff, WECC members, and WECC stakeholders—signals a major landmark in the

history of the organization. Under this new structure the reliability coordinator and interchange authority functions in the Western Interconnection became a separate company from WECC. When established, Peak Reliability will provide core and other associated reliability coordination services within the Western Interconnection. As anticipated, the Commission approved the relevant documents by the end of December 2013; however, as there were outstanding compliance filings, the bifurcation was not finalized during the assessment period. Nevertheless, WECC and Peak Reliability began operating as separate entities in many respects by that time.

Appendix B
Regional Entity Responses to Specific Concerns Raised in the Commission's September 16, 2010 Order on the Three-Year ERO Performance Assessment

In the order on the Electric Reliability Organization's Three-Year Performance Assessment (2010 Order), the Commission discussed several specific concerns regarding Regional Entity activities including: (i) compliance monitoring and enforcement issues concerning all Regional Entities; (ii) NERC's evaluation of each Regional Entity compliance program; (iii) SPP independence; and (iv) WECC's voting structure.[141] The first topic has been addressed throughout the 2014 JRESA. The other three region-specific topics are addressed below (italicized paragraphs come from the 2010 Order).

NERC's Evaluation of Each Regional Entity

222. *With respect to **FRCC**, NERC states that FRCC needs to improve its timeliness in: (1) reporting alleged violations to NERC; (2) issuing notices of alleged violation; (3) confirming violations and issuing notices of confirmed violation or entering into settlement agreements; and (4) obtaining Board of Trustees Compliance Committee approval of confirmed violations. NERC relates that FRCC recently has increased its compliance program staffing and, as of the Performance Assessment filing date, had the second lowest number of registered functions per full-time equivalent (FTE) committed to compliance of any Regional Entity.*

The FRCC improved its timeliness in all aspects of the compliance and enforcement processes during the assessment period. Notices of alleged violations, notices of confirmed violations and settlements were handled by the FRCC Compliance Enforcement staff. In January 2010, FRCC created a new position of manager of compliance enforcement, promoted a senior auditor to that position, and added two new enforcement positions, an enforcement specialist and a compliance legal assistant. The enforcement specialist position was filled in January 2010, and the legal assistant was filled in May 2010. Subsequently, the FRCC added two more enforcement positions, both CIP enforcement specialists. With the increased enforcement staff, the FRCC worked steadily to improve all of its processes. Additionally, FRCC developed internal processes and goals to support and facilitate the processing of alleged violations, as follows:

- Created enforcement processing checklists;
- Developed violation and mitigation plan responsibility flowcharts;
- Developed enforcement procedures;
- Created annual success plan goals for enforcement team members;
- Implemented departmental caseload goal;
- Developed internal enforcement processing metrics;
- Collaborated with other Regional Entities in a Consortium Users Group (CUG) to improve data base management tool;
- Automated database reporting tools which improved efficiency;

[141] *North American Electric Reliability Corporation, et al*., 132 FERC ¶ 61,217 (2010) at PP 198-244.

- Implemented a secure vault system for registered entity CIP data, which eliminated onsite reviews; and
- Compiled with NERC requests to complete processing of all violations through 2011 to NERC goals.

223. *NERC views **MRO** as an effective Regional Entity. NERC indicates that MRO should improve by providing accurate statements of fact for each violation and assess penalties according to the facts of each situation. NERC has concerns about several of MRO's compliance processes, which NERC has not yet reviewed or approved. NERC states that although these methods may be effective, they are not consistent with NERC practices and could lead to inconsistency with other regions.*

NERC's 2009 assessment alluded to two situations which occurred in that year. The first involved the issuance by FERC of a formal notice extending the time for consideration of a NOP (NP09-21-000), in which FERC requested additional information and clarification of certain facts. While MRO was the first of the Regional Entities to receive such a formal notice, similar notices were subsequently issued to all of the Regional Entities. In some instances, the Commission issued multiple requests to the same region. In only one instance, during the assessment period, did the Commission undertake its own review of a regional enforcement determination (WECC decision in Turlock, FERC Docket No. NP10-18-000), which was ultimately affirmed. MRO has not received any other formal requests from FERC for additional information and clarification.

Also in 2009, the NERC BOTCC remanded an enforcement action because MRO characterized a self-certification as a self-report in its determination. This was a simple administrative error, which MRO appreciates being found by NERC. Subsequently, MRO worked with NERC staff to develop a process whereby NERC staff works with Regional Entity staff to ensure agreement with or clarification of discrepancies prior to presenting enforcement actions to the BOTCC for approval. At the time, the MRO self-certification process was a manual process, which then required MRO compliance staff to enter the information into the data management system (CDMS). In this instance, MRO compliance staff entered the self-certification into the CDMS application as a self-report without indicating that the possible violation was actually identified through the self-certification process. This was the only instance where such an error occurred and it did not change the enforcement determination.

Finally, MRO believes that NERC's concerns about several of MRO's compliance processes, which NERC stated may be effective, were due to NERC's misunderstanding MRO's practices at the time. Shortly before the submission of the 2009 JRESA, MRO adopted its three-step process for activities within the CMEP: (i) Compliance Monitoring, (ii) Risk Assessment and Mitigation, and (iii) Enforcement, each performed by its own personnel within MRO. Compliance Monitoring staff conducts audits and spot checks of compliance with Reliability Standards by registered entities. Risk Assessment and Mitigation undertakes an independent review of the facts and circumstances surrounding each violation discovered by Compliance Monitoring, and determines whether sufficient evidence supports each possible violation. Risk Assessment and Mitigation works with the registered entity to develop an effective mitigation plan in the event that a violation is confirmed. Confirmed violations move to the Enforcement

department staff, who review recommendations made by Risk Assessment and Mitigation staff, verify all relevant facts, and evaluate appropriate enforcement actions. The factual review conducted by Risk Assessment and Mitigation and Enforcement staff is intended to ensure a consistent, accurate application of the NERC Reliability Standards. The three-step process also provides for segregation of duties, establishing independence among those making the findings, those assessing risk, and those determining and negotiating penalties and sanctions. MRO believes that this process provides a high level of assurance that determinations are accurate, fair and non-discriminatory.

224. *NERC views **NPCC** as effective in that it is processing and completing identified violations in a timely manner. However, NERC is concerned that NPCC's low level of alleged violations per registered reliability function may indicate that NPCC is not identifying all violations that are occurring. NERC points out that, among the Regional Entities, NPCC had the second highest number of FTEs committed to the compliance program and the highest ratio of registered functions per compliance FTE as of the Performance Assessment filing date. NERC states that it will continue to work with NPCC to improve its process for compliance violation investigations.*

NPCC continues to have a low level of alleged violations per registered reliability function; however, the ratio is in line with several of the other Regional Entities. NPCC credits in part its low level of alleged violations per registered reliability function to its thorough outreach and communication both on an individual basis and through workshops and other forums with the registered entities within its region. Such outreach assists the registered entities in their compliance activities and enhances reliability. In addition, by the end of the assessment period, while NPCC had the lowest number of full-time equivalents (FTEs) committed to the compliance program and the highest ratio of registered functions per compliance FTE, it supplemented its compliance program with independent contractors that perform many of the compliance duties. In this manner, NPCC has been able to build a very cost effective compliance program. NPCC welcomes ERO-wide collaboration on improvements to the process for compliance violation investigations and other process related issues, and is actively involved in RAI-related projects, including running pilots on analyzing registered entities' internal controls, the auditor check list and workbook, and the transition from CIP version 3 to version 5 Reliability Standards.

225. *NERC and its outside auditing firm independently audited **RF's** compliance program and found no material deficiencies. NERC observes that RF was the first Regional Entity to receive approval from the NERC Board of Trustees Compliance Committee for a notice of penalty that imposed a non-zero dollar penalty. NERC notes that RF does need to find ways to increase its efficiency with respect to conducting enforcement activities.*

Since 2009, ReliabilityFirst has taken several steps to increase its efficiency with respect to conducting enforcement activities.

First, ReliabilityFirst has internal violation processing goals that are tied to its overall corporate goals. Second, enforcement staff members hold regular meetings to discuss their plans to meet these violation processing goals. At these meetings, enforcement staff members provide

projected timeframes for the resolution of their matters, and are held accountable to those timeframes. Third, ReliabilityFirst has held formal and informal meetings to better focus enforcement staff on how to tailor their fact gathering efforts and resolving documents to only relevant information. As a result, enforcement staff became more efficient at resolving violations in a shorter amount of time. Fourth, ReliabilityFirst has focused its efforts on those violations that pose the greatest risk to reliability, and expedited its processing of lesser risk violations via the FFT process. To date, ReliabilityFirst has processed approximately 330 FFTs. (Even prior to the FFT process, ReliabilityFirst followed an internal "fast track" process, where it expedited the processing of minimal risk violations in a separate internal process from its other violations.)

ReliabilityFirst's efforts to increase its efficiency in the enforcement process were successful, and to date, ReliabilityFirst has processed over 1,400 alleged violations through NERC and the Commission. The volume of compliance work at ReliabilityFirst has increased significantly since the 2009 self-assessment,[142] but ReliabilityFirst has nevertheless become more efficient at processing violations. As a result, ReliabilityFirst has not only kept up with its caseload, but has simultaneously refined its approach to better focus its efforts on high risk violations and ensuring that major reliability enhancements result from their corresponding enforcement actions. ReliabilityFirst staff's focus on high risk violations is fundamental to regulatory effectiveness as it is critical to prevent staff at the Regional Entities from spending unnecessary amounts of time on minimal risk issues, so they can focus on the high risk issues that are critical to reliability.

226. *NERC views **SERC** as an effective Regional Entity. NERC audited SERC's compliance program and did not find any material deficiencies, but urges SERC to improve on its timeliness in issuing notices of alleged violation. NERC notes that SERC continues to use industry volunteer subject matter experts in addition to its own staff on compliance audits.*

SERC made significant progress during the assessment period to address the concerns raised in 2009. For example, in order to improve violation processing cycle time, SERC staff developed a comprehensive plan that included increasing productivity, improving process and tools, and reviewing staffing levels. This plan was unanimously approved by the SERC Board Executive Committee.[143] Furthermore, SERC implemented process improvements in order to

[142] In 2009, ReliabilityFirst received 169 new violations, and in 2010, this number jumped to 453 violations. In 2011, ReliabilityFirst received 514 violations, in 2012, ReliabilityFirst received 549 violations, and as of August 9, 2013, ReliabilityFirst received 520 violations.

[143] In 2011, SERC removed some collateral duties from Enforcement staff to ensure a focus on violation processing and reduced the ancillary meetings attended by Enforcement staff by 50%. In 2011, SERC developed a corporate metric focused on improving violation processing time, increasing the average number of determinations completed per FTE from 1.4 determinations per month to 4 determinations per month. In 2012, SERC developed a corporate metric focused on improving violation processing to continue its work towards achieving a 12-month violation processing cycle time for Planning and Operations issues. In 2013, SERC developed a corporate metric focused on improving CIP violation processing to continue its work towards achieving a 12-month violation processing cycle time while maintaining a 12-month or less violation processing cycle time for Planning and Operations issues. In addition, SERC provides an ongoing interface and training for Enforcement, legal, and audit staff to allow for discussion of lessons learned and feedback to improve violation assessments and risk statements.

streamline the enforcement process and ensure that SERC has the necessary information to conduct a thorough and timely assessment. These improvements included automation of notification and letters, increased use of requests for information, seminars and outreach, simplified review steps for violation processing, continued use of streamlined enforcement processing (FFT and SNOP), and expanded capabilities for access to CIP evidence and data.

In addition to the increased focus on productivity and process improvements, SERC also has worked to implement organizational efficiencies. To this end, SERC restructured Enforcement staff after a review of other regional structures. Enforcement now reports directly to the vice president and chief program officer, which removes a redundant reporting structure and serves to elevate Enforcement in the organization, given its priority at SERC. SERC has also reviewed its staffing levels and has increased the number of Enforcement staff focused on CIP issues based on the increase in CIP possible violations reported to the region.

As a final matter, with respect to SERC's use of volunteer industry subject matter experts, during the assessment period, the Commission reviewed SERC's use of volunteer industry subject matter experts (ISMEs) on compliance audits as part of its audit of SERC (FERC Docket No. FA12-6-000). FERC found that SERC's use of ISMEs was consistent with the NERC ROP, but did recommend that SERC: (i) revise its process, procedures, and controls regarding ISME participation in compliance activities and ensure SERC has an adequate and detailed set of policies governing ISMEs' participation in compliance activities; and (ii) ensure greater awareness of SERC's ongoing training and education programs and use the feedback from ISME participation in compliance activities to better focus these outreach programs. SERC has committed to implement the recommendations contained in the FERC audit report.

227. *As of the filing date of the Performance Assessment, NERC views* ***SPP Regional Entity*** *as less effective in administering its compliance program than some other Regional Entities. NERC commends SPP Regional Entity for its ability to accurately identify high risk violations, but is concerned about SPP Regional Entity's ability to process alleged violations to completion in a timely manner and its situational awareness capabilities. NERC notes that SPP Regional Entity has been unaware of events that occurred within its footprint, while NERC and the Commission were aware of those events. NERC states that among the Regional Entities, SPP Regional Entity stands eighth in FTEs committed to the compliance program and second in the number of registered functions per compliance FTE.*

SPP RE has significantly reduced the amount of time it takes to process alleged violations to completion. Prior to January 1, 2009, SPP RE's average time to process alleged violations to completion was 24 months, compared to 9.2 months (as of June 30, 2013). The reduction is due to a number of factors, including developing internal Enforcement procedures, streamlining internal Enforcement processing procedures, and increasing the Enforcement staff.[144] SPP RE staff members have also taken several steps to increase their awareness of system events within the region. These steps include SPP RE staff's registering to receive NERC Reliability Coordinator Information System information and *NERC Alerts*, and their receiving and reviewing the *SPP RTO Daily Operations Report*, the *NERC Situational Awareness Morning*

[144] Since January 1, 2009, SPP RE has increased its Enforcement staff from one FTE to ten FTEs and one part-time employee, and has steadily decreased the number of registered functions per compliance FTE to 11.62 (2013 figure).

Report, and the NERC BPS *System Awareness Daily Report*. In addition, SPP RE participates on weekly situational awareness calls with NERC staff, and has increased its outreach through workshops, webinars, newsletters, and personal communication to encourage reporting of events.

228. *NERC rates **TRE** as an effective Regional Entity, commending TRE for focusing on identifying higher risk violations and noting that TRE excels in processing alleged violations through completion. NERC does have questions about a contrast between TRE's high percentage of "failure to perform" violations and low number of violations TRE has recommended for a non-zero dollar penalty. NERC states that it will continue to explore these concerns with TRE.*

In 2007 and 2008, Texas RE recommended zero-dollar penalties in most cases because the Reliability Standards were new and registered entities were still learning how to comply with them. In 2009, in an effort to deter noncompliance, Texas RE began recommending more non-zero dollar penalties for "failure to perform" violations. However, in 2010 Texas RE implemented the Administrative Citation NOP process and by 2012 Texas RE adopted the FFT program. Using the Administrative Citation process and FFT processes, Texas RE stopped recommending monetary penalties for issues involving "failure to perform" if the issues presented low risk to reliability and had been mitigated.

231. *NERC states that **WECC** is "one of the less effective Regional Entities" to date, but notes that WECC made significant progress in the spring of 2009, particularly with respect to processing a backlog of violations. NERC points out that although, as of the Performance Assessment filing date, WECC had the highest level of FTEs committed to the compliance program among the Regional Entities, WECC had the fourth highest ratio of registered functions to compliance FTEs. NERC notes that, due to the violations processing backlog, WECC cancelled all compliance audits scheduled for the fourth quarter of 2008 without coordinating with NERC. According to NERC, WECC also took several other unilateral actions, including issuing compliance bulletins containing Reliability Standards interpretations and/or guidance. NERC indicates that it will continue to work with WECC to resolve these issues. NERC also suggests that WECC create stronger separation between its compliance encouragement efforts and its enforcement activities, examine its staffing levels and compliance processes and stay focused on processing violations to completion. (Footnote omitted.)*

WECC has thoughtfully and thoroughly addressed each of the areas of concern identified in the Three-Year ERO Performance Assessment and the 2010 Order. First, WECC cleared all of its pre-2012 violations caseload by December 31, 2013. As reported to the NERC Board in September 2013, WECC has a caseload index of 8.3 months, ranking third among the Regional Entities.[145] Second, WECC completed all audits contemplated in its annual Implementation Plans. Specifically, during the assessment period, WECC conducted 598 audits and 62 spot checks. The number of audits increased from 90 in 2009 to 165 in 2013, an increase of 83

[145] The caseload index refers to a NERC metric that computes the number of months that it takes to clear the violations that are either in the Regional Entity's inventory, NERC's inventory, or the ERO's inventory based upon the respective average monthly processing rate over the preceding 12-month period. This metric is used to evaluate the efficiency of processing violations over time.

percent. Third, WECC developed and maintains a highly qualified Compliance staff, which increased from 31 to 57 during the assessment period. To further improve its compliance capabilities, in 2013, WECC launched an audit tracking system to assure timely audit completion and document integrity. WECC's internal metric for providing final audit reports to registered entities is 60 days after the close of the audit, a goal which was met 97 percent of the time. Fourth, WECC enhanced, streamlined and documented all of its Enforcement processes, an effort aided by using dedicated subject matter experts and tools such as FFT and expedited settlement agreements. As a result, by the end of the assessment period, WECC was able to process violations from intake through filing with NERC in less than five months, on average. Fifth, WECC successfully implemented new IT solutions and systems, and provided extensive training to registered entities on the new systems. Sixth, WECC expanded and enhanced its compliance encouragement and outreach efforts while ensuring "adequate separation between compliance encouragement efforts and its enforcement activities." This was accomplished in part by personnel changes and strengthening the role of the director of stakeholder outreach. Finally, WECC worked collaboratively with the other Regional Entities and NERC to bring forward the Omnibus proposal; proposed Rules of Procedure changes to streamline TFE processing; developed new registration system tools; and actively participated in several ongoing NERC IT projects, lending expertise and practical experience.

SPP Independence

In the 2010 Order, the Commission laid out its initial concerns about the possible conflicts of interest between SPP RE and SPP RTO, and emphasized the heavy burden on SPP RE to demonstrate a strong separation of functions between the two organizations.[146] As a consequence, the Commission had required NERC to provide an appropriate discussion of SPP RE's bylaws in its first performance assessment. In response to NERC's submission, the Commission generally found that SPP RE had achieved sufficient separation from SPP RTO, citing in particular SPP RE's efforts to ensure that its standards development process was not unduly influenced by the RTO.[147] While the Commission's analysis in the 2010 Order does not necessarily require a further response at this time, SPP RE would like to point out that the Commission's second audit of SPP RE, which was finalized in 2011, reinforced the adequacy of Regional Entity's separation from the RTO.[148] Among other things, the second audit report described how SPP RE's general manager is the primary contact between NERC and SPP RE, with responsibility for administering SPP RE's programs under the Delegation Agreement. The report also described how SPP RE is governed by three independent trustees who operate separately from the SPP RTO board of directors, and that SPP RE trustees have autonomy over decisions in fund allocation and approval of SPP RE's budget, as well as oversight of SPP RE decisions on regional Reliability Standards, compliance enforcement actions, and penalties. In addition, as the report set out, SPP RE's organizational structure makes it independent from the

[146] *See* 132 FERC ¶ 61,217 (2010), at P 232.

[147] *See id*. PP 237-241.

[148] *See generally Audit of Regional Entity Operations at Southwest Power Pool (SPP) for Compliance with its Bylaws, Delegation Agreement, Membership Agreement, and its Independence as an Regional Entity*, Final Audit Report, Delegated Order (October 5, 2011).

RTO in its performance of CMEP functions while linking with shared resources to use their expertise when performing delegated functions outside of the CMEP. Finally, the report detailed how SPP RE has reduced its reliance on shared staff and increased the number of FTEs since January 1, 2009.[149]

WECC Voting Structure

In the 2010 Order, the Commission took note of some initial concerns that NERC had regarding the effectiveness of WECC's stakeholder voting structure, but that those concerns had been largely allayed by changes to WECC's bylaws and its process for developing and approving regional Reliability Standards.[150] WECC continues to improve its regional Reliability Standards development process. For example, on March 1, 2012, the Commission approved WECC's revised RRSDP, which call for voting by eligible members of the WECC Ballot Body rather than by a lead Standing Committee of WECC. In addition, WECC has developed a web-based system for balloting, and make all the proceedings of the standards drafting teams available using WECC's website. Available information includes notification of meetings, team meeting agenda and minutes, draft and final documents and supporting documents. Finally, WECC strives for continuous improvement and is always open to feedback from the various committees, standards drafting teams, and stakeholders at large.

[149] *See id*., at pp. 5-7.

[150] *See* 132 FERC ¶ 61,217 (2010), at P 243.

Appendix C
Regional Entities' Satisfaction of Statutory and Regulatory Criteria

During the 2009 through 2014 assessment period, all eight Regional Entities continued to satisfy the three sets of criteria set out in FPA §215(e)(4), 16 U.S.C. §824o(e)(4), as reiterated in §39.8 of the Commission's regulations, 18 C.F.R. §39.8 (2013), to maintain the authority delegated to them by the ERO, as approved by the Commission, to propose and enforce mandatory Reliability Standards. The three sets of criteria are:

1. The Regional Entity is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board.

2. The Regional Entity meets the requirements otherwise applicable to the ERO in FPA §215(c)(1) and (2), 16 U.S.C. §824o(c)(1)(2), namely that it (a) has the ability to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk-power system; and (b) has established rules that (i) assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure, (ii) allocate equitably reasonable dues, fees, and other charges among end users for all activities, (iii) provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties, (iv) provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties, and (v) provide for taking appropriate steps to gain recognition in Canada and Mexico,

3. The Regional Entity operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability.

Specifically, the eight Regional Entities continued to satisfy the statutory and regulatory criteria for their delegated authority as follows:

Florida Reliability Coordinating Council, Inc. (FRCC)

1. **FRCC "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board."** The FRCC board of directors (FRCC Board) is a balanced stakeholder board. The FRCC Board has a minimum of sixteen (16) members, who are allocated among the region's six sectors, and the chief executive officer (CEO). The sector representation is as follows: (i) three directors from the Suppliers Sector; (ii) two directors from the Non-Investor Owned Utility Wholesale Sector; (iii) two directors from the Load Serving Entity Sector (one Municipal and one Cooperative); (iv) three directors from the Generating Load Serving Entity Sector; (v) three directors from the Investor Owned Utility Sector; and (vi) two directors from the General Sector. FRCC's CEO is an ex-officio non-voting director. Directors are elected by their sector and serve two-year terms.

2. **FRCC meets the requirements of Federal Power Act Section 215 (c)(1)(2), because**:
   a. **FRCC is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system**. The FRCC has a RRSDP that is based on the set of common attributes that provide for an open, balanced, fair, transparent and inclusive process. During the assessment period, FRCC placed two standards development projects on hold awaiting the completion of NERC standards development projects, and terminated one project as NERC's continent-wide standard was determined to be sufficient for FRCC reliability needs. Finally, the FRCC Registered Ballot Body and FRCC Board approved one project, which was nevertheless held in abeyance while the adequacy of the NERC continent-wide standard was evaluated, and will be withdrawn if the NERC Reliability Standard is determined to be sufficient for FRCC's needs. FRCC prefers the development of continent-wide standards, but will follow its RRSDP should a need arise for a more stringent standard or a standard to cover an area that NERC standards do not.

      Compliance monitoring and enforcement of Reliability Standards is carried out by FRCC compliance staff which grew during the assessment period. FRCC enforcement staff began reporting directly to the vice president and executive director of standards and compliance in 2012, while the monitoring staff continued to report to the director of compliance. FRCC implemented this separation to provide more independence in enforcement decisions.

      FRCC took additional steps to enforce reliability standards and provide an adequate level of reliability for the BPS. For example, its Compliance staff developed approximately 30 detailed internal procedures for all aspects of the compliance process, which were regularly reviewed and updated. These procedures helped promote consistent and effective application of its internal procedures and ensured that it met the obligations in the NERC ROP. In addition, FRCC upgraded its compliance portal application in 2012, to provide needed enhancements to protect security of the application and data held within the application along with providing some desired improvements in the use of many of its components.

      FRCC improved its enforcement caseload processing during the assessment period, and also experienced a reduction of new violations in the last two years of that period. FRCC attributes the reduction in new violations in part to increased understanding of the registered entities in what the requirements mean and what their compliance expectations are. In addition to this reduction, FRCC worked hard to streamline its enforcement activities to utilize the available processes and were able to reduce its caseload index to approximately 6.5.

   b. **FRCC has established rules that:**
      i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure.** During the assessment period, FRCC implemented an annual employee recital and disclosures, which

includes a copy of the *FRCC Conflict of Interest Policy* and a process where each employee signs a *Conflict of Interest Questionnaire*, a *Disclosure Statement of Stock Ownership of FRCC Member Companies* and a *Non-Disclosure Acknowledgement*. As previously described, the governance of the FRCC is performed by a balanced stakeholder board, which assures fair stakeholder representation while also practicing balanced decision making where no one sector can block or no two sectors can pass any decision.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities.** The funding for the FRCC Regional Entity division is allocated among the FRCC load serving entities (LSEs) through a formula which is based on NEL. Each entity reports, on an annual basis, the NEL for the previous year. After the FRCC reviews this information, it is provided to NERC as part of the business plan and budget development process. The FRCC develops an annual budget each year, which is based on common assumptions that have been developed collaboratively by NERC and the eight Regional Entities, and which provides for the resources to carry out all of its delegated functions. The budget and accompanying LSE assessments are approved by the FRCC Board, the NERC Board, and the Commission.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties**. The FRCC has adopted the NERC CMEP, Appendix 4C to the NERC ROP. This is the primary document that the FRCC uses to provide fair and impartial procedures for enforcement. With respect to the calculation of penalties, the FRCC consistently uses the penalty calculator tool provided by NERC in order to provide a consistent application of the penalty and sanctions guidelines. In addition, the FRCC Board and their alternates are required to sign a *Code of Conduct* that obligates each of them to act in the best interest of FRCC and refrain from involvement in any situation where there is an actual or potential conflict of interest. In addition, since the FRCC Board is a balanced stakeholder board, FRCC does not allow members of the board to participate directly in settlement discussions with FRCC on behalf of their registered entities to avoid any conflict of interest or undue influence situation.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties**. FRCC has a RRSDP that is based on the required set of common attributes that provide for an open, balanced, fair, transparent and inclusive process. The process has the following characteristics:

- Due Process – Any entity that is directly and materially affected by the reliability of the FRCC BPS has a right to participate in this process.

- Openness – Participation is open to any entity that is directly and materially affected by the reliability of the FRCC BPS. Participation is not conditional upon membership in the FRCC. All FRCC RRSDP meetings will be open and noticed on the FRCC website.

- Balance – The FRCC RRSDP process shall have a balance of interests and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter.

The FRCC also provides reasonable notice and opportunity for public comment in its compliance monitoring and enforcement activities as required by the CMEP and the NERC ROP.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico**. This criterion is not applicable to the FRCC region.

3. **FRCC operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. On June 12, 2012, the Commission approved the amended and restated FRCC Delegation Agreement which incorporated benefits of NERC's and FRCC's mutual experience and lessons learned while operating under the predecessor agreement. The revised Delegation Agreement provides for more efficient and effective execution of responsibilities that promote the reliability of the BES. These responsibilities include: (i) development and proposal of Reliability Standards; (ii) enforcement of compliance with Reliability Standards; (iii) certification of BPS entities; (iv) registration of owners, operators, and users of the BPS; (v) reliability assessment and performance analysis; (vi) event analysis and reliability improvement; (vii) training and education; and (viii) situation awareness and infrastructure security.

Midwest Reliability Organization (MRO)

(1) **MRO "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board.**" During most of the assessment period, MRO was governed by a balanced stakeholder board. On June 25, 2012, the Commission approved MRO's proposal to change from a balanced stakeholder board to a combination independent and balanced stakeholder board. MRO's two independent board members were elected for terms beginning January 2013; they bring cyber and data security expertise to the MRO Board's set of executive and technical skills and expertise.

(2) **MRO meets the requirements of Section 215 (c)(1)(2) of the Federal Power Act, because**:

a. MRO is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system. MRO supports the development of continent-wide standards to maintain the reliable operations of the BES as opposed to regional Reliability Standards, particularly in the Eastern Interconnection, and decided during the assessment period to forego the development of regional

standards. Nevertheless, MRO has a RRSDP manual, which is found in Exhibit C to its Delegation Agreement with NERC, and a stakeholder Standards Committee comprised of subject matter experts in the event there was a need for a regional Reliability Standard in the future.

MRO also has the requisite staff both in terms of number of people and expertise, and adequate processes and procedures, to enforce the operating and CIP Reliability Standards. Notably, during the assessment period, MRO split the CMEP function into three distinct steps with their own assigned personnel— (i) Compliance Monitoring, (ii) Risk Assessment and Mitigation, and (iii) Enforcement. Compliance monitoring staff conducts audits and spot checks of compliance with reliability standards by registered entities. Risk Assessment and Mitigation undertakes an independent review of the facts and circumstances that surround each violation discovered by Compliance Monitoring, and determines whether sufficient evidence supports each possible violation. Risk Assessment and Mitigation also works with the registered entity to develop an effective and comprehensive mitigation plan in the event that a violation is confirmed. Confirmed violations move to the Enforcement department staff, who review recommendations made by Risk Assessment and Mitigation staff, verify all relevant facts, and evaluate appropriate enforcement actions.

The factual review conducted by Risk Assessment and Mitigation and Enforcement staff is intended to ensure a consistent, accurate application of the NERC reliability standards. The three-step process also provides for segregation of duties, establishing independence among those making the findings, those assessing risk, and those determining and negotiating penalties and sanctions. As a result of this approach, registered entities in the MRO region accept responsibility in 90% of all violations and settlements are reserved only for the more complicated compliance matters (thus, expediting less serious violations and lowering administrative costs).

b. MRO has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure.** In particular, MRO assures the independence of the users and owners and operators of the BPS by establishing processes and procedures for the conduct of its work. For example, by having a three-step process to implement the CMEP, MRO assures that its internal work is subjected to review and validation. MRO also has specific policies that prevent stakeholder conflicts of interest and prevent stakeholders from participating in its CMEP work. In addition, all MRO members elect the two independent directors; the remaining directors are elected by his or her sector.

ii. Allocate equitably reasonable dues, fees, and other charges among end users for all activities. MRO's funding requirements are equitably allocated in a manner similar to the one used by the other Regional Entities. Each year,

MRO develops an annual business plan and budget that describes in detail the resources MRO needs to carry out its delegated functions. The annual business plan and budget is reviewed and approved by the MRO Board and then submitted to NERC and ultimately filed with the Commission for approval. Assessments are made to MRO's LSEs through a formula which is based on NEL. MRO does not charge additional fees to be a member or to participate in its training. The annual business plan and budget as well as annual audits by independent auditors and periodic audits by FERC help ensure that MRO's expenses and assessments to end users are reasonable.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties**. To ensure fair and impartial procedures, as described above, MRO has implemented a three-step approach to fulfill its delegated responsibilities under the CMEP. MRO Compliance Monitoring staff conducts compliance monitoring activities, including audits, self-certifications, and spot checks. Risk and Mitigation staff is responsible for scoping MRO's compliance monitoring work under RAI. Risk and Mitigation staff also works with the entity to develop a thorough, comprehensive, and effective mitigation plan, not only to resolve the concern but to prevent recurrence of the noncompliance. MRO Enforcement staff completes the process by reviewing any recommendations from MRO Risk Assessment and Mitigation staff, verifying that all relevant facts have been gathered, and evaluating the possible violation for the appropriate enforcement action.

There are many factors which may affect a penalty determination. MRO does not utilize the penalty calculator/SIV tool for most minimal risk concerns, as those violations are currently resolved through the FFT process and under RAI, they will be primarily resolved as compliance exceptions outside the enforcement process. The penalty calculator/SIV tool is used as a resource for violations that pose greater risk. As a result of the extensive risk assessment conducted by MRO Risk Assessment and Mitigation staff, Enforcement is able to make fair, accurate and reasonable enforcement decisions scaled on the risk posed by an individual violation – the greater the risk, the greater the penalty and scrutiny of review and approval.

In addition MRO has policies and procedures to avoid conflicts of interest in its CMEP work. Those policies and procedures provide:

(1) No MRO director or member of MRO committees may participate in any way in compliance violation investigations, compliance audits, reports, sanction determinations, or other matters within the CMEP.

(2) An MRO director or member of an MRO committee may engage in actions on behalf of his or her employer regarding a compliance monitoring and enforcement matter undertaken by MRO; however,

that director or member of an MRO committee must recuse himself or herself from any board or committee decisions, meetings, and actions related to that compliance monitoring and enforcement matter. Potential concerns about the participation of a MRO director or member of an MRO committee are brought to the attention of the president and CEO who will seek an appropriate resolution of the matter with the advice and counsel of the independent directors.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties**. MRO does not have any regional Reliability Standards and does not anticipate developing any regional Reliability Standards because of its strong support for continent wide, or at least interconnection wide, standards. Nevertheless, MRO has a RRSDP manual which has been approved by NERC and FERC. This RRSDP manual is based on the set of common attributes that provide for an open, balanced, fair, transparent and inclusive process, and includes specific provisions relating to the process for the opportunity to comment and be heard.

v. **Provide for taking appropriate steps to gain recognition in Canada**. MRO operates under provincial Manitoba regulations which were adopted in 2012. Prior to the adoption of regulations, MRO had a memorandum of understanding with Manitoba Hydro.

During the assessment period, MRO also had a memorandum of understanding with Saskatchewan Power Corporation and NERC governing MRO's work in Saskatchewan, Canada.

(3) **MRO operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. MRO has adopted principles associated with the theory of a "Highly Reliable" organization in its approach to its delegated responsibilities, an approach that has positioned MRO and its registered entities to move to the risk based approach contemplated by RAI. These principles recognize risk, and emphasize self-monitoring with strong corrective action programs. The approach has fostered greater engagement with registered entities to solve technical problems and resulted in a corporate theme—clarity, assurance, and results (CAR). Clarity sets clear expectations for registered entities on the technical requirements of the standards. Assurance measures performance against these key requisites. Results can be seen in improved reliability. For example, MRO leveraged the technical expertise of subject matter experts on stakeholder-led committees to develop application guides for NERC standards that provide clear expectations of compliance. While these application guides are not authoritative, they provide much needed direction on compliance requirements. As a result, MRO has seen a measurable drop in the frequency and severity levels of violations in higher risk standards, beginning with the most violated Reliability Standard several years ago, PRC-005.

Additionally, during the assessment period, an MRO stakeholder-led committee developed an internal controls and procedures framework for use by registered entities to strengthen their internal compliance programs. These types of guidelines provide the necessary clarity to industry to assure that key reliability requirements are met. This has now become part of a pilot project under RAI.

Registered entities, too, need to provide assurance to MRO staff that they understand the requirements and have established sustainable management practices to detect, correct, report, and prevent problems. For example, MRO staff sampled self-reported violations from 2013. In 90% of these violations, the registered entity's assessment of risk matched MRO's staff assessment of risk. When registered entities and MRO staff view risk the same way and accept responsibility, they have greater day-to-day, sustainable assurance.

Northeast Power Coordinating Council, Inc. (NPCC)

1. **NPCC "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board."** On October 17, 2011, the Commission approved NPCC's proposal to change its board to a hybrid (combination independent and balanced stakeholder) board. That change became effective on January 1, 2012. NPCC's board of directors consists of seven stakeholder voting sectors that each consist of a maximum of two directors per sector, an independent sector consisting of two independent directors, an independent board chair with voting rights to preclude board deadlocks, and the president and CEO. Within NPCC, no two sectors can control and no one sector can block action.

2. **NPCC meets the requirements of Section 215(c)(1)(2) of the Federal Power Act, because:**
    a. **NPCC is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system.** NPCC has developed a RRSDP that provides the design-basis approach to a consensus building process by which NPCC may develop regional Reliability Standards and regional variances to be proposed to the ERO for adoption, under delegated authority by the FERC and the Canadian provincial regulatory and/or governmental authorities. This procedure contains common attributes that provide for an adequate level of reliability to provide for an open, balanced, fair, transparent, and inclusive standards development process. NPCC's RRSDP sets forth the structure for developing reliability standards that provide for an adequate level of reliability.

    Illustratively, during the assessment period, NPCC developed a disturbance monitoring regional Reliability Standard, PRC-002-NPCC-01, to ensure that adequate disturbance data is available to facilitate BES event analyses. The Reliability Standard addresses a specific recommendation from the *August 14, 2003 Blackout Final NERC Report - Conclusions and Recommendations* (July 13, 2004) regarding the use of time-synchronized data recorders.[151] Substantively, the Reliability Standard outlines the basic requirements for the type, location and capability of

[151] *See* http://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx.

equipment to be placed on the power system to enable the analysis of grid disturbances effectively and efficiently. The Reliability Standard is intended to fill the reliability gap related to disturbance monitoring and reporting by establishing enforceable disturbance monitoring and reporting requirements for the NPCC region.

Compliance and enforcement activities are carried out by the NPCC compliance staff and are independent of all users, owners and operators of the international BPS and from the hearing officer. Compliance and enforcement activities are governed in the U.S. by the Delegation Agreement between NERC and NPCC, delegating portions of NERC's authority as the ERO to NPCC. In addition, pursuant to an agreement between NPCC and WECC that was approved by the Commission, NPCC assumed responsibility for the CMEP with respect to the WECC RC function and the WECC IA function from January 1, 2012 through the end of the assessment period.

Examples of NPCC's efforts to monitor compliance with, and enforcement of, the reliability standards include its use of extensive pre-audit data collection and pre-audit conference calls with the registered entities. NPCC staff thoroughly reviews the first round of data submittals, and via questions, routinely collects a second round of data from the registered entity before the audit is performed. From these pre-audit activities, NPCC is able to conduct a more targeted audit. This results in an efficient and effective audit for both NPCC and the registered entity. This efficiency also permits the auditors to drill down into other areas and to make recommendations to the registered entity for enhanced reliability performance. In addition, during the assessment period, developed an enforcement dashboard, highlighting the regional caseload index and the status of mitigation plans associated with high risk violations among other compliance parameters. The enforcement dashboard is an informational tool to both management and to the industry.

NPCC amended its hearing procedures to provide for a hearing body comprised of an independent hearing officer and two independent directors. As a result of the amendments, the hearing body will always be comprised of independent members and will not have stakeholder members to assure enforcement of reliability standards provides for an adequate level of reliability.

b. NPCC has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure**. The rules and procedures contained in the Delegation Agreement, ROP, amended and restated NPCC bylaws, and other NPCC committee governance documents assure the independence of the users and owners and operators of the BPS while assuring fair stakeholder representation and balanced decision-making at the same time. Fair stakeholder representation and participation is assured by NPCC's committees, subcommittees, task forces and other groups as the board of directors may deem appropriate. Industry technical experts from

within the membership also provide valuable input to the board through various working groups and task forces as well as the committees.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities.** The allocation of dues, fees, and other charges by NPCC is governed by Article XIII of its bylaws. Funding of Regional Entity division activities are undertaken pursuant to FPA §215 in accordance with the funding provisions and procedures of that law and related FERC regulations and orders. The NPCC board of directors approves the annual Business plan and Budget in time for submission to the ERO and to FERC for approval. NPCC funds reliability activities in Canadian provinces pursuant to the mechanisms established by the applicable Canadian provincial regulatory authority. Budgets for the costs of reliability activities are allocated equitably based on the NEL and other relevant factors consistent with applicable law, the Delegation Agreement, and any agreements with Canadian provincial authorities. NPCC members are not assessed an annual membership fee. For NPCC's Criteria Services division, which establish and monitor regional-specific non-statutory criteria, full members that perform the balancing authority function are assessed and pay based upon a NEL. Special assessments for Criteria Services may be separately budgeted to full members that perform the balancing authority function or upon Full Members with full members' consent.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties**. The NERC ROP is the primary document that NPCC uses to provide fair and impartial procedures for enforcement. Additionally, NPCC has in place *Conflict of Interest Guidelines* that require each NPCC director, officer, and employee to avoid and refrain from involvement in situation where there is an actual conflict of interest, disclose any actual or potential conflicts of interest that may arise, recuse himself or herself from participation in any action involving an actual or potential conflict of interest, and refrain from voting on any actions where there is an actual or potential conflict of interest. In addition, NPCC's *Code of Conduct*, which applies to its officers, board of directors, employees, and all participants of NPCC committees, task forces, and working groups, requires each individual to recognize conflicts of interest that may arise and to take steps to disclose such conflicts of interest and to refrain from voting and/or influencing others with respect to such conflicts of interest. With respect to penalties, NPCC consistently uses the penalty calculator tool for consistency in penalty calculation determinations

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties**. NPCC follows a RRSDP that provides that participation in the development of a regional Reliability Standard shall be open to all organizations that are directly and materially

affected by the NPCC BPS reliability, that there shall be no undue financial barriers to participation, that participation shall not be conditioned upon membership in NPCC or unreasonably restricted on the basis of technical qualifications or other such requirements. Meetings of drafting teams are open to the NPCC members and others.

Compliance and enforcement activities are carried out by the NPCC compliance staff and are independent of all users, owners and operators of the international BPS and from the hearing officer. Compliance and enforcement activities are governed in the U.S. by the Delegation Agreement between NERC and NPCC, delegating portions of NERC's authority as the ERO to NPCC. NPCC's hearing procedures provide for a hearing body comprised of an independent hearing officer and two independent directors.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico**. NPCC has MOUs in place with the Northeastern Canadian provinces (New Brunswick, Nova Scotia, Ontario, and Quebec). At the end of the assessment period, NPCC was in the process of updating and revising MOUs to respond to recent Canadian legislative and regulatory changes and initiatives.

3. **NPCC operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. Effective January 1, 2012, NPCC executed an amended and restated Delegation Agreement, which delegated to NPCC certain activities pursuant to FPA §215. These delegated activities include certification of BPS Entities, registration of owners, operators, and users of the BPS as responsible for compliance with requirements of Reliability Standards, developing assessments of the reliability of the BPS, developing and maintaining, and collecting data in support of the development and maintenance of, reliability performance metrics and assessments of risks to the reliable operation of the BPS, conducting and coordinating event analysis, providing training and education to registered entities, and gathering and assessing situation awareness information. NERC has also delegated NPCC the authority to propose Reliability Standards, regional variances, or modifications thereof to NERC and to develop regional Reliability Standards. In summary, the Delegation Agreement promotes the effective and efficient administration of the BPS by clearly identifying the delegation of authority provided to NPCC.

ReliabilityFirst Corporation (RF)

1. **RF "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board**." RF is governed by a combination independent and balanced stakeholder board, which consists of 14 directors: (i) three are independent directors; (ii) three are at-large directors elected by all the industry sectors voting together as a single class; and (iii) eight are elected by their industry sectors (suppliers elect two directors, transmission companies elect two directors, RTOs elect one

director, small LSEs elect one director, medium LSEs elect one director, and large LSEs elect one director).

2. **RF met the requirements of Section 215 (c)(1) (2) of the Federal Power Act, because**:
   a. **RF is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system**. Although RF no longer develops regional Reliability Standards in order to avoid duplication with the NERC continent-wide Reliability Standards, RF has adopted a RRSDP, and has otherwise proved its ability to develop regional Reliability Standards, as illustrated by its development of RF's BAL-502-RFC-02 (Planning Resource Adequacy Analysis, Assessment and Documentation), which was approved by the Commission on March 17, 2011.

      RF has sufficient staff with the requisite expertise to conduct compliance audits, investigations, spot checks, and other compliance reviews, and to enforce Reliability Standards as demonstrated in part by its performing over 290 audits and over 200 spot checks during the assessment period, and ensuring the mitigation of over 1,400 alleged violations of those standards. These enforcement activities have resulted in tangible improvements to the reliability of the BPS. To enhance its risk-determination process in enforcement, RF developed a "Risk-Harm" process which, among other things, provided for technical experts to answer a series of questions about the risk and harm posed by each violation using a common scale to ascertain a quantified risk assessment for each violation. Additionally, for serious violations of the NERC Reliability Standards, RF works with registered entities to implement substantial "above and beyond" activities to enhance reliability on their system and on the BPS.

   b. **RF has established rules that**:
      i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure.** As described earlier, RF is governed by a combination independent and balanced stakeholder board. Pursuant to RF's bylaws, no two industry sectors can control any RF decision and no single industry sector can veto any RF decision. This hybrid board structure assures RF's independence, while still assuring fair stakeholder representation and balanced decision-making. To further assure RF's independence of the users, owners and operators of the BPS, RF has the following protections in place:

         - First, RF adopted the NERC CMEP, Appendix 4C to the NERC ROP, which provides fair and impartial procedures for the monitoring and enforcement of Reliability Standards.

         - Second, all RF employees and contractors sign and must adhere to non-disclosure and confidentiality agreements and conflict of

interest forms, and RF employees, contractors, and directors are governed by the RF *Conflict of Interest Policy*, the RF *Code of Business Conduct and Ethics*, and §1500 of the NERC ROP.

- Third, to ensure the independence of its staff and eliminate any potential conflicts of interest, RF does not allow stakeholder participation in its compliance or enforcement activities (i.e., a registered entity staff member may not be on an RF audit or compliance investigation team).

- Fourth, RF does not allow its industry sector directors to participate in settlement discussions with RF on behalf of their registered entity.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities**. The funding for RF's activities is equitably allocated among its end users and recovered through a formula based on NEL. Each year, RF develops an annual business plan and budget, which describes the adequate resources needed for RF to carry out its delegated functions. The annual business plan and budget and the assessments to the end users must be approved by the Commission. The annual business plan and budget process, the Commission's approval of the assessments, and periodic financial audits by the Commission all ensure that RF's expenses and assessments to end users are reasonable.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties.** RF has adopted the NERC CMEP, Appendix 4C to the NERC ROP, which provides fair and impartial procedures for the enforcement of Reliability Standards within RFC's geographic boundaries. Additionally, RF maintains the RF *Conflict of Interest Policy* and the RF *Code of Business Conduct and Ethics* to ensure the integrity and independence of its compliance and enforcement staff. To assess fair, impartial, and consistent penalties, RF follows the *Sanction Guidelines*, as set out in ROP Appendix 4B.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties.** Although RF no longer develops regional Reliability Standards, RF's RRSDP provides for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in the development of Reliability Standards.

The RRSDP includes public notice and a comment period for any proposed standard, due consideration of those public comments, and a ballot of interested stakeholders. Participation in the standards development process is open to all entities that are directly and materially affected by reliability in the

RF region, and there are no undue financial barriers to participation. The standards development process is balanced: it may not be dominated by any two interest categories, and no single interest category shall be able to defeat a matter.

RF provides for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in its CMEP activities. A registered entity has the right to receive notice when it is placed on the NCR, and may appeal their registration to NERC and to the Commission.

The CMEP requires RF to provide notice to a registered entity when it determines that the registered entity has violated a Reliability Standard, and the registered entity has an opportunity to respond. If a registered entity wishes to contest an alleged violation of a Reliability Standard or a penalty, it may request and receive a hearing, and may appeal the hearing decision to NERC. A registered entity also has the right to request a hearing to contest a twice-rejected mitigation plan or a remedial action directive.

At the conclusion of an enforcement matter, NERC publicly files a NOP with the Commission, which promotes openness and the opportunity for public comment. The ERO balances the interest in openness with the concern for the security of critical infrastructure information, and as such, all sensitive critical infrastructure information is redacted from all public NOP filings.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico.** This criterion is not applicable to RF, as its geographic boundaries do not include any portion of Canada or Mexico.

3. **RF operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. Effective January 1, 2011, RF executed an amended and restated regional Delegation Agreement with NERC, which delegated to RF certain activities pursuant to FPA §215. These delegated activities include: (i) certification of BPS entities; (ii) registration of owners, operators, and users of the BPS responsible for compliance with the requirements of Reliability Standards; (iii) reliability assessment and performance analysis; (iv) event analysis and reliability improvement; (v) training and education; (vi) situational awareness and infrastructure security; (vii) the development and proposal of Reliability Standards to NERC; (viii) monitoring of compliance with Reliability Standards; and (ix) enforcement of compliance with Reliability Standards. These delegated activities are necessary for the effective administration of BPS reliability. RF only performs those activities delegated to it under the Delegation Agreement. This ensures that RF is not distracted by any other activities, and in turn promotes the efficiency and effectiveness of the corporation's efforts to improve reliability.

SERC Reliability Corporation (SERC)

1. **SERC "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board**." SERC is governed by a balanced stakeholder board. Stakeholders are classified by the SERC Board Executive Committee in one of seven sectors (investor-owned utility sector, federal/state sector, cooperative sector, municipal sector, marketer sector, merchant electricity generator sector, and ISO-RTO sector). SERC's bylaws establish voting rules that ensure that no two sectors are able to approve a decision and that no one sector can veto a decision.

2. **SERC met the requirements of Section 215 (c)(1)(2) of the Federal Power Act, because**:
   a. **SERC is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system**.

      Standards: The SERC RRSDP defines the process for the development, revision, reaffirmation, and withdrawal of regional Reliability Standards. The SERC RRSDP requires any proposed regional Reliability Standard to be more stringent than a continent-wide Reliability Standard, whether the regional Reliability Standard addresses matters that the continent-wide Reliability Standard does not or the regional Reliability Standard is necessitated by a physical difference in the BPS within the SERC region. SERC regional Reliability Standards are required to provide for as much uniformity as possible with continent-wide reliability standards. Proposed SERC regional reliability standards are subject to approval by NERC and FERC prior to becoming mandatory and enforceable within the SERC region.

      SERC has one FERC-approved regional Reliability Standard, PRC-006-SERC-01, which addresses automatic underfrequency load shedding requirements. SERC currently is not developing any additional Regional Reliability Standards because the continent-wide NERC Reliability Standards are presently adequate for the SERC region. SERC also participates in the NERC Standards Committee, hosts biannual meetings of the SERC Standards Committee, and hosts specific commenting sessions for NERC Standards Projects as NERC requests comments, all of which involve the discussion of proposed changes to NERC Reliability Standards.

      Compliance: SERC's authority to monitor reliability standards is based on the authority granted in its Delegation Agreement with NERC. SERC has the expertise on staff to conduct compliance audits, investigations, spot checks and other compliance reviews for the Operating, Planning, and CIP Reliability Standards. SERC develops and posts an annual CMEP implementation plan that is complementary to the NERC CMEP, but also addresses reliability issues specific to the SERC region. SERC builds upon the NERC actively monitored list and incorporates additional Standards or Requirements that relate to the SERC region's BES. SERC utilizes off-site and on-site audits, spot checks, and other compliance monitoring methods to assess registered entity compliance with NERC Reliability Standards. Compliance prepares detailed reports on each audit and makes

recommendations to Enforcement about possible violations of NERC Reliability Standards.

Enforcement: Over the past five years, SERC has demonstrated its ability to enforce Reliability Standards by processing approximately 800 alleged violations originating from audits, spot checks, self-certifications, complaints, self-reports, and compliance investigations following the requirements of the CMEP and NERC ROP. Enforcement staff conducts a thorough assessment of all possible violations to determine whether there is a sufficient basis to allege a violation. If a sufficient basis exists, Enforcement staff determines the complete scope of the violation and the actual and potential risk to the reliability of the BPS. Enforcement staff reviews the registered entity's mitigating activities to ensure that the entity corrects the noncompliance and prevents recurrence. Enforcement staff also participates in settlement negotiations with the registered entity. If a registered entity challenges the findings of the violation and/or penalty, Enforcement staff would prosecute the case before the Board Compliance Committee, which acts as SERC's hearing body. SERC's processing of possible violations has improved because of increased resources and improved tools such as FFT and the SNOP filing mechanisms.

b. SERC has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure**. SERC's bylaws allow each SERC member company to appoint a director to SERC's board. The SERC Board Executive Committee is made up of 12 sector representatives from among the directors. All directors, alternate directors, and board committee representatives are required to comply with SERC's standards of conduct policy that prohibits participation in decisions that could pose a conflict of interest.

SERC's bylaws establish voting rules that ensure that no two sectors are able to approve a decision and that no one sector can veto a decision. These voting rules assure SERC's independence of the users, owners, and operators of the BPS. In addition, SERC has adopted the NERC CMEP, Appendix 4C to the NERC ROP, which provides fair and impartial procedures for the monitoring and enforcement of Reliability Standards. In addition, SERC employees and contractors sign non-disclosure and confidentiality agreements and conflict of interest forms.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities**. SERC develops a budget annually that will accomplish all delegated duties. The budget is reviewed and approved by SERC's board before going to NERC and FERC. The budget is paid by all registered entities based on their proportionate share, based on the NEL. Pursuant to §202 of the NERC ROP, NEL is the 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. Each entity reports the energy generated on an annual basis for the previous year. After verification by SERC, this data is provided to NERC. NERC produces an allocation of the budgets to each appropriate region.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties**. SERC has adopted without exception the NERC CMEP, Appendix 4C to the NERC ROP, and the associated *Sanction Guidelines*, ROP Appendix 4B, which provide fair and impartial procedures for the enforcement of Reliability Standards within the SERC region. SERC maintains a *Conflict of Interest Policy* to ensure the integrity and independence of its compliance and enforcement staff. To ensure consistency and remain fair, unbiased and balanced in assessing penalties, SERC follows the *Sanction Guideline*s of NERC, utilizes the NERC penalty tool to develop a proposed penalty, and compares the proposed penalty with similarly situated violations that have been filed with and approved by FERC. All proposed penalties are reviewed and approved by a technical peer group, legal counsel, the director of enforcement, and the SERC CEO or vice president.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and other exercising its duties**. The SERC RRSDP requires SERC to provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in development reliability standards.

SERC provides for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in its CMEP activities. A registered entity has the right to receive notice when it is placed on the NCR, and may appeal its registration to NERC and to the Commission.

The CMEP requires SERC to provide notice to a registered entity when it determines that the Registered Entity has violated a Reliability Standard, and the registered entity has an opportunity to respond. If a registered entity wishes to contest an alleged violation of a Reliability Standard or a penalty, it may request and receive a hearing, and may appeal the hearing decision to NERC. A registered entity also has the right to request a hearing to contest a twice-rejected mitigation plan or a remedial action directive.

At the conclusion of an enforcement matter, NERC publicly files a NOP with the Commission, which promotes openness and the opportunity for public comment. The ERO balances the interest in openness with the concern for the

security of critical infrastructure information, and as such, all sensitive critical infrastructure information is redacted from all public NOP filings.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico**. The SERC region does not extend into any part of Canada or Mexico. Thus SERC has no need to establish rules that provide for taking appropriate steps to gain recognition in Canada or Mexico.

3. **SERC operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. On January 1, 2011, SERC executed an amended and restated regional Delegation Agreement with NERC, which delegated to SERC certain activities pursuant to FPA §215. FERC approved this Delegation Agreement on June 12, 2012. These delegated activities include: (i) certification of BPS entities; (ii) registration of owners, operators, and users of the BPS responsible for compliance with the requirements of Reliability Standards; (iii) reliability assessment and performance analysis; (iv) event analysis and reliability improvement; (v) training and education; (vi) situational awareness and infrastructure security; (vii) the development and proposal of Reliability Standards to NERC; (viii) monitoring of compliance with Reliability Standards; and (ix) enforcement of compliance with Reliability Standards. These delegated activities are necessary for the effective administration of BPS reliability. SERC only performs those activities delegated to it under the Delegation Agreement.

Southwest Power Pool Regional Entity (SPP RE)

1. **SPP RE "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board**." SPP RE is governed by three independent Regional Entity trustees. These trustees have autonomy over decisions in fund allocation and SPP RE budget approval, as well as oversight of SPP RE decisions on regional standards, compliance enforcement actions, and penalties. SPP RE's general manager reports directly to the SPP RE trustees. Only the trustees and certain SPP RE staff members have authority to make compliance and enforcement decisions.

2. **SPP RE met the requirements of Section 215 (c)(1)(2) of the Federal Power Act, because:**
   a. **SPP RE is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system**. SPP RE is not actively developing any reliability standards at this time; however, it does have a RRSDP if the need for such standards were to arise.[152] The RRSDP allows for a fair and open process for adoption, approval, revision, reaffirmation, and deletion of a regional Reliability Standard. Due process is the key to ensuring that the Reliability Standards are developed in an environment that is equitable, accessible and responsive to the requirements of all interested and affected parties. SPP RE supports development of continent-wide

[152] *SPP RE Regional Reliability Standards Development Process Manual* (SPP RRSDP Manual), version 0 became effective October 2, 2007. A petition, in Docket No. RR14-1-000, to update the SPP RRSDP manual was filed by NERC with FERC on December 20, 2013. A 10-day comment period ended on January 10, 2014 with no comments being received.

Reliability Standards at NERC and any regional Reliability Standard developed by SPP RE will go beyond, add detail to, or cover matters not addressed in the NERC Reliability Standards.

Moreover, SPP RE is able to enforce reliability standards by the implementation of the CMEP. Illustratively, during the assessment period, SPP RE experienced a dramatic reduction in the average time to process violations to completion, a dramatic increase of self-reported violations, a dramatic reduction in average time for issuance of final on-site compliance audit reports, and a dramatic reduction in average time for issuance of a notice of possible violation (NPV). Specifically, prior to January 1, 2009, SPP RE's average time to process alleged violations to completion was 24 months, compared to 9.2 months during 2013. In 2009, only 3.1 % of incoming possible violations came from either self-reports or self-certifications, compared to 68.4% in 2013. In 2008, the average time to issue a final on-site compliance audit report to registered entities was 152 days, compared to 54 days during 2013. Prior to January 1, 2009, the average days for SPP RE to issue an NPV was 20.5 days, compared to 3.6 days in 2013.

b. SPP RE has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure**. SPP is governed by an independent board of directors and has an extensive organizational group structure comprised of stakeholders that represent the membership's diversity. SPP's bylaws provide for fair stakeholder representation and balanced decision-making. SPP RE does not have a separate committee structure or bylaws; however, it is an independent unit of SPP. and reports to its Regional Entity Trustees (SPP RE Trustees). In addition, SPP RE's employees are subject to standards of conduct, its employees and contractors are screened for conflicts of interest, and its compliance monitoring teams must agree to maintain strictly the confidentiality of their auditing efforts.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities**. SPP RE follows the common assumptions developed by NERC and the Regional Entities to guide its budget projections. As such, SPP RE allocates projected statutory costs to end users via an annual assessment fee based on the SPP RE's registered entity's NEL. At the end of each budget cycle, a reserve balance is determined by taking the difference between the monies collected from end users through the assessment fee and the statutory costs incurred. This reserve balance is then used to offset the next year's funding requirement in addition to any penalty monies received during a twelve-month period. The annual assessment fee is adjusted at the beginning of each budget year (January 1).

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties**. The following, generally

describes the steps the SPP RE enforcement attorneys follow for penalty determinations, which are outlined in SPP RE's internal processes and procedures:

Step 1: Utilizing the NERC penalty determination framework tool (Penalty Tool), the enforcement attorney determines a suggested penalty amount for the violation. Note: Although not procedurally codified, once the SPP RE enforcement attorney member has calculated a preliminary penalty via the Penalty Tool, the enforcement attorney compares the proposed penalty (when possible) with similarly situated previous violations that have been filed and subsequently approved by FERC. Furthermore, enforcement attorneys implement guidance from *Sanction Guidelines*, ROP Appendix 4B, the NERC CMEP, ROP Appendix 4C, and FERC orders as to how the enforcement attorneys should assess factors such as load loss and repeat/similar/affiliate violation history.

Step 2: The enforcement attorney submits its proposed penalty amount, the Penalty Tool, notice(s) of alleged violation and proposed penalty or sanction and/or settlement documents, and any other information relevant to the proposed penalty to the sanctions review team (SRT), which consists of the SPP RE general manager, the manager of enforcement, and the director of compliance.

Step 3: The SRT reviews the information presented by the enforcement attorney and collectively either approves the proposed penalty amount or determines the appropriate penalty amount for the violation or violations. **Note:** Penalties in excess of $250,000 are required by procedure to receive additional approval of the SPP RE Trustees.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties**. The SPP RE RRSDP includes steps for a fair and open standards process that is open to all regional stakeholders. Any entity within the SPP RE or SPP RTO region has a right to participate by: (a) expressing a position and its basis; (b) having that position considered; (c) voting through a segment-weighted balanced process; and (d) having the right to appeal.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico.** This criterion does not apply to SPP RE.

3. **SPP RE operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. The Delegation Agreement between SPP RE and NERC grants SPP RE the authority to carry out certain statutory activities, including: (i) certification of BPS entities; (ii) registration of owners, operators, and user of the BPS as responsible for compliance with requirements of Reliability Standards; (iii) reliability assessment and performance analysis; (iv) event analysis and reliability improvement; (v)

training and education; and (vi) situational awareness and infrastructure security. This delegation of authority has promoted the effective and efficient administration of the BPS. Through its delegated authority from NERC, SPP RE has successfully implemented the NERC CMEP, and is working with NERC and the other Regional Entities to improve both the effectiveness and efficiency of the program. As evidence of the success of the early program, SPP RE's region successfully navigated nine consecutive quarters without a reportable transmission vegetation contact.

SPP RE has also, in combination with the other Regional Entities and NERC, greatly enhanced the functionality of the electronic tool (webCDMS), used by registered entities to report compliance issues. Enhancements to webCDMS have allowed both the Regional Entities and registered entities to realize efficiency gains through the automation of processes such as: (i) self-reports, (ii) self-certifications, (iii) submission of mitigation plans, (iv) exchange of mitigation information, (v) mis-operations reporting, (vi) analysis of prior violations, and (vii) violation processing in general. Furthermore, the SPP RE compliance audit teams utilize a risk-based assessment to determine the scope of the compliance audit, and adjust the scope of compliance audits based on violation history and the particular risk presented by certain registered functions. To further improve the effectiveness and efficiency of the program going forward, SPP RE is working with NERC and the other Regional Entities to shift the focus of the ERO Enterprise to those areas of the BPS that present the greatest risk to reliability. To that extent, SPP RE is an active participant in the RAI process.

In addition, since January 1, 2009, SPP RE has steadily increased its outreach efforts. SPP RE has held annual workshops since 2009 and attendance has increased each year. SPP RE staff has made incremental improvements to the workshops, such as inviting more guest speakers from outside the SPP RE footprint including FERC Commissioners, NERC Board members, and Department of Homeland Security staff, adding break-out sessions to give registered entities a smaller setting to ask questions and voice concerns, and refining both advance and on-site preparations to ensure the workshops run smoothly and on-time. In 2011, workshop attendees began providing feedback via evaluation forms following the workshops; feedback has generally been very favorable. In 2011, SPP RE began publishing monthly newsletters and implemented an e-news format that is easily readable on handheld devices. In 2012, SPP RE created a video training webpage and began filming and publically posting training videos in-house and at workshops. The feedback from the training videos has been generally positive and benefits not only registered entities in the SPP RE footprint, but registered entities across all Regional Entities.

Texas Reliability Entity, Inc. (TRE or Texas RE)

1. **TRE "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board**." Texas RE currently has a combination independent and balanced stakeholder board. From 2007 to 2010, the Regional Entity for the ERCOT region was Texas Regional Entity, Inc., an independent division of the Electric Reliability Council of Texas, Inc. (ERCOT, the ISO for the region). During that time, Texas RE shared the same board of directors as ERCOT ISO.

To ensure that the Regional Entity would remain independent from all registered entities, including ERCOT, a new Texas non-profit corporation called Texas Reliability Entity, Inc. (Texas RE), was formed to take over the functions as Regional Entity effective July 1, 2010. As part of this process, Texas RE separated its board of directors from ERCOT ISO. Texas RE is now governed by a combination independent and balanced stakeholder board consisting of nine members: (i) four independent directors; (ii) two industry-affiliated directors; (iii) the Texas RE CEO; and (iv) two ex-officio non-voting directors (the Public Utility Commission of Texas Chairman or delegate, and the Public Counsel from the Office of Public Utility Counsel). The independent directors are elected by Texas RE membership to serve staggered three-year terms. The two-industry-affiliated directors may not be from the same market sector and may not concurrently serve on the ERCOT ISO board of directors.

2. **TRE met the requirements of Section 215 (c)(1) (2) of the Federal Power Act, because**:
   a. **TRE is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system.** Texas RE follows the requirements as defined by the NERC ROP, including the CMEP, and by the Delegation Agreement with NERC, including TRE's current RRSDP, and has used these documents to develop standards and to audit and enforce compliance with the standards.

      Standards Development: Texas RE participates in the NERC Standards Committee and develops, comments and votes on Reliability Standards. Texas RE also hosts quarterly meetings of the Reliability Standards Committee (RSC) and twice-monthly meetings of the NERC Standards Review Subcommittee (NSRS). Changes and proposed changes to NERC Reliability Standards are discussed in these forums. Texas RE created one major regional Reliability Standard (BAL-001-TRE) and several minor regional Reliability Standards (CIP-001 regional variance and IRO-0006-TRE) designed to improve reliability. The major regional Reliability Standard, BAL-001-TRE, was designed to maintain Interconnection steady-state frequency within defined limits in the ERCOT region. It requires individual generation facilities to operate with properly configured governors in service to meet frequency response performance requirements.

      Compliance: Between January 1, 2009 and December 31, 2013, Texas RE successfully completed more than 260 audits of registered entities for compliance with Reliability Standards. Texas RE uses the complete list of NERC-approved actively monitored Reliability Standards and Requirements as the minimum audit scope. Audit staff also investigates possible violations of the Reliability Standards arising from BPS disturbances, outages, self-reports, and complaints. Texas RE requires all Compliance employees, not just the auditors, to complete NERC scheduled basic training classes for auditors so that all employees have an understanding of the significance of the auditing process. In addition, Texas RE has developed a robust CIP compliance and audit program. All current CIP auditors have earned Department of Defense 8570 recognized certifications (e.g., CISSP, CEH, CISA, and Network+).

Enforcement: In addition to the auditing program, Texas RE has implemented a separate Enforcement program with a dedicated staff. The Enforcement group processes alleged violations originating from audits, spot checks, self-certifications, complaints, and self-reports. This includes managing settlement negotiations, supporting legal staff in contested case hearings, and reviewing and approving mitigation plans. Texas RE has been successful in streamlining the Enforcement process since 2009 by implementing a new webCDMS data management system and implementing new processes such as the FFT program.

b. TRE has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure.** Texas RE has adopted bylaws to assure its independence from industry while assuring fair stakeholder representation in selection of its directors and balanced decision-making in its committees. Its bylaws first provide that Texas RE membership is voluntary and open to any entity that is a user, owner or operator of the ERCOT region BPS that registers as a member with Texas RE and complies with Texas RE bylaws. In addition to the structure of the board described earlier, independent directors and members of their immediate families or households may not: (1) have current or recent status (within the past two years) as a director, officer or employee of an ERCOT region NERC registered entity or ERCOT region electric Market Participant, or (2) have direct business relationships, other than as customers, with any NERC registered entity or ERCOT region electric Market Participant. The industry-affiliated directors are selected annually by the Texas RE Member Representatives Committee and each must come from a different Texas RE membership sector: System Coordination and Planning, Transmission and Distribution, Cooperative, Municipal Utility, Generation, or Load-Serving and Marketing. The Texas RE bylaws prohibit an entity from belonging to any two membership sectors, and require the board of directors and any of its committees to operate using balanced decision-making.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities.** Texas RE bylaws and its Delegation Agreement with NERC provide that it will allocate equitably reasonable dues, fees, and other charges among end users for its statutory activities. Each year Texas RE produces a draft budget using templates provided by NERC, and posts the draft on its website for public comment. The budget includes the costs necessary to perform Texas RE's statutory functions under the Delegation Agreement with NERC and any expected income, such as membership fees. The budget is reviewed for reasonableness by the Texas RE Member Representatives Committee and approved by the Texas RE board of directors, NERC and FERC. Pursuant to Exhibit E to

its Delegation Agreement, assessments to fund Texas RE delegated functions and related activities are allocated to all load-serving entities in the region on the basis of NEL. Penalty monies received by Texas RE are applied as a general offset to its budget requirements for the subsequent fiscal year.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties.** Texas RE has adopted and implemented the CMEP in accordance with its Delegation Agreement with NERC. Texas RE is committed to five guiding principles: (1) independence; (2) ethics and integrity; (3) inclusiveness; (4) fairness and openness; and (5) organizational effectiveness and efficiency. Texas RE strives to be fair, unbiased and balanced in its enforcement actions and imposition of penalties, and its internal procedures incorporate these concepts. After a possible violation is found by the Compliance group, the violation is reviewed and verified by a member of the Enforcement group. Penalties are calculated using the NERC *Sanction Guidelines* and are reviewed in relation to similar penalties assessed in this and other regions. In addition, all penalties are reviewed by the director of enforcement prior to issuance.

Texas RE also has implemented policies and procedures to ensure its employees act with independence, ethics, integrity, fairness, and openness. All Texas RE employees and contractors must annually sign an ethics agreement which requires them to conduct Texas RE business with total objectivity and to avoid situations in which his or her personal or financial interests conflict or appear to conflict with the interests of Texas RE. A conflict of interest arises when: (1) the personal, financial, or other interest of a Texas RE employee is significantly affected or may reasonably appear to be affected by the employee's actions or decisions in the employee's capacity at Texas RE; or (2) the action of any employee is in any way detrimental to the best interests of Texas RE. Financial interest includes any ownership, investment, or compensation interest by the employee or a member of the employee's household, and specifically includes any direct or indirect remuneration, as well as gifts or favors which are not insubstantial. An employee must immediately inform the Texas RE legal department if a conflict of interest or even the appearance of a conflict of interest might exist, to allow Texas RE management to evaluate the situation. After full disclosure by the employee, Texas RE management may agree to conditions that appropriately limit any potential influence from a conflict of interest.

Texas RE also follows the CMEP requirement to provide biographies of all potential audit team members to registered entities prior to a Compliance engagement and provide opportunity for entities to object to use of any employee where a potential conflict of interest exists. At the

end of each audit, registered entities are also provided a questionnaire which allows them to directly report to NERC any concerns they have with fairness, openness, or objectivity with respect to how Texas RE conducted the audit. In addition, Texas RE has implemented a Compliance hotline to allow anyone to report (anonymously if desired) any noncompliance by a registered entity and any ethics complaints they have concerning Texas RE.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties**. As part of its Delegation Agreement, Texas RE has adopted and follows a RRSDP designed to provide for reasonable notice and opportunity for public comment, due process, and balancing of interests. The RRSDP requires that proposed Reliability Standards must be drafted by a standards drafting team and be posted publicly, and it requires a public comment period prior to any vote on the standard by Texas RE membership.

Texas RE also conducts its general operations in a manner that is transparent to the public. As required by its bylaws, it posts public notices of its board and committee meetings on its public website and posts meeting materials, including draft budgets, for public review prior to the meetings. The Texas RE public website includes training materials, useful compliance information, and the contact information for key Texas RE personnel.

Texas RE also provides due process to registered entities seeking to contest a violation, penalty or sanction. Texas RE adheres to the NERC ROP and CMEP, which require Regional Entities to provide registered entities reasonable notice of possible violations, the ability to contest a violation or penalty or sanction, and the ability to appeal such matters to the NERC Compliance Committee and FERC. In August 2013, FERC approved Texas RE's request to begin using the same hearing procedures as are used by the other seven Regional Entities.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico.** This criterion is not applicable to Texas RE.

3. **TRE operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability**. Under its Delegation Agreement with NERC, Texas RE has promoted effective and efficient administration of the BES in the ERCOT region. Texas RE has worked with industry to create a major regional Reliability Standard (BAL-001-TRE) and several minor regional Reliability Standards (CIP-001 regional variance and IRO-006-TRE) designed to improve reliability in the ERCOT region. The major regional Reliability Standard requires individual generation facilities to operate with properly configured governors in service to meet frequency

response performance requirements. Texas RE also has successfully implemented the CMEP in the region, performing more than 260 audits since January 2009 and developing a robust CIP audit program. Since 2009, Texas RE has streamlined its Enforcement processing by implementing the webCDMS data management system in 2011 and implementing the FFT program to more quickly process lower risk violations. From 2010 to 2012, Texas RE also worked in cooperation with NERC, the other regions and industry to develop an events analysis program in which registered entities report their performance during system events and develop lessons learned to be shared with the industry. Early in the program, when Texas faced rotating outages during the 2011 Southwest Cold Weather Event, Texas RE used the framework the events analysis program provided to quickly collect and analyze information from the event and to disseminate it to FERC, NERC, and the industry.

Western Electricity Coordinating Council (WECC)

1. **WECC "is governed by an independent board, a balanced stakeholder board or a combination independent and balanced stakeholder board**." Since its creation, WECC has been governed by a hybrid board of directors including both non-affiliated directors and a balanced group of stakeholder directors as envisioned by the FPA §215(e)(4), 16 U.S.C. §824o(e)(4). However, on June 27, 2013, the WECC Board approved the bifurcation of the company into a Regional Entity (WECC) and a Reliability Coordination Company, Peak Reliability. This decision—the culmination of a year of work by various WECC board committees, staff, WECC members, and WECC stakeholders—signals a major landmark in the history of the organization. Under this new structure the RC and IA functions in the Western Interconnection will become a separate company from WECC. When established, Peak Reliability will provide core and other associated reliability coordination services within the Western Interconnection. As anticipated, the Commission approved the relevant documents by the end of December 2013;[153] however, as there were outstanding compliance filings, the bifurcation was not finalized during the assessment period.[154] Nevertheless, WECC and Peak Reliability began operating as separate entities in many respects by that time.

2. **WECC met the requirements of Section 215 (c)(1) (2) of the Federal Power Act, because**:
    a. **WECC is able to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system**. WECC's authority to enforce Reliability Standards is based on the authority granted in its Delegation Agreement with NERC. FERC's approval of the Delegation Agreement conferred authority to WECC to manage and enforce compliance with FERC-approved Reliability Standards and to apply penalties up to the extent of FERC's civil penalty

[153] *See Western Electricity Coordinating Council*, Order on Petition for Declaratory Order, 143 FERC ¶ 61,239, *order on reh'g*, 145 FERC ¶ 61,202 (2013), *appeal pending sub nom. Edison Electric Institute v. FERC*, No. 14-1012 (D.C. Cir. Jan. 27, 2014).

[154] The Commission accepted the compliance filings on February 12, 2014. *See North American Electric Reliability Corporation; Western Electricity Coordinating Council*, 146 FERC ¶ 61,092 (2014), *order on reh'g*, 147 FERC ¶ 61,063 (2014), *appeal pending sub nom. Edison Electric Institute v. FERC*, No. 14-1071 (D.C. Cir. May 9, 2014).

authority. Additionally, WECC develops Regional Criteria and practices to improve the functioning and efficiency of the Western Interconnection. This combination provides a forum for addressing system-wide issues and an oversight role to promote reliable operation of the Western Interconnection.

WECC also demonstrated its ability to enforce reliability standards during the assessment period, by successfully clearing its backlog of Enforcement work; completing all audits contemplated in its annual Implementation Plans; developing and maintained highly qualified Compliance staff; enhancing, streamlining and documenting all the Enforcement processes; successfully implementing new IT solutions and systems; and expanding and enhancing its compliance encouragement and outreach efforts. Furthermore, WECC worked collaboratively with the other Regional Entities and NERC to bring forward the Omnibus proposal; proposed NERC ROP changes to streamline TFE processing; developed new registration system tools; and, actively participated in several ongoing NERC IT projects, lending expertise and practical experience.

b. WECC has established rules that:

i. **Assure its independence of the users and owners and operators of the bulk-power system, while assuring fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organization structure**. WECC currently has a hybrid board comprised of member class directors and non-affiliated (independent) directors, who are subject to standards of conduct set out in WECC's bylaws. This ensures that member/stakeholder views are well-represented and that board decisions are ultimately made fairly and in the best interests of WECC as a whole. Effective January 1, 2014, WECC transitioned to an all independent director board. Accordingly, directors are directly elected by the WECC membership and members are represented on a newly created Member Advisory Committee that has direct access to the WECC Board to provide advice and recommendations regarding WECC policy and proposed board decisions. In addition, WECC staff members, and representatives from WECC member entities, routinely participate in ERO and ERO Enterprise committees and work groups.

ii. **Allocate equitably reasonable dues, fees, and other charges among end users for all activities**. The allocation of dues, fees and other charges is governed by §12.1 of the WECC bylaws, Funding of Reliability Activities. WECC funds all activities undertaken pursuant to FPA §215 in accordance with the funding provisions and procedures of that law and related FERC regulations and orders. The WECC Board approves the annual business plan and budget in time for submission to the ERO and to FERC for approval. WECC funds reliability activities undertaken pursuant to any agreements with appropriate Canadian or Mexican authorities in accordance with the provisions of those agreements. In adopting budgets for the costs of reliability activities, the WECC Board seeks an equitable allocation based upon the NEL

and other relevant factors consistent with applicable law, the Delegation Agreement and any international reliability agreements. To the extent that WECC elects to fund any activities not eligible for funding pursuant to §§12.1.1 and 12.1.2, it does so through the use of service fees, charges or dues applicable to the persons or entities that voluntarily participate in such activities.

iii. **Provide fair and impartial procedures for enforcement of reliability standards through the imposition of penalties.** WECC's Delegation Agreement with NERC is based on the NERC *pro forma* Delegation Agreement and has been reviewed and approved by FERC. As required, WECC developed an annual CMEP Implementation Plan, which identifies the NERC Reliability Standards on the actively monitored list as well as the compliance monitoring methods that will be used to enforce those standards. The plan was submitted to NERC for approval. Additionally, WECC has developed and documented all formal processes and procedures relating to enforcement activities, including penalties. In this regard, WECC uses the NERC *Sanction Guidelines* as a framework for assessing fair and reasonable penalties, and considers all facts associated with the registered entity and the alleged violation. Individuals responsible for assessing, recommending, or negotiating penalties are not otherwise involved in compliance monitoring or discovery of violations. In other words, WECC specifically segregates the duties associated with violation discovery or review and violation disposition and penalty assessment. Furthermore, WECC has a layered review approach to penalties, including non-monetary ones. Specifically, the manager of enforcement policy reviews all penalties and communicates with the director of enforcement, who then reviews and, as appropriate, approves them. WECC management reviews these processes and procedures bi-annually. Finally, WECC's enforcement staff receives regular training on all aspects of their duties to ensure consistency of application. This training is delivered in weekly staff meetings as well as at formal training sessions held at least annually.

iv. **Provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties.** WECC uses the FERC-approved WECC RRSDP to develop regional Reliability Standards along with regional criteria and regional business practices. These procedures assure that the documents will be developed in a fair and open manner with contribution and review by subject matter experts and that all affected parties will have the chance to comment and vote on the documents. Illustratively, proposed standards are drafted by a standards drafting team, publicly posted, and subject to a mandatory public comment period prior to any vote.

In regard to the exercise of its other duties, WECC posts on its website notices of, and agendas and materials for, board and committee meetings. WECC

also adheres to the NERC ROP and the CMEP processes, which provide due process protections to registered entities with respect to compliance obligations and enforcement of standards violations. Accordingly, registered entities are provided reasonable notice of possible violations, and the right to contest a violation, penalty or sanction, and to appeal the Regional Entity's decisions to the NERC Board of Trustees Compliance Committee, and the Commission.

v. **Provide for taking appropriate steps to gain recognition in Canada and Mexico**. WECC has negotiated various agreements with the applicable governmental authorities for British Columbia, Canada, Alberta, Canada, and Baja, Mexico, the three international areas included in the Western Grid, as detailed below:

British Columbia:

Under the Administration Agreement (dated October 8, 2009) between the British Columbia Utilities Commission (BCUC) and the WECC, WECC acts as the administrator for the BCUC in carrying out certain activities relating to the Mandatory Reliability Standards program in British Columbia. Working under this agreement, WECC monitors compliance to the standards adopted in BC. WECC receives and reviews self-reports, self-certifications, and periodic data submittals; conducts audits; and reviews mitigation plans and other such activities. At the BCUC's request, WECC has set up a separate webCDMS portal, an electronic system to collect compliance data, dedicated to BCUC and its entities.

Alberta:

WECC acts as the Compliance Monitor for the Alberta Market Surveillance Administrator (Alberta MSA), under the Services Agreement (dated April 30, 2010) between the Alberta MSA and WECC, in carrying out certain activities related to Alberta Reliability Standards, specific to the Alberta Electric System Operator (AESO), in Alberta, Canada. WECC operates under the Services Agreement with the MSA, and as contemplated in the membership and operating agreement (MOA) (dated September 23, 2008) with the AESO.

Mexico:

Under the MOA (dated December 31, 2010) between Comisión Federal de Electricidad (CFE) and WECC, WECC acts as CFE's compliance monitor for certain activities in Baja California, Mexico, monitoring compliance with its mandatory Reliability Standards. The agreement between CFE and WECC requires that WECC not disclose any confidential data to anyone other than CFE. Any request from NERC or FERC to WECC for data relating to WECC activities in Mexico is directed to CFE. The CFE/WECC annual Implementation Plan, based on WECC's

recommendations and after consultation with the Area de Control Baja California (ACBC), CFE's compliance program administrator, includes a list of actively monitored standards, a description of the monitoring methods WECC uses for designated entities, and the compliance audit timeline. As with British Columbia, the Alberta MSA, and the AESO, WECC set up a separate webCDMS portal for use by CFE.

In summary, WECC does not have enforcement or registration authority for any of the international jurisdictions within the Western Interconnection. WECC provides monitoring, reviews mitigation plans and completed mitigation plans, and assessment recommendations with respect to alleged violations.

3. WECC operates under a delegation agreement that promotes effective and efficient administration of bulk-power system reliability. WECC assures the reliability and efficient administration of the Western Interconnection through a variety of activities authorized under its Delegation Agreement. To start with, during the assessment period, WECC continued to develop regional Reliability Standards, in large part due to its unique situation among the Regional Entities. Indeed, WECC has developed the most regional Reliability Standards because of a mandatory program it had in place prior to the approval of NERC as the ERO and the delegation to WECC. Under this program (called the Reliability Management System (RMS)), WECC is required to translate existing reliability criteria into regional mandatory standards. As a consequence, whereas all of the other Regional Entities have a total of seven regional Reliability Standards, WECC alone has a total of eight.[155]

WECC likewise promoted effective and efficient administration of the BPS in the Western Interconnection during the assessment period through its implementation of NERC's CMEP approved by the Commission. Illustratively, WECC successfully cleared its backlog of Enforcement work; completed all audits contemplated in its annual Implementation Plans; developed and maintained a highly qualified Compliance staff; enhanced, streamlined and documented all the Enforcement processes; successfully implemented new IT solutions and systems; and expanded and enhanced its compliance encouragement and outreach efforts. Furthermore, WECC worked collaboratively with the other Regional Entities and NERC to bring forward the Omnibus proposal; proposed ROP changes to streamline TFE processing; developed new registration system tools; and, actively participated in several ongoing NERC IT projects, lending expertise and practical experience.

As a separate matter with respect to the administration of the Western Interconnection, during the assessment period, WECC managed a comprehensive planning database, provided guidance on the analysis and modeling of the transmission system, and developed scenario

[155] These eight regional Reliability Standards are: (i) FAC-501-WECC-1 (Transmission Maintenance); (ii) VAR-002-WECC-1 (Automatic Voltage Regulators); (iii) VAR-501-WECC-1 (Power System Stabilizer); (iv) PRC-004-WECC-1 (Protection System and Remedial Action Scheme Misoperation); (v) IRO-006-WECC-1 (Qualified Transfer Path Unscheduled Flow Relief); (vi) BAL-004-WECC-01 (Automatic Time Error Correction); (vii) TOP-007-WECC-1 (System Operating Limits); and (viii) BAL-002-WECC-2 (Contingence Reserve) (replacing BAL-STD-002-2).

studies of system performance to establish operating policies and limits, and regional transmission planning. In addition, WECC performed annual assessments of 10-year loads and resources in the Western Interconnection and created a 10-year coordinated plan of system growth. WECC also provided information to NERC for their annual summer and winter assessments of the reliability of the BPS. Beginning in 2012, WECC produced an annual *State of the Interconnection* report to provide WECC's members and stakeholders with an independent assessment of data collected annually in the Western Interconnection. The goal was to develop reasonable measurements that would identify reliability trends in the Interconnection.

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-____

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 3

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

NERC ASSESSMENT OF REGIONAL ENTITY DELEGATED FUNCTIONS

JULY 21, 2014

Attachment 3

TABLE OF CONTENTS

I. RELIABILITY STANDARDS DEVELOPMENT 2

A. Regional Entity Standards Development Process 3

B. Review of Each Regional Entity's Standards Development Activities During the Assessment Period 4

1. Florida Reliability Coordinating Council, Inc. 5
2. Midwest Reliability Organization 5
3. Northeast Power Coordinating Council, Inc. 6
4. ReliabilityFirst Corporation 6
5. SERC Reliability Corporation 7
6. Southwest Power Pool Regional Entity 7
7. Texas Reliability Entity, Inc. 8
8. Western Electricity Coordinating Council 9

II. COMPLIANCE MONITORING AND ENFORCEMENT 12

A. Organization Registration and Certification 13

B. Compliance Monitoring 16

1. NERC Oversight of Regional Entity Compliance Monitoring Activities 16
   a. Annual CMEP Implementation Plan 17
   b. Key Reliability Standard Spot Check Program 18
   c. Oversight Audits of Regional Entity Audits of Registered Entities 19
   d. NERC Training Activities for Regional Entity Compliance Staff 19
2. NERC Evaluation of Regional Entity Compliance Monitoring Programs 20
   a. Registered Entity Training, Education, and Outreach Programs for Registered Entity Personnel 20
   b. Assessments of the Individual Regional Entities 21
      i. Data on Regional Entity Compliance Resources 22
      ii. Florida Reliability Coordinating Council, Inc. 23
      iii. Midwest Reliability Organization 26
      iv. Northeast Power Coordinating Council, Inc. 30
      v. ReliabilityFirst Corporation 33

vi. SERC Reliability Corporation 38
vii. Southwest Power Pool Regional Entity 43
viii. Texas Reliability Entity, Inc. 46
ix. Western Electricity Coordinating Council 48

C. Compliance Investigations 54

D. Compliance Enforcement 55

1. Performance of the ERO Enterprise 55
a. Overview 55
b. Improvements in Enforcement Processing, 2009-2013 57
i. The Composition of the ERO Enterprise Caseload 57
ii. The Caseload Index 60
iii. Efforts to Reduce Older Caseload 61
iv. Implementation of Streamlined Enforcement Processing Mechanisms 63
v. Implementation of Compliance Data Systems 66
vi. Quality of Submitted Information 66
c. Improving Reliability Across the ERO Enterprise 67
i. Encouraging Internal Discovery of Violations 67
ii. Ensuring the Timely Mitigation of Violations 68
iii. Promoting Reliability through Enforcement Philosophy and Practices 69
d. NERC's Ongoing Monitoring of Specific Regional Entity Processes Under the CMEP 69
e. Conclusion 71
2. Evaluation of Florida Reliability Coordinating Council, Inc. 72
a. Overview 72
b. Evaluation of Caseload Processing Efficiency 73
i. The Composition of FRCC's Caseload 73
ii. Caseload Index 74
iii. Efforts to Reduce Older Caseload 74
iv. Implementation of Streamlined Enforcement Processing Mechanisms 75
c. Improving Reliability 75
i. Encouraging Internal Discovery of Violations 75
ii. Ensuring the Timely Mitigation of Violations 76

iii. Promoting Reliability through Enforcement Philosophy and Practices 77
d. FRCC's Implementation of Various Aspects of the CMEP 78
e. Conclusion 78
3. Evaluation of Midwest Reliability Organization 79
a. Overview 79
b. Evaluation of Caseload Processing Efficiency 80
i. The Composition of MRO's Caseload 80
ii. Caseload Index 82
iii. Efforts to Reduce Older Caseload 82
iv. Implementation of Streamlined Enforcement Processing Mechanisms 82
c. Improving Reliability 83
i. Encouraging Internal Discovery of Violations 83
ii. Ensuring the Timely Mitigation of Violations 84
iii. Promoting Reliability through Enforcement Philosophy and Practices 85
d. MRO's Implementation of Various Aspects of the CMEP 86
e. Conclusion 87
4. Evaluation of Northeast Power Coordinating Council, Inc. 87
a. Overview 87
b. Evaluation of Caseload Processing Efficiency 88
i. The Composition of NPCC's Caseload 88
ii. Caseload Index 90
iii. Efforts to Reduce Older Caseload 90
iv. Implementation of Streamlined Enforcement Processing Mechanisms 90
c. Improving Reliability 91
i. Encouraging Internal Discovery of Violations 91
ii. Ensuring the Timely Mitigation of Violations 92
iii. Promoting Reliability through Enforcement Philosophy and Practices 93
d. NPCC's Implementation of Various Aspects of the CMEP 93
e. Conclusion 94
5. Evaluation of ReliabilityFirst Corporation 94
a. Overview 94
b. Evaluation of Caseload Processing Efficiency 95

i. The Composition of ReliabilityFirst's Caseload 95

ii. Caseload Index 97

iii. Efforts to Reduce Older Caseload 97

iv. Implementation of Streamlined Enforcement Processing Mechanisms 98

c. Improving Reliability 99

i. Encouraging Internal Discovery of Violations 99

ii. Ensuring the Timely Mitigation of Violations 99

iii. Promoting Reliability through Enforcement Philosophy and Practices 100

d. ReliabilityFirst's Implementation of Various Aspects of the CMEP 101

e. Conclusion 102

6. Evaluation of SERC Reliability Corporation 102

a. Overview 102

b. Evaluation of Caseload Processing Efficiency 103

i. The Composition of SERC's Caseload 103

ii. Caseload Index 105

iii. Efforts to Reduce Older Caseload 105

iv. Implementation of Streamlined Enforcement Processing Mechanisms 106

c. Improving Reliability 107

i. Encouraging Internal Discovery of Violations 107

ii. Ensuring the Timely Mitigation of Violations 107

iii. Promoting Reliability through Enforcement Philosophy and Practices 108

d. SERC's Implementation of Various Aspects of the CMEP 109

e. Conclusion 110

7. Evaluation of Southwest Power Pool Regional Entity 110

a. Overview 110

b. Evaluation of Caseload Processing Efficiency 111

i. The Composition of SPP RE's Caseload 111

ii. Caseload Index 113

iii. Efforts to Reduce Older Caseload 113

iv. Implementation of Streamlined Enforcement Processing Mechanisms 113

c. Improving Reliability 114

i. Encouraging Internal Discovery of Violations 114

ii. Ensuring the Timely Mitigation of Violations 115

iii. Promoting Reliability through Enforcement Philosophy and Practices 116

d. SPP RE's Implementation of Various Aspects of the CMEP 117

e. Conclusion 118

8. Evaluation of Texas Reliability Entity, Inc. 118

a. Overview 118

b. Evaluation of Caseload Processing Efficiency 119

i. The Composition of Texas RE's Caseload 119

ii. Caseload Index 121

iii. Implementation of Streamlined Enforcement Processing Mechanisms 121

c. Improving Reliability 122

i. Encouraging Internal Discovery of Violations 122

ii. Ensuring the Timely Mitigation of Violations 123

iii. Promoting Reliability through Enforcement Philosophy and Practices 124

d. Texas RE's Implementation of Various Aspects of the CMEP 125

e. Conclusion 125

9. Evaluation of Western Electricity Coordinating Council 126

a. Overview 126

b. Evaluation of Caseload Processing Efficiency 127

i. The Composition of WECC's Caseload 127

ii. Caseload Index 129

iii. Efforts to Reduce Older Caseload 129

iv. Implementation of Streamlined Enforcement Processing Mechanisms 129

c. Improving Reliability 130

i. Encouraging Internal Discovery of Violations 130

ii. Ensuring the Timely Mitigation of Violations 131

iii. Promoting Reliability through Enforcement Philosophy and Practices 132

d. WECC's Implementation of Various Aspects of the CMEP 133

e. Conclusion 134

III. RELIABILITY ASSESSMENTS 134

A. Overview of Regional Entity Responsibilities 134

B. Regional Entity Responsibilities in the Preparation of Assessment Reports 136

1. Reliability Assessment Data Collection 136

2. Reliability Assessment Narratives 137

C. Regional Entity Responsibilities in the Preparation of *State of Reliability* Reports 137

D. Regional Entity Responsibilities in the Collection of Data for NERC Reliability Databases 138

E. Regional Entity Resources Budgeted for Reliability Assessment and Performance Analysis During the Assessment Period 138

F. Evaluation of Regional Entity Performance in Reliability Assessment Activities and Areas for Improvement 139

IV. RELIABILITY RISK MANAGEMENT (SITUATION AWARENESS AND EVENT ANALYSIS) 142

A. Regional Entity Progress in Identifying and Analyzing System Events and Improving Situation Awareness 142

B. Hurricane Sandy Provided a Meaningful Case Study and Test of the ERO's Situation Awareness Capabilities 144

C. Areas for Future Improvements and Enhancements 145

V. BUSINESS PLANNING AND BUDGETING, FINANCE AND ACCOUNTING 146

A. Provisions of Commission Orders, the RDAs and the ROP Concerning the Regional Entities' Business Plans and Budgets and Financial Accounting and Reporting 146

B. Regional Entity Performance in Business Planning and Budgeting, Accounting, and True-Up Reporting 147

This **Attachment 3** is NERC's assessment of the Regional Entities' performance of their delegated functions during the five-year assessment period 2009 through 2013. Following are brief descriptions of the geographic footprints of the eight Regional Entities.

Florida Reliability Coordinating Council, Inc. (FRCC) is the Federal Energy Regulatory (FERC or Commission)-approved Regional Entity for the territory covering peninsular Florida in the Eastern Interconnection.

Midwest Reliability Organization (MRO) is the FERC-approved Regional Entity for the north central region of North America within the Eastern Interconnection. MRO's footprint spans the states of North Dakota, Minnesota, and Nebraska, the majority of the territory in the states of South Dakota, Iowa, and Wisconsin, portions of Michigan and Montana, and the Canadian provinces of Saskatchewan and Manitoba.

Northeast Power Coordinating Council, Inc. (NPCC) is the FERC-approved Regional Entity for the northeastern North American region in the Eastern Interconnection. NPCC's footprint includes the states of Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont, as well as the Canadian provinces of New Brunswick, Nova Scotia, Ontario, and Quebec.

ReliabilityFirst Corporation (ReliabilityFirst) is the FERC-approved Regional Entity for portions of the mid-Atlantic and east central areas of the United States within the Eastern Interconnection. ReliabilityFirst's footprint includes all or portions of the states of New Jersey, Pennsylvania, Delaware, Maryland, Virginia, West Virginia, Ohio, Michigan, Kentucky, Tennessee, Indiana, Illinois, Wisconsin, and the District of Columbia.

SERC Reliability Corporation (SERC) is the FERC-approved Regional Entity for the southeastern United States region within the Eastern Interconnection. SERC's footprint includes the states of Alabama, Georgia, Mississippi, Missouri, North Carolina, South Carolina, and Tennessee, and portions of the states of Arkansas, Florida, Illinois, Iowa, Kentucky, Louisiana, Oklahoma, Texas, and Virginia.

Southwest Power Pool Regional Entity (SPP RE) is the FERC-approved Regional Entity for the central southern United States within the Eastern Interconnection. SPP RE's footprint includes all or parts of the states of Arkansas, Kansas, Louisiana, Mississippi, Missouri, New Mexico, Oklahoma, and Texas. SPP RE is an independent and functionally separate division of Southwest Power Pool, Inc., one of nine independent system operators (ISOs)/RTOs in North America.

Texas Reliability Entity, Inc. (Texas RE) is the FERC-approved Regional Entity for the Electric Reliability Council of Texas (ERCOT) region in the Texas Interconnection. At the time of the three-year performance assessment, Texas Regional Entity, an independent division of ERCOT, performed compliance monitoring and enforcement activities for the ERCOT region. Texas RE was formed on January 1, 2010 to become the successor Regional Entity for the ERCOT region. Effective July 1, 2010, NERC delegated to Texas RE the authority and responsibility for

the continuation of all compliance monitoring and enforcement activities that it had previously delegated to Texas Regional Entity.

Western Electricity Coordinating Council (WECC) is the FERC-approved Regional Entity for the portions of the Western United States and Canada in the Western Interconnection. WECC's footprint extends from the provinces of Alberta and British Columbia in Canada to the northern portion of Baja California, Mexico. WECC's service territory includes all or portions of 14 states in the western United States. Geographically, WECC's territory is the largest of all the Regional Entities.

I. RELIABILITY STANDARDS DEVELOPMENT

Section 215(d) of the Federal Power Act (FPA), 16 U.S.C. §824o(d), requires NERC to develop mandatory and enforceable Reliability Standards that are subject to Commission review and approval. A Regional Entity may also develop a Reliability Standard for approval by NERC and by the Commission, to be effective in that Regional Entity only. The FPA and Commission regulations provide that the ERO shall rebuttably presume that a proposal from a Regional Entity organized on an interconnection-wide basis for a Reliability Standard or modification to a Reliability Standard to be applicable on an interconnection-wide basis is just, reasonable, and not unduly discriminatory or preferential, and in the public interest.[1] This presumption is also embodied in the Regional Delegation Agreements (RDAs), which delegate to each Regional Entity authority to propose regional Reliability Standards to NERC for approval.

In Order No. 672, the Commission stated that:

> As a general matter, we will accept the following two types of regional differences, provided they are otherwise just, reasonable, not unduly discriminatory or preferential and in the public interest, as required under the statute: (1) a regional difference that is more stringent than the continent-wide Reliability Standard, including a regional difference that addresses matters that the continent-wide Reliability Standard does not; and (2) a regional Reliability Standard that is necessitated by a physical difference in the Bulk-Power System.[[2]]

These parameters are embodied in the NERC Rules of Procedure (NERC ROP). Section 312.1 of the NERC ROP specifies that 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. Section 313.1 of the NERC ROP specifies that Regional Entities may develop Regional Criteria that are necessary to implement, augment, or comply with NERC Reliability Standards, but which are not Reliability Standards; or which address issues not within the scope of Reliability Standards.

---

[1] FPA §215(d)(3), 16 U.S.C. §824o(d)(3), 18 C.F.R. §39.5(b).

[2] *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, at P 291, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

Regional Reliability Standards must be approved by NERC and are then submitted by NERC to the Commission; they become enforceable as NERC Reliability Standards under §215 of the FPA in the U.S. once they are approved by the Commission. Therefore, regional Reliability Standards must meet the requirements set out by the Commission for approval of such standards, including having violation risk factors (VRFs) and violation severity levels (VSLs) that meet the criteria the Commission has set out in its various orders.

To evaluate each Regional Entity's performance during the assessment period, NERC focused on two parameters. First, NERC reviewed whether each Regional Entity has in place a regional Reliability Standards Development Procedure (RSDP) that meets applicable requirements. This portion of the evaluation was straightforward because, as described in §I.A below, each Regional Entity is required to have in place, as part of its RDA, a NERC-approved and Commission-approved RSDP that satisfies a pre-established set of attributes. During the assessment period, some of the Regional Entities developed revisions to their RSDPs, which were approved by NERC and by the Commission. Second, NERC reviewed each Regional Entity's activity, if any, in developing proposed regional Reliability Standards during the assessment period. As described in §I.B below, with the exception of WECC, the Regional Entities have, in general, suspended regional Reliability Standards development activities in favor of devoting resources and stakeholder participation to the development of, and reliance on, NERC's continent-wide Reliability Standards. However, during the assessment period, NPCC, ReliabilityFirst, SERC and Texas RE, in addition to WECC, had regional Reliability Standards approved by the Commission. The Regional Entities will continue to develop regional Reliability Standards only to the extent that NERC Reliability Standards do not address a perceived gap in reliability specific to a particular region.

A. Regional Entity Standards Development Processes

Exhibit C to each RDA contains (i) the list of NERC's common attributes of an appropriate RSDP, and (ii) each Regional Entity's current RSDP. In reviewing and approving a Regional Entity's RSDP for inclusion in Exhibit C to the RDA, NERC reviews the RSDP against the common attributes to determine whether the RSDP meets the common attributes. During the assessment period, some of the Regional Entities' RSDPs were revised and approved by NERC and then by the Commission.[3]

The RSDPs include the process that each Regional Entity uses to develop regional Reliability Standards that are proposed to NERC for adoption, and, where applicable, regional variances if the Regional Entity is organized on an interconnection-wide basis. While the RSDPs are not identical, each one must, as noted, satisfy the common attributes that advance the development of regional Reliability Standards consistent with the objective of a uniform reliability program. Among other things, participation in the development of a regional Reliability Standard must be open to all organizations that are directly and materially affected by the bulk power system (BPS) located in the Regional Entity's footprint, with no constraints based on financial capability, technical expertise or membership in the organization. The RSDP must provide for an appropriate

[3] NERC maintains on its website each Regional Entities' RSDP which lists the date of the current version. *See* http://www.nerc.com/pa/Stand/Pages/RegionalStandardsDevelopment.aspx.

balance of interests and the process must be structured so that it may not be dominated by any two interest categories and no single interest category can defeat a matter. All entities with a direct and material interest in the BPS in the Regional Entity may participate in the development of regional Reliability Standards by expressing a position and support for that position. Participating entities then will have that position considered and have the right to appeal the final outcome. The RSDP must also allow for reasonable notice and opportunity for public comment, and include language that states that all actions material to the development of any regional Reliability Standards be transparent.[4]

Based on its review and approval of the Regional Entities' RSDPs for inclusion in the RDAs and the subsequent approval by the Commission, NERC believes that during the assessment period, all of the Regional Entities met the requirements applicable to the ERO in the development of regional Reliability Standards.[5] Specifically, the Regional Entities: (i) demonstrated the ability to develop Reliability Standards that provide for an adequate level of reliability of the BPS; (ii) established rules that assure the independence of the users and owners and operators of the BPS, (iii) took action to ensure balanced decision-making in applicable committees or subordinate organization structures; and (iv) developed rules that provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards. During the assessment period, each Regional Entity fulfilled the obligation to provide an open, fair, balanced, and inclusive process for the development of regional Reliability Standards, as demonstrated by the approval of those processes by NERC and the Commission.

B. Review of Each Regional Entity's Standards Development Activities During the Assessment Period

NERC focuses on the development of its continent-wide Reliability Standards as consistent with the goal of a reliable BPS. The Regional Entities have developed relatively few regional Reliability Standards to address unique situations with specific or more stringent requirements in a particular interconnection or geographic region which the NERC continent-wide standards may not address. Since the Commission issued Order No. 693 in 2007, approving the initial set of NERC continent-wide Operations and Planning Reliability Standards, the Commission has approved a total of only seven regional Reliability Standards submitted by Regional Entities other than WECC.

The Regional Entities are concentrating their standards development resources on working with NERC and stakeholders to develop clear, reasonable, and technically sound continent-wide Reliability Standards in a timely and efficient manner, and to ensure that regional concerns are addressed in the continent-wide Reliability Standards. This approach also avoids duplicating NERC's efforts at the regional level. Barring the existence of a perceived region-specific gap in reliability not addressed by NERC Reliability Standards, the Regional Entities will refrain from developing further regional Reliability Standards.

---

[4] NERC maintains on its website a current overview of regional Reliability Standards under development, with detailed information on the status of the proceeding.
See http://www.nerc.com/pa/Stand/Pages/RegionalReliabilityStandardsUnderDevelopment.aspx.

[5] FPA §215(c)(1) and (2); 16 U.S.C. §824o(c)(1)(2).

To this end, the Regional Entities are actively encouraging awareness and participation by stakeholders in their respective areas in the NERC standards development process, by engaging in educational outreach efforts, and through participation in the NERC Standards Committee (NERC SC) and related subcommittees. The Regional Entities also have standards committees or similar groups at the regional level that analyze the draft ERO standards to determine their quality and effectiveness and evaluate whether the reliability objective is adequate and cost effective, and to provide input on these topics in the NERC standards development process.

The following subsections provide a review of the activities of each Regional Entity in the development of regional Reliability Standards during the assessment period.

1. Florida Reliability Coordinating Council, Inc.

The most recent version of the FRCC RSDP was approved by the Commission on June 12, 2012 and is included as Appendix C to the FRCC RDA. FRCC currently has no FERC-approved regional Reliability Standards or regional variances. During the assessment period, FRCC placed two regional Reliability Standards development projects on hold awaiting the completion of NERC standards development projects, and terminated one project because NERC's continent-wide Reliability Standard was determined to be sufficient for FRCC's reliability needs. Additionally, FRCC's registered ballot body and board of directors approved one project, which was held in abeyance while the adequacy of the NERC continent-wide Reliability Standard was evaluated, and will be withdrawn if it is determined to be sufficient for FRCC's needs. FRCC prefers the development of continent-wide Reliability Standards, but will follow its regional RSDP should a need arise for a more stringent standard or a standard to cover an area that NERC Reliability Standards do not.

2. Midwest Reliability Organization

MRO supports the development of continent-wide Reliability Standards to maintain the reliable operations of the BPS, as opposed to regional Reliability Standards, particularly in the Eastern Interconnection. Therefore, MRO decided during the assessment period to forego the development of regional Reliability Standards. Nevertheless, MRO has a regional RSDP in effect. The most recent revised version of the MRO RSDP was approved by the Commission on June 12, 2013[6] and is included as Appendix C to the MRO RDA. The principal purposes of these amendments to the MRO RSDP include: (i) to provide greater alignment of MRO's standards develop procedures with the NERC *Standard Processes Manual*; (ii) to incorporate a requirement for a review of the MRO RSDP every five years; and (iii) to provide various clarifications to the process development steps in the MRO RSDP. MRO also has a stakeholder-based Standards Committee comprised of subject matter experts (SMEs) in the event there is a need for a regional Reliability Standard in the future.

[6] *North American Electric Reliability Corporation*, Docket Nos. RR13-5-000 (June 12, 2013) (unpublished letter order).

3. Northeast Power Coordinating Council, Inc.

NPCC has developed a revised RSDP that provides a results-based, consensus building approach by which NPCC may develop regional Reliability Standards and Regional Variances proposals to the ERO for adoption, under delegated authority by the Commission and the Canadian Provincial regulatory and/or governmental authorities.

During the assessment period, NPCC developed a disturbance monitoring regional Reliability Standard, PRC-002-NPCC-01, to ensure that adequate disturbance data are available to facilitate event analyses. This NPCC regional Reliability Standard addresses a specific recommendation from the August 14, 2003 Blackout final NERC report regarding the use of time-synchronized data recorders.[7] Substantively, this NPCC regional Reliability Standard outlines the basic requirements for the type, location and capability of equipment to be placed on the BPS to enable analysis of grid disturbances to be conducted effectively and efficiently. This regional Reliability Standard is intended to establish enforceable and uniform requirements for disturbance monitoring throughout the NPCC region. On October 20, 2011, the Commission issued an order approving regional Reliability Standard PRC-002-NPCC-01, the related VRFs and VSLs, implementation plan, and two associated regional definitions in the *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary).

NPCC also developed regional Reliability Standard PRC-006-NPCC-1, Automatic Underfrequency Load Shedding, during the assessment period. The purpose of PRC-006-NPCC-1 is to provide a regional Reliability Standard that ensures the development of an effective regional automatic underfrequency load shedding (UFLS) program in order to preserve the security and integrity of the BPS during declining system frequency events, in coordination with the NERC UFLS Reliability Standard characteristics. Further, this NPCC regional Reliability Standard creates a region-wide and fully coordinating single set of UFLS requirements that will serve as a last resort to preserve the BPS during a major system failure that may cause a system frequency collapse. On February 21, 2013, the Commission issued Order No. 775 approving regional Reliability Standard PRC-006-NPCC-1, the related VRFs and VSLs, implementation plan, and the effective dates proposed by NERC.[8]

4. ReliabilityFirst Corporation

ReliabilityFirst has an approved RSDP in place as Exhibit C to its RDA. ReliabilityFirst no longer develops regional Reliability Standards, in order to avoid duplication with the NERC continent-wide Reliability Standards. However, ReliabilityFirst has proved its ability to develop regional Reliability Standards, as shown by its development of regional Reliability Standard BAL-502-RFC-02, Planning Resource Adequacy Analysis, Assessment and Documentation, during the assessment period. The purpose of this standard and associated definitions is to establish common criteria based on the principle of "one day in ten years" loss of load expectation for the analysis,

[7] *See Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* available at: http://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx.

[8] *Regional Reliability Standard PRC-006-NPCC-1 – Automatic Underfrequency Load Shedding*, Order No. 775, 142 FERC ¶ 61,128 (2013).

assessment, and documentation of resource adequacy for load in the ReliabilityFirst footprint and to establish requirements for planning coordinators in the ReliabilityFirst region regarding resource adequacy assessment, a subject matter not addressed in NERC's continent-wide Reliability Standards. The Commission approved regional Reliability Standard BAL-502-RFC-02 and related filings in an order issued on March 17, 2011, directing that the regional Reliability Standard and associated VSLs, VRFs, and definitions become effective on the date of that order.[9]

5. SERC Reliability Corporation

The SERC RSDP, included in Exhibit C to the SERC RDA, defines the process for the development, revision, reaffirmation, and withdrawal of SERC regional Reliability Standards. The SERC RSDP requires any proposed SERC regional Reliability Standard to be more stringent than a continent-wide Reliability Standard, whether the regional Reliability Standard addresses matters that the continent-wide Reliability Standard does not or the regional Reliability Standard is necessitated by a physical difference in the BPS within the SERC region. SERC regional Reliability Standards are required to provide for as much uniformity as possible with continent-wide Reliability Standards.

SERC has one Commission-approved regional Reliability Standard, PRC-006-SERC-01, Automatic Underfrequency Load Shedding Requirements. The purpose of this standard and the associated VSLs and VRFs is to establish consistent and coordinated requirements for the design, implementation, and analysis of automatic UFLS schemes among all applicable entities within the SERC region so that distribution providers and transmission owners may effectively mitigate the consequences of an underfrequency event. The standard effectively mitigates the consequences of an underfrequency event while accommodating differences in system transmission and distribution topology among SERC planning coordinators. The Commission approved regional Reliability Standard PRC-006-SERC-01 in Order No. 772 issued on December 20, 2012.[10]

SERC currently is not developing any additional regional Reliability Standards because the continent-wide NERC Reliability Standards are presently adequate for the SERC region.

6. Southwest Power Pool Regional Entity

SPP RE has a RSDP in place and included in Exhibit C to its RDA. During the assessment period, SPP RE developed a substantially revised RSDP. A principal objective of the revisions was to confirm the SPP RE RSDP more closely to the NERC *Standard Processes Manual*. The revised SPP RE was approved by NERC and filed with the Commission for approval in December 2013, and was approved by the Commission in an order issued January 31, 2014.[11]

---

[9] *Planning Resource Adequacy Assessment Reliability Standard*, *Final Rule*, Order No. 747, 134 FERC ¶ 61,212 (2011).

[10] *Regional Reliability Standard PRC-006-SERC-01—Automatic Underfrequency Load Shedding Requirements*, 141 FERC ¶ 61,243 (2012).

[11] *Revised Southwest Power Pool Regional Entity Standards Development Process Manual*, Docket No. RR14-1-000 (January 31, 2014) (unpublished letter order).

SPP RE is not actively developing any Reliability Standards at this time. SPP RE supports development of continent-wide Reliability Standards at NERC. Any regional Reliability Standard developed by SPP RE will go beyond, add detail to, or cover matters not addressed in the NERC Reliability Standards.

During the assessment period, SPP RE developed proposed regional Reliability Standard PRC-006-SPP-1, Automatic Underfrequency Load Shedding Requirements. On November 7, 2012, the NERC Board of Trustees (NERC Board) approved the proposed standard. The purpose of the proposed standard was to ensure the development and implementation of an effective automatic UFLS program for entities in the SPP RE region in order to preserve the security and integrity of the BPS during declining system frequency events. The regional Reliability Standard was designed to develop, coordinate and document requirements for automatic UFLS programs to arrest declining frequency and assist recovery of frequency following underfrequency events in the SPP RE region. On April 26, 2013, NERC submitted the proposed standard to the Commission for approval,[12] but on December 11, 2013, NERC submitted a Notice of Withdrawal of the petition because, due to the creation and pending approval of NERC Reliability Standard PRC-024-1, changes to PRC-006-SPP-01 could be needed to account for generator trip zones that may differ between proposed regional Reliability Standard PRC-006-SPP-01 and NERC Reliability Standard PRC-024-1.[13]

7. Texas Reliability Entity, Inc.

Texas RE has a RSDP in effect and included in Exhibit C to its RDA, and has used its RSDP to develop Texas RE regional Reliability Standards. Texas RE has developed one major regional Reliability Standard, BAL-001-TRE-1, Primary Frequency Response in the ERCOT Region, and two minor regional standards (CIP-001-2a regional variance and IRO-006-TRE-1). The major regional Reliability Standard, BAL-001-TRE, was designed to maintain Interconnection steady-state frequency within defined limits in the ERCOT region; its purpose is to provide a regional Reliability Standard for the ERCOT Interconnection related to the maintenance of steady-state frequency within defined limits by balancing real power demand and supply in real-time. This proposed standard was developed to establish and maintain adequate frequency response in the ERCOT region by ensuring prompt and sufficient frequency response from resources to stabilize frequency during changes in the system generation-demand balance. Because there are physical differences present in the ERCOT system, a more stringent means of assuring frequency response performance was needed than that provided by the continent-wide NERC Reliability Standard. The Commission unconditionally approved the proposed standard by letter order on January 16, 2014 as well as the staggered implementation date requested by NERC

[12] Available at: http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/FINAL_Petition%20PRC-006-SPP-01_complete.pdf.

[13] *Notice of Withdrawal of the Joint Petition for Approval of Proposed Regional Reliability Standard PRC-006-SPP-01 (Underfrequency Load Shedding*), Docket No. RD13-9-000 (December 11, 2013), available at: http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final_Notice_of_Withdrawal_of_PRC-006-SPP-01_20131211.pdf.

and Texas RE.[14] (The Commission concurrently approved NERC Reliability Standard BAL-003-1, which addresses frequency response on a continent-wide basis.)

8. Western Electricity Coordinating Council

WECC uses the Commission-approved WECC RSDP to develop regional Reliability Standards along with Regional Criteria and Regional Business Practices. WECC develops Regional Criteria and Regional Business Practices to improve the functioning and efficiency of the Western Interconnection. This combination provides a forum for addressing system-wide issues and enables effective oversight to promote reliable operation of the Western Interconnection.[15]

As of the end of the assessment period, WECC had the following eight Commission-approved WECC regional Reliability Standards in effect.

- **FAC-501-WECC-1 (Transmission Maintenance)**

FAC-501-WECC-1 requires, for specified transmission paths, a highly detailed maintenance and inspection plan for all transmission and substation equipment components. This ensures that certain transmission owners of transmission paths identified by a table titled "Major WECC Transfer Paths in the Bulk Electric System" (including associated facilities) have a transmission maintenance and inspection plan (TMIP); and perform and document maintenance and inspection activities in accordance with the TMIP.[16]

- **VAR-002-WECC-1 (Automatic Voltage Regulators)**

NERC continent-wide Reliability Standard VAR-002-1a requires that generator operators operate a generator connected to the interconnected transmission system in automatic voltage control mode unless the operator has notified the transmission operator. WECC regional Reliability Standard VAR-002-WECC-1 adds an additional responsibility for compliance in the WECC region, requiring all synchronous generators within the WECC region to have their voltage regulators in service at all times, with exceptions only for specified circumstances.[17]

- **VAR-501-WECC-1 (Power System Stabilizer)**

NERC continent-wide standard VAR-002-1a requires that a generator operator notify its transmission operator when it removes power system stabilizers (PSS) from service, but does not limit the amount of time for operating generators without PSS in service. WECC regional

[14] *North American Electric Reliability Corporation*, Docket No. RD13-12-000 (January 16, 2014) (unpublished letter order).

[15] While WECC currently maintains Regional Business Practices, all of these fit within the description of Regional Criteria contained in the NERC ROP §313 (Other Regional Criteria, Guides, Procedures, Agreements, etc.). WECC is currently undertaking efforts to re-categorize its Regional Business Practices as Regional Criteria so that going forward WECC will no longer create or maintain items called Regional Business Practices.

[16] *Version One Regional Reliability Standards for Facilities Design, Connections, and Maintenance; Protection and Control; and Voltage and Reactive*, Order No. 751, 135 FERC ¶ 61,061 (2011).

[17] *Id.*

Reliability Standard VAR-501-WECC-1 is more stringent than the NERC Reliability Standard; it ensures that synchronous generators shall be kept in service in order to ensure that the generator provides the proper damping to maintain system stability when generation and transmission outages occur, and an exception is provided only for very specific conditions and for a cumulative time limit per quarter.[18]

- **PRC-004-WECC-1 (Protection System and Remedial Action Scheme Misoperation)**

WECC regional Reliability Standard PRC-004-WECC-1 sets a specific timeframe for the analysis and mitigation of all transmission and generation protection system and remedial action scheme misoperations on major WECC Transfer Paths. This standard augments requirements for certain entities found under NERC continent-wide Reliability Standards PRC-003-1 and PRC-004-1.[19]

- **IRO-006-WECC-2 (Qualified Transfer Path Unscheduled Flow Relief)**

The purpose of WECC regional Reliability Standard IRO-006-WECC-2 is to provide a regional standard that specifies the mitigation of transmission overloads due to unscheduled flow on qualified transfer paths. The standard modifies IRO-006-WECC-1 to correct references, wording, and format issues that would update the standard and bring it into compliance with NERC's drafting conventions for Reliability Standards. On December 20, 2013, NERC and WECC submitted a joint petition to the Commission seeking approval of IRO-006-WECC-2 along with an associated implementation plan and new or revised definitions in the NERC Glossary. On May 13, 2014, FERC issued a letter order approving IRO-006-WECC-2.[20]

- **BAL-004-WECC-02 (Automatic Time Error Correction)**

During the assessment period, WECC revised its regional Reliability Standard BAL-004-WECC-01, Automatic Time Error Correction, resulting in BAL-004-WECC-02. The revision was developed in response to a directive from the Commission in Order No. 723 to modify regional Reliability Standard BAL-004-WECC-01 to clarify certain terms used therein.[21] The purpose of the revised regional Reliability Standard is to maintain Interconnection frequency and to ensure that time error corrections and primary inadvertent interchange playback are effectively conducted in a manner that does not adversely affect the reliability of the Interconnection. On August 20, 2013, NERC and WECC submitted a joint petition to the Commission seeking approval of BAL-004-WECC-02 along with an associated implementation plan, new definitions in the NERC Glossary, and a regional variance to BAL-001-1.[22] The Commission unconditionally approved

[18] *Id.*

[19] *Id.*

[20] *North American Electric Reliability Corporation*, Docket No. RD14-9-000 (May 13, 2014) (unpublished letter order).

[21] *Western Electricity Coordinating Council Regional Reliability Standard Regarding Automatic Time Error Correction*, Order No.723, 127 FERC ¶ 61,176 (2009).

[22] Available at: http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20BAL-004-WECC-02%20and%20BAL-001-1.pdf.

the revised WECC regional Reliability Standard on October 16, 2013, and it became effective as of the date of the order.[23]

- **TOP-007-WECC-1 (System Operating Limits)**

The primary purpose of WECC regional Reliability Standard TOP-007-WECC-1 is to implement the directives in Order No. 693 approving NERC Reliability Standard TOP-007-0, and related concerns, by ensuring that actual flows and associated scheduled flows on major WECC transfer paths do not exceed system operating limits for more than 30 minutes. The Commission approved TOP-007-WECC-1 in an order issued April 21, 2014.[24] In approving TOP-007-WECC-1, the Commission ordered WECC to address the concern regarding the need for WECC to develop a means to provide consistency and transparency when making revisions to the list of major transmission paths instead of the WECC transfer path table and to modify the associated VRFs and VSLs to adequately reflect the size and scope of the actual violation. Any future modifications will be handled through the established standards process.

- **BAL-002-WECC-2 (Contingence Reserve)**

On March 25, 2009, NERC submitted to the Commission for approval WECC regional Reliability Standard BAL-002-WECC-1, Contingency Reserves, but in 2010, the Commission issued Order No. 740 wherein it remanded this standard based on concerns that WECC had not provided adequate technical support to demonstrate that the requirements of the proposed regional Reliability Standard are sufficient to ensure the reliable operation of the BPS within WECC.[25] The purpose of proposed regional Reliability Standard BAL-002-WECC-2 is to provide a regional Reliability Standard that specifies the quantity and types of contingency reserve required to ensure reliability under normal and abnormal conditions. In response to the Commission's directives in Order No. 740, WECC developed modifications to proposed regional Reliability Standard BAL-002-WECC-1. On April 12, 2013, NERC filed a petition with the Commission to approve regional Reliability Standard BAL-002-WECC-2, Contingency Reserve, and associated VRFs and VSLs. On November 21, 2013, the Commission issued Order No. 789 approving WECC regional Reliability Standard BAL-002-WECC-2, the associated VRFs, VSLs, implementation plan, the effective date proposed by NERC and WECC, and the retirement of BAL-STD-002-0 and two WECC regional definitions from the NERC Glossary. In that order, the Commission directed NERC to submit an informational filing after the first two years of implementation of the regional

[23] *North American Electric Reliability Corporation*, Docket No. RR13-11-000 (October 16, 2013) (unpublished letter order).

[24] *Version One Regional Reliability Standard for Transmission Operations*, 135 FERC ¶ 61,062 (2011).

[25] *Version One Regional Reliability Standard for Resource and Demand Balancing*, Order No. 740, 133 FERC ¶ 61,063 (2010).

Reliability Standard that addresses the adequacy of contingency reserve in the Western Interconnection.[26]

II. COMPLIANCE MONITORING AND ENFORCEMENT

The RDAs set forth the delegated authorities and responsibilities of the Regional Entities with respect to compliance monitoring and enforcement.[27] In Exhibit D to each RDA, each Regional Entity adopts the uniform NERC Compliance Monitoring and Enforcement Program (CMEP; Appendix 4C to the NERC ROP) in its entirety, adopts the uniform NERC CMEP with stated differences, or adopts a separate CMEP (however, the CMEP of a Regional Entity that has deviations from or is different than the uniform CMEP must comply with the requirements of the RDA and with §403 of the NERC ROP).

The RDA gives the Regional Entities delegated authorities and responsibilities to, among other things, maintain a program of proactive monitoring and enforcement of compliance with Reliability Standards in accordance with the CMEP and the annual NERC CMEP Implementation Plan (IP);[28] report to NERC any possible violations, alleged violations or confirmed violations of Reliability Standards and the dispositions thereof; maintain violations as nonpublic until the matter is filed with the Commission as a Notice of Penalty (NOP); conduct, in a confidential manner, compliance investigations of possible violations and alleged violations; and maintain a conflict of interest policy to ensure the integrity and independence of the Regional Entity's CMEP, including the integrity and independence of the persons or decision-making bodies making final determinations in compliance enforcement actions.

In addition, the RDAs give the Regional Entities responsibilities with respect to the registration of owners, operators and users of the BPS as entities responsible to comply with mandatory Reliability Standards; and with respect to the certification of certain registered entities to perform certain reliability functions.[29]

Section 4 of the RDAs obligates the Regional Entity to comply with, among other things the NERC ROP. Provisions of the ROP applicable to compliance monitoring and enforcement functions, include, in addition to the uniform CMEP, the following ROP sections and appendices: §400, Compliance Enforcement (§403 sets forth required attributes of Regional Entity CMEPs), §500, Organization Registration and Certification, Appendix 4B, *Sanction Guidelines*, Appendix 5A, *Organization Registration and Certification Manual*, Appendix 5B, *Statement of Compliance Registry Criteria*, and Appendix 5C, *Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of Bulk Electric System* (effective July 1, 2014).

---

[26] *Regional Reliability Standard BAL-002-WECC-2 – Contingency Reserve*, Order No. 789, 145 FERC ¶ 61,141 (2013).

[27] Generally, each Regional Entity's responsibilities with respect to compliance monitoring and enforcement are set forth in §6 of its RDA.

[28] Available at: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx.

[29] These provisions are generally found in §7 of the RDAs.

In this §II, NERC describes and evaluates the Regional Entities' performance during the assessment period separately with respect to the three major components of their compliance monitoring and enforcement responsibilities: Organization Registration and Certification (ORC) (§II.A below), Compliance Monitoring (§II.B below), and Compliance Enforcement (§II.D below). In addition, Compliance Investigations are discussed separately in §II.C.

A. Organization Registration and Certification

NERC is ultimately responsible for devising the criteria that determine which BPS users, owners and operators are subject to approved Reliability Standards, and for maintaining the NERC Compliance Registry of organizations subject to Reliability Standards. In carrying out these responsibilities, NERC relies on the Regional Entities to apply and implement registration and certification criteria as part of the ORC program. Pursuant to the RDAs and §500 and Appendices 5A (*Organization Registration and Certification Manual*) and 5B (*Statement of Compliance Registry Criteria*) of the NERC ROP, the Regional Entities are responsible for the following registration and certification tasks:

Registration

(1) Providing NERC with timely and accurate information relating to registrations and registered entities to enable NERC to maintain a registration database that is accurate and up-to-date;

(2) Collecting data on and mapping BPS facilities and those facilities that have a material impact on the BPS within each Regional Entity's defined regional boundaries;[30]

(3) Approving or disapproving entity registration applications;

(4) Notifying NERC of each coordinated functional registration (CFR) and joint registration organization (JRO) that the Regional Entity accepts; and

(5) Maintaining a list of active CFRs and JROs.

Certification

(1) Verifying that all reliability coordinators, balancing authorities, and transmission operators (i.e., the reliability entities required to be certified to perform their reliability functions) meet the registration requirements of ROP §501.1.4;

(2) Reviewing entity certification applications for completeness and notifying NERC of applications;

[30] Each Regional Entity's boundaries are defined in Exhibit A to its RDA.

(3) Evaluating the competency of entities requiring certification to meet the NERC certification requirements;

(4) Establishing certification procedures, including (i) evaluation processes, schedules, and deadlines; (ii) expectations of the applicants and all entities participating in the process; and (iii) requirements for certification team members;

(5) Approving or denying certification team recommendations and notifying the entity and NERC of the decision; and

(6) Providing leadership to the certification team throughout the certification process.

NERC and the Regional Entities are working towards two goals for registration. First, they recognize the need for consistency between and among Regional Entities and across the continent in the application of the criteria for registering entities. Second, any entity whose facilities or operations are reasonably deemed material to the reliability of the BPS will be registered, irrespective of other considerations.

During the assessment period, the NERC ORC program increased its efforts regarding consistency and transparency. The ORC program developed and posted on NERC's website eight registration and 38 certification templates to be used by the Regional Entities and industry. The ORC program worked with the Certification and Registration Working Group to develop a prototype common registration form (CRF). The CRF requires the provision of information related to entity relationships, and will thereby provide greater assurance that all entities that should be registered are in fact registered. Further, since consistent forms are now used by each Regional Entity, entities that need to register in multiple Regional Entities should find the registration process more streamlined.

During the assessment period, the ERO experienced an incremental increase in the number of registered entities. As of January 30, 2009, NERC and the Regional Entities had registered a total of 1,860 entities for a total of 4,482 reliability functions. As of May 1, 2014, NERC and the Regional Entities have registered 1,920 entities for 4,774 reliability functions. Further, a review of the registration activity by Regional Entity shows a significant number of registrations and deactivations in four Regional Entities (NPCC, ReliabilityFirst, Texas RE, and WECC) for the following three functions: (i) generator owners; (ii) generator operators; and (iii) purchasing-selling entities. This trend is in part attributed to corporate ownership changes. The registration and deactivation activity in the remaining Regional Entities (FRCC, MRO, SERC, and SPP RE) was minimal.

The JRO and CFR mechanisms are important components of the ORC program. These vehicles are used to define the responsibilities and accountability among entities separately registered for the same function. During the assessment period, revisions to NERC ROP §507 and the addition of §508, approved by the Commission on June 10, 2010, clarified the operations of

both types of registration.[31] Specifically, revised ROP §507 allows an entity to 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. The registering entity thereby accepts on behalf of such members or related entities all compliance responsibility for that function or those functions including all reporting requirements. NERC ROP §508 allows multiple entities to register using a CFR for one or more Reliability Standard(s) or for one or more requirements or sub-requirements with particular Reliability Standard(s) applicable to a specific function. The CFR is the complete registration for each entity, with each entity taking full compliance responsibility for those Reliability Standards or requirements or sub-requirements applicable to the CFR.

Many of the registered entities that use the NERC ROP §507 process are cooperatives, municipalities, and other publicly-owned or member-owned utilities. As of May 1, 2014, a total of 34 JROs are registered; however, NPCC, SPP RE, and WECC have not registered any JROs.[32] Since its initial implementation, use of the joint registration option has been fairly static, with few additional entities registering as JROs or changing their JRO status. Many registered entities have, however, taken advantage of the opportunity to coordinate their registered functions pursuant to NERC ROP §508. There are a total of 44 CFR agreements, with FRCC being the only Regional Entity in which there is not a coordinated registration. Some of these coordinated registration agreements cross Regional Entity boundaries.

As the above discussion indicates, the registration and certification processes have been fairly stable during the assessment period in terms of the numbers of entities registered and certified. However, NERC has identified several initiatives or opportunities for improvement in how the Regional Entities perform their registration and certification functions. The first initiative is in the area of multi-regional registered entities (MRREs). MRREs are entities that own or operate BES facilities in two or more Regional Entity footprints. MRREs pose a consistency challenge because they are subject to multiple compliance programs. To address this challenge, during the assessment period, several Regional Entities partnered to coordinate their compliance and enforcement efforts with respect to MRREs. In particular, they developed a "lead region" model in which the involved Regional Entities select one of them to lead the compliance and enforcement efforts for a given MRRE. The purpose of this MRRE initiative is to describe the coordinated CMEP processes that will be used by NERC and the Regional Entities for a subset of registered entities that are registered in multiple Regional Entities and volunteer for this program. The MRRE process provides the opportunity for these entities to request to be accountable to one Compliance Enforcement Authority (CEA). The coordinated MRRE process provides for increased efficiencies in compliance resource allocation for NERC, the Regional Entities, and the registered entities while, maintaining the reliability of the BPS.

[31] *North American Electric Reliability Corporation*, Docket No. RR10-8-000 (June 10, 2010) (unpublished delegated letter order).

[32] *See* the JRO member listing Excel spreadsheet available at: http://www.nerc.com/pa/comp/Pages/Registration-and-Certification.aspx.

A second area of opportunity for improvement is the efficiency with which a Regional Entity is able to process registration activation and deactivation requests. This initiative is part of the risk-based registration effort described in further detail in the *Overview of NERC Activities and Accomplishments in the Five-Year Period*.

B. Compliance Monitoring

1. NERC Oversight of Regional Entity Compliance Monitoring Activities

NERC's oversight of and involvement with the Regional Entities' compliance monitoring activities is ongoing and continuous. Although this document is a five-year assessment of the Regional Entities' performance of specified functions, including compliance monitoring, NERC's ongoing oversight of and involvement with the Regional Entities' compliance monitoring activities provides a significant component of the informational and observational basis for NERC's evaluation of the Regional Entities in this area. This §II.B.1 provides an overview of NERC's oversight activities for the Regional Entity compliance monitoring programs, which is one of the key information and observation sources for NERC's assessment of the Regional Entities' performance.

At the start of the assessment period, the Regional Entity audit program consisted of Agreed-Upon Procedures (AUP) developed by NERC in collaboration with an independent third-party. The AUP oversight program operated on a three-year audit cycle.

In 2010, NERC restructured its Regional Entity oversight program. Based on NERC's observations of the audits completed under the AUP oversight program, NERC determined that conducting an AUP audit once every three years did not provide the desired level of qualitative evaluation of effectiveness of the programs within and across the Regional Entities. As a result, NERC refocused the Regional Entity audit program to move to an on-going and simultaneous evaluation of performance-based objectives to gauge the effectiveness of the Regional Entities' CMEPs. NERC staff utilized the findings, exceptions and lessons learned from the initial AUP program engagements to develop processes and procedures for the restructured audit program. The restructured Regional Entity oversight program provides for continuous oversight of each Regional Entity in focused, discrete time intervals that allows NERC to provide immediate feedback to Regional Entity compliance staff. This feedback enables Regional Entity staff to improve the consistency of its compliance processes and their application in a timelier manner.

Under NERC's current oversight model, NERC Audit Assurance and Oversight (AAO) staff and the Regional Entities conduct compliance monitoring of registered entities primarily through regular and scheduled compliance audits and random spot checks. Each Regional Entity has a compliance monitoring program that includes all the compliance monitoring methods specified in the uniform NERC CMEP, Appendix 4C to the NERC ROP.[33] NERC is responsible

[33] The compliance monitoring methods are compliance audits, self-certification, spot checks, investigations, self-reports, periodic data submittals, and complaints. *See* CMEP §3.0 (Compliance Monitoring Processes). The Regional Entities review self-certifications for all registered entities at least once annually. Some Regional Entities also require monthly self-certifications for certain Reliability Standards and requirements. Periodic data submittals occur on an ongoing basis, with certain information due to the Region Entity on a monthly basis, and other data due on a quarterly basis.

for oversight and monitoring of the Regional Entities' compliance monitoring activities, which must be carried out in accordance with the NERC ROP and the terms of the RDAs. NERC uses the following tools (each of which is described in the subsections below), to carry out its oversight and monitoring of the Regional Entities' activities:

(1) An annual review of Regional Entity CMEP IPs for approval and posting, as well as an annual review of each Regional Entity's CMEP for incorporation into the ERO's annual CMEP report;

(2) Annual assessments of compliance monitoring for selected Reliability Standards for consistency of approach through the Key Reliability Standard Spot Check (KRSSC) program;

(3) Oversight audits of selected registered entity compliance audits performed by Regional Entities, as well as periodic assessments of Regional Entity auditor capabilities;[34] and

(4) NERC training for Regional Entity CMEP personnel.

The oversight engagement of NERC AAO staff and Critical Infrastructure department (CID) staff, as well as NERC Training and Education program staff, increased over the assessment period, thereby providing an enhanced view of the Regional Entities' performance. These oversight activities are further discussed below.

a. Annual CMEP Implementation Plan

As part of NERC's annual oversight, each Regional Entity is required to develop and submit to NERC, for approval, an annual Regional Entity CMEP IP in accordance with Appendix 4C of the ROP. In its IP, each Regional Entity identifies which Reliability Standards and requirements it will actively monitor, evaluate, report, sanction and appeal during the period covered by the IP (both those Reliability Standards and requirements that NERC specifies shall be monitored, and any additional Reliability Standards and requirements the Regional Entity proposes to monitor). These IPs are submitted to NERC on the schedule established by NERC, generally on or about October 1 of the preceding year. NERC previously published the Regional Entity IPs, and its own IP, as separate documents; however, beginning with the 2014 IPs, NERC now combines its IP and the Regional Entity IPs into a single document.[35]

Each Regional Entity must also report annually to NERC regarding how the Regional Entity carried out its delegated compliance monitoring and enforcement authority in the previous year, the effectiveness of its CMEP, and changes it expects to make to correct any deficiencies

[34] Due to ongoing restructuring and transitioning pursuant to the Reliability Assurance Initiative (RAI), these compliance activities ceased in early 2013, but are scheduled to resume in the fourth quarter of 2014.

[35] *See ERO Compliance Monitoring and Enforcement Program 2014 ERO CMEP Implementation Plan*, version 1.1, available at: http://www.nerc.com/pa/comp/Resources/ResourcesDL/2014_ERO_CMEP_IP_v1.1_%2804012014%20posting%29.pdf.

identified. Each Regional Entity provides its annual report on a schedule established by NERC, generally on or about February 15 of the following year. The Regional Entities' annual reports, along with Regional Entity responses to an annual NERC CMEP survey, are used to prepare NERC's annual CMEP report.

b. Key Reliability Standard Spot Check Program

The KRSSC program focuses on issues that have the highest potential to result in major impacts to the BPS. Through the KRSSC program, NERC compares and contrasts the procedures Regional Entities use when auditing a set of high-risk, high-impact or frequently violated Reliability Standards. The KRSSC focuses on the observation activities of the Regional Entity compliance audit team during pre-audit work and on-site audit work, as these are the primary audit observation procedures used in gathering and analyzing evidence. Through this program, NERC seeks to identify issues that Regional Entity audit teams experience when evaluating compliance with selected Reliability Standards, as well as areas in Regional Entity audit evaluations for which additional guidance may be needed to improve evaluation processes or to promote consistency in evaluations. The objective of the KRSSC program is not to identify a minimum acceptable auditing approach or to determine the best practices for determining compliance; rather, the emphasis is upon enhancing consistency and improving auditing approaches. The KRSSC process addresses a need, which was identified early in the assessment period, to increase opportunities to share best practices among Regional Entities.

For issues identified during KRSSCs, NERC provides Regional Entities with overall recommendations and guidance as needed regarding how to remediate issues and to enhance consistency across all the Regional Entities. Regional Entities also receive individualized information through confidential appendices. NERC audit staff holds teleconferences with each Regional Entity to discuss both Regional Entity-specific results and cross-Regional Entity results. NERC's proposed best practices are intended to apply to enhance elements of the Regional Entities' auditing practices and approaches. While NERC typically derives the KRSSC recommendations and best practices from review of the auditing practices for specific Reliability Standards, many of the audit practices and approaches identified have broader applicability to other Reliability Standards.

During the assessment period, NERC conducted three KRSSCs with the Regional Entities. The three KRSSCs focused on the following Reliability Standards: EOP-005-1, PRC-005-1, CIP-001, and EOP-004 (the latter two were evaluated jointly). For each KRSSC, two registered entity compliance audits from each Regional Entity were selected based upon the potential and actual risk posed to the BPS by the audited registered entities as well as the completion date of the audits. As part of its evaluation, NERC AAO staff examined the credentials, resource levels and audit implementation methods of the individual Regional Entities in conducting their compliance audits. NERC evaluated the Regional Entities separately during this process; however, in an effort to increase consistency, NERC communicated any departure from best practices to the individual Regional Entities.

c. Oversight Audits of Regional Entity Audits of Registered Entities

NERC conducts oversight audits of selected registered entity audits being performed by Regional Entities. The purpose of an oversight audit is to determine whether the Regional Entity conducted its compliance audit and related tasks in accordance with the requirements of the NERC ROP, the CMEP and the RDAs. NERC staff members observe a Regional Entity compliance audit of a registered entity on-site at the registered entity or at the relevant Regional Entity's office. A Regional Entity audit of Operations and Planning Reliability Standards is observed by NERC AAO staff, while a Regional Entity audit of Critical Infrastructure Protection (CIP) Reliability Standards is observed by NERC CID staff. The Commission may also assign auditors to participate by observing the pre-audit activities and the on-site audit, although Commission participation is not specifically a component of the NERC oversight audit. Following the oversight audit, NERC AAO staff identifies best practices and recommendations for the Regional Entity.

d. NERC Training Activities for Regional Entity Compliance Staff

Early in the assessment period, NERC and the Regional Entities identified training, education and communication as key initiatives for compliance monitoring. As a result, during the assessment period, training opportunities for Regional Entity CMEP staff (as well as for registered entities) have been increased.[36]

Training of CEA staff is a central component of NERC's compliance monitoring oversight of Regional Entities. NERC's training programs for compliance auditors are based upon the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards (GAGAS) for performance audits. GAGAS is primarily used by auditors of government entities and entities that receive government grants and other funding. All of NERC's CEA training material is reviewed and updated based on changes to GAGAS, the CMEP, the NERC ROP, and internal procedures, as well as feedback from experience.

From 2009 to 2013, NERC conducted the following training sessions for ERO compliance auditors:

- 18 auditor workshops and webinars
- 11 audit team leader (ATL) training sessions
- 3 CIP training sessions
- 12 compliance investigation training sessions

In addition, NERC made a total of 25 presentations at Regional Entity compliance workshops, including 18 presentations in 2012. Examples of topics presented in the auditor workshops and webinars during this period included:

- Fundamentals of NERC Compliance Audits
- GAO Auditing Standards
- Audit Scoping

[36] Regional Entity training activities provided for registered entities are described in §II.B.2.a below and in the individual Regional Entity assessments in §II.B.2.b below.

- Auditor Checklist and Handbook
- Gathering Quality Evidence
- Sampling/Random Sampling Techniques
- Quality Audit Documentation
- Conducting Performance Audits
- Find, Fix, Track, and Report (FFT) Process
- Internal Controls
- CIP Reliability Standards
- Critical Asset Identification and CIP-002 Sufficiency Reviews
- CIP Compliance

2. NERC Evaluation of Regional Entity Compliance Monitoring Programs

Subsection 2.a below discusses, on a collective basis, the Regional Entities' training and education programs for registered entity personnel. Each Regional Entity maintains, for organizational, budgeting and accounting purposes, a Training, Education, and Operator Certification program separate from its Compliance Monitoring and Enforcement and Organization Registration and Certification program. For purposes of this assessment, the Regional Entities' training, education and outreach activities are being discussed and assessed as part of the evaluation of their compliance programs because these activities are heavily focused on compliance-related topics. Subsection 2.b then evaluates each Regional Entity's compliance monitoring program on an individual basis.

a. Regional Entity Training, Education, and Outreach Programs for Registered Entity Personnel

The RDAs provide that the Regional Entity "may provide training and education to registered entities, as it deems necessary, in support of its performance of delegated functions and related activities under this Agreement."[37] Providing training for registered entities is critical to reliability for the following reasons:

(1) To ensure that registered entities understand what is required to comply with Reliability Standards, with a particular focus on the most frequently violated Reliability Standards;

(2) To equip registered entities with the tools to identify risks to reliability; and

(3) To help registered entities establish compliance programs that systematically detect, report, correct and prevent risks to reliability and therefore reduce violations.

The Regional Entities offer two types of training opportunities for registered entities. First, each Regional Entity conducts training and outreach initiatives with registered entities through its

[37] This provision is generally found in §7(e) of the RDAs.

Training, Education, and Operator Certification program. Under this program, Regional Entities offer NERC-approved continuing education program courses and activities necessary to maintain one's status as a NERC-certified system operator. The target audience of the program is BPS operating personnel, including system operations personnel, operations support personnel (engineering and information technology), supervisors and managers, and training personnel. NERC's Personnel Certification and Continuing Education staff and Training and Education staff support the Regional Entities' efforts in this area. Second, Regional Entities conduct supplemental compliance and enforcement training for registered entities, typically through workshop events. For the supplemental compliance and enforcement training and outreach for registered entities, the Regional Entity has the discretion to choose the content, delivery method, and location of such training.

Feedback from registered entities regarding the Regional Entity training workshops has been very positive, and participants have sought coverage of additional topics. To address requests from the industry for an increased level of compliance information as well as for enhanced CMEP transparency, many Regional Entities have committed more resources to training in order to engage in additional training, education and outreach activities. These increased activities have included additional workshops, newsletters to industry, and other direct communications. Much of the information covered by these increased outreach and communication activities takes the form of lessons learned.

b. Assessments of the Individual Regional Entities

As an overall evaluation, during the assessment period, the Regional Entities made meaningful progress in improving their compliance monitoring programs and their audit practices and procedures consistent with the requirements of the ROP (specifically, the CMEP, Appendix 4C) and the RDAs. Overall, the Regional Entities worked diligently to plan and complete their scheduled compliance audits during the assessment period. NERC's oversight of the Regional Entity compliance programs shows that the Regional Entities are meeting the baseline requirements of the ROP and the RDAs. NERC's oversight has also shown that there continue to be varying compliance monitoring practices across the ERO.

NERC has three main objectives for the continued evolution of the compliance monitoring program. First, the Regional Entities are revising their existing practices to better align with risk using generally accepted audit practices. Second, NERC and the Regional Entities have developed a standardized audit checklist to ensure consistent conduct of audits across the ERO. Third, NERC, in conjunction with the Regional Entities, has developed competency guidelines for compliance monitoring staff and is developing training to accompany the competency guidelines. Through RAI, the ERO Enterprise is moving away from a one-size-fits-all approach for monitoring registered entities to a compliance oversight approach that considers risk and the controls registered entities have established around compliance with Reliability Standards.

NERC AAO staff has collaborated with the Regional Entities to develop RAI pilot projects conducted by several Regional Entities. Some Regional Entities volunteered to establish pilot programs to test strategies regarding: (i) entity risk assessment; (ii) management controls (identification and testing methodology); (iii) audit scope linked to risk; and (iv) data gathering techniques (interviews, surveys, etc.) and the process for disseminating the pilot across the ERO.

The participating Regional Entities then conducted the pilot programs with registered entities within their respective footprints. Each participating Regional Entity used varying techniques with the goal of establishing a repeatable risk assessment and internal control review process, tied to Reliability Standards that could be replicated by non-participating Regional Entities.

In the individual Regional Entity assessments that follow, NERC examines how the Regional Entities satisfied the baseline requirements of the ROP and RDAs in executing their compliance monitoring responsibilities during the assessment period. NERC's review encompassed two major areas: (i) department structure and staffing, and (ii) compliance monitoring tools and audit planning. With respect to the first area, NERC examined the structure of the Regional Entity CMEP departments, the adequacy and qualifications of staff resources, and the involvement of industry SMEs and Regional Entity members, as well as the existence of policies to maintain the independence and integrity of the Regional Entity compliance staff. In the second area, NERC examined the compliance monitoring tools available to assist the Regional Entities in audit planning and execution. Elements central to these audit planning and execution efforts are validation of data accuracy, confidentiality of audit information, and quality assurance of audit findings and audit reports. In addition, for each Regional Entity compliance monitoring program, NERC reviewed the Regional Entity's guidance and training offered to industry stakeholders and its participation to date in RAI.

i. Data on Regional Entity Compliance Resources

The following two tables show the amounts of (i) budgeted direct expenses and (ii) budgeted direct full-time equivalent (FTE) staffing in each Regional Entity's CMEP in 2009 and 2014, as taken from their business plans and budgets filed with the Commission. These figures are for the Regional Entity's entire Compliance Monitoring and Enforcement and Organization Registration and Certification program.[38] As the tables show, during the assessment period, each Regional Entity significantly increased its budgeted direct expenses and its budgeted FTE staffing for its CMEP.

Regional Entity	2009 Budget	2014 Budget	Percent Increase
FRCC	$2,019,650	$4,281,909	112.0%
MRO	$2,071,510	$3,864,192	86.5%
NPCC	$2,095,204	$5,080,485	142.5%
RFC	$5,099,328	$9,788,246	92.0%
SERC	$4,805,617	$7,389,556	53.8%
SPP RE	$1,283,653	$4,258,217	231.7%
Texas RE	$1,628,935	$5,991,654	267.8%
WECC	$6,165,303	$8,592,053	39.4%

Regional Entity	2009 FTE	2014 FTE	Percent Increase
FRCC	9.26	19.26	108.0%
MRO	10.00	21.26	112.6%

[38] MRO's 2014 budgeted expense does not include the expenses for its Organization Registration and Certification activities, which MRO conducted in and budgeted under its Reliability Standards program.

NPCC	9.00	16.00	77.8%
RFC	23.00	43.00	87.0%
SERC	21.50	42.50	97.7%
SPP RE	6.00	22.10	268.3%
Texas RE	14.15	40.00	182.7%
WECC	30.00	58.00	93.3%

ii. Florida Reliability Coordinating Council, Inc.

Department Structure / Staffing / Conflict of Interest Avoidance

During the assessment period, FRCC's Compliance department was split into two sections, a Compliance Monitoring group and an Enforcement group. In October 2012, FRCC separated the reporting of these two groups to create more independence between monitoring and enforcement activities. The manager of compliance enforcement reports directly to the vice president and executive director of reliability standards and compliance while the manager of compliance audits reports to the director of compliance. In addition, in June 2014, FRCC created a third group, Risk Assessment and Mitigation. This group is focused on risk assessment, both before a compliance monitoring activity takes place, to help determine the scope of the monitoring oversight; and after a possible violation is discovered, to help to determine the risk posed by the violation so that the most efficient disposition can take place. The risk evaluation before a compliance monitoring activity takes place will include both inherent risk assessment and assessment of the registered entity's internal controls. Additionally, the Risk Assessment and Mitigation group is now the primary contact for registered entities with respect to the development, implementation and completion of mitigation plans. The manager of risk assessment and mitigation reports to the director of compliance.

While NERC does not specifically endorse a particular organizational structure for CMEP departments at the Regional Entity level, NERC supports department models that facilitate the prioritization of risk. All Regional Entities are currently evaluating the structure of their CMEP departments to similarly assess how best to organize around risk.

With the recent change just described, FRCC's Compliance Monitoring group consists of eight positions, while the Risk Assessment and Mitigation group consists of four positions. Many of FRCC's audit team members individually have over 15 years of industry experience. Five audit team members were certified or hold active NERC certifications as system operators. Between 2011 and 2012, FRCC increased its staffing to add areas of expertise.

FRCC CIP auditors are required to at least have Certified Information Systems Security Professional (CISSP) certification or Certified Internal Security Auditor (CISA) certification and to demonstrate security background knowledge covering multiple domains including physical and network security. Each CIP auditor is required to maintain this certification by attending annual conferences and training seminars to achieve the required minimum of 20 continuing professional education hours annually. The FRCC manager of compliance audits is responsible for vetting the topics covered during these conferences and seminars.

The FRCC Compliance Monitoring group prepares its Operations and Planning auditors to be supplemental team members during CIP audit engagements by conducting training sessions for them to review NERC CIP Reliability Standards and evidence that can be used to demonstrate compliance with those Reliability Standards. The Operations and Planning auditors serve as supplemental team members for CIP audits on a rotational basis to increase their knowledge of CIP Reliability Standards.

FRCC tracks the on-going educational needs related to certifications for both CIP and Operations and Planning auditors. FRCC also develops an annual budget to support this training effort. During the assessment period, FRCC began using the *Compliance Auditor Capabilities and Competency Guide* recently developed by the ERO Enterprise,[39] as well as building a matrix to plan for and ensure training and development opportunities for the range of skills needed in the auditor positions. The FRCC audit team members participate in various auditor training sessions and workshops. FRCC audit staff members are required to attend NERC-sponsored ERO training.

Although FRCC is not presently using SMEs from outside the organization for its CIP or Operations and Planning audit engagements, FRCC has developed a procedure should it need to use such experts in the future. This procedure is titled *Procedure for the Use of Industry Volunteer Subject Matter Experts* and is posted alongside the *Nomination Form for the Industry Volunteer Subject Matter Expert Pool* on FRCC's website. This procedure guides FRCC compliance staff on the use of industry volunteer SMEs.

FRCC has adopted policies and procedures to avoid conflicts of interest in its CMEP work. During the assessment period, FRCC implemented an Annual Employee Recital and Disclosures process. Each FRCC employee receives a copy of the FRCC *Conflict of Interest Policy* and signs the *Conflict of Interest Questionnaire, Disclosure Statement of Stock Ownership of FRCC Member Companies*, and *Non-Disclosure Acknowledgement*. FRCC maintains a document titled *FRCC Auditor Objectivity, Independence and Impairment* on its public web page. This document provides, among other things, that auditors must remain free from "personal impairments to independence" that might cause auditors to limit the scope of their audit or alter audit findings.

Compliance Monitoring Tools and Procedures

FRCC utilizes a number of tools to execute its audits, several of which are highlighted in this section. FRCC uses an evidence index tool to catalogue evidence submitted throughout the audit process. FRCC references the evidence index numbers when referring to documentation during compliance audits and includes these references in its audit documentation. FRCC also developed its own tool for tracking additional evidence requests and for issuing follow-up data requests. These tools increase the efficiency of its audits by facilitating tracking. In addition to these tools, FRCC audit teams use several other standard auditor tools. For example, FRCC utilizes the RSAWs and the Regional Advanced Techniques Staff (RAT-STATS) sampling tool.

[39] *See ERO Enterprise Compliance Auditor Manual* (Auditor Manual) available at: http://www.nerc.com/pa/comp/Pages/ERO-Enterprise-Compliance-Auditor-Manual.aspx.

In 2012, FRCC developed its own risk assessment document to use as an interim step until NERC and the Regional Entity working groups create a template for ERO-wide use.

FRCC maintains copies of its *Compliance Audit Procedure*, *Spot Check Procedure*, and *Compliance Investigation Procedure* on its public web page. The procedures are reviewed periodically and updated as necessary. FRCC's Compliance Tracking and Submittal system (CTS) is also central to its compliance monitoring efforts. The database provides multiple functionality for entities registered in FRCC including:

(1) The ability to input and maintain registered entity contact information;

(2) The ability to submit and update CIP Technical Feasibility Exceptions (TFEs);

(3) The ability of FRCC Compliance staff to review draft registered entity compliance responses, such as mitigation plans, prior to submittal by the registered entity;

(4) The ability to submit compliance-related documentation; and

(5) The ability to allow the review of historical compliance submittals.

FRCC Compliance staff use a related software system called Compliance Information Tracking System (CITS) to store information related to processing of violations and mitigation plans. CITS is also used for developing reports for management, development of metrics and for supplying data to the NERC associated database.

Quality Assurance

After each compliance audit or spot check, the FRCC team involved conducts a lessons learned session focused on quality and process improvement. Action plans are developed to address these lessons learned. To ensure completeness and consistency, the manager of compliance audits reviews all audit reports before they are finalized and shared with NERC and the registered entity. FRCC Compliance staff have developed a number of internal procedures based upon the procedures and requirements identified in the NERC ROP. These procedures are reviewed on an annual basis and updated as necessary. These procedures are followed to ensure that FRCC Compliance staff implement compliance and enforcement activities in accordance with the guidance established by NERC and FERC.

Guidance and Training for Industry Stakeholders

FRCC utilizes its compliance workshops as the primary mechanism for outreach to its registered entities. In 2013, FRCC hosted two general compliance workshops (with an Operations and Planning focus) and one CIP compliance workshop. During these workshops, multiple techniques are used to increase the effectiveness of addressing current topics including use of registered entities to provide presentations on "best practices." Registered entities are encouraged to discuss compliance-related topics with auditors during small group breakout sessions. FRCC also conducts webinars on various topics of interest to registered entities throughout the year. Previous webinars covered topics such as preparing for an audit, enforcement process, audit approaches for specific Reliability Standards, the transition to Version 5 of the CIP Reliability

Standards, and the annual FRCC CMEP IP. FRCC also maintains a Frequently Asked Questions section on its website. FRCC Compliance staff participates in regular Regional Entity Committee and Compliance Forum (RECCF) meetings to disseminate the latest information regarding its compliance program to industry stakeholders. In addition FRCC CIP auditors are regularly scheduled on the agenda of the regional member services CIP Subcommittee meetings that are held monthly to address CIP monitoring processes and CIP audit approach issues.

Maintaining Confidentiality

There are strict confidentiality requirements associated with all CMEP activities.[40] FRCC follows the NERC CMEP to maintain the confidentiality of any complaint and maintains a link to NERC's complaint reporting page from the FRCC web site. FRCC ensures that its officers, directors, and employees with access to confidential data and information are under obligations of confidentiality pursuant to the *FRCC Confidentiality Policy*. Annually, all FRCC Compliance and Enforcement staff is trained on the *FRCC Confidentiality Policy*. FRCC has also implemented a secure vault system to receive electronic compliance evidence from registered entities. The vault system uses 256-bit advanced encryption standard (AES) cipher encryption to deliver evidence to FRCC. Access to the vault is restricted to Compliance staff and supporting IT staff, and CIP evidence is limited to viewing only in the vault.

Participation in RAI

FRCC Compliance staff have been involved in several aspects of RAI. FRCC provided a participant on the ERO Compliance and Enforcement Management Group (ECEMG) Manual Task Force (MTF) that developed the *Compliance Auditor Handbook* and associated *Compliance Auditor Checklist*, as found in the Auditor Manual. FRCC also provided personnel to aide in the training of auditors relative to the handbook and checklist at the ERO auditors workshop.

In January 2014, FRCC Enforcement staff began to triage and review all possible violations to determine the disposition method within 60 days on average. FRCC is participating in the piloting of an approach that allows selected registered entities to aggregate and submit periodically any possible minimum risk violations they may have for certain Reliability Standards and requirements.

FRCC Compliance staff have been involved with the pilot integration team that is reviewing the results of Regional Entity pilots concerning inherent risk assessment and internal controls evaluation to determine the ERO approach to scoping more risk-based compliance monitoring.

iii. Midwest Reliability Organization

Department Structure / Staffing / Conflict of Interest Avoidance

In 2009, MRO split its CMEP function into three distinct departments, each with its own assigned personnel: (i) Compliance; (ii) Risk Assessment and Mitigation; and (iii) Enforcement.

[40] *See* ROP §402.8 (NERC Oversight of the Regional Entity Compliance Monitoring and Enforcement Programs — Confidentiality).

MRO Compliance staff conduct audits and spot checks of compliance with Reliability Standards by registered entities. Since 2009, MRO has expanded its Compliance staff from five to eight auditors, split evenly between Operations and Planning and CIP, with most of the additions being CIP auditors. MRO seeks to achieve a balance of skills in its Compliance department, including technical expertise and audit experience. This balance is achieved through hiring of staff with needed skillsets and experience (i.e., system planning, protection systems, or cybersecurity) as well as through supplemental training. Training on core skills, such as ethics or audit practices, is offered generally, while specific skill gaps or training needs are identified on an individual basis. MRO currently has Operations and Planning auditors who are all certified as either NERC system operators or registered professional engineers. CIP audit staff generally hold certifications, such as CISSP and CISA that align with Department of Defense requirements.[41]

MRO Risk Assessment and Mitigation staff undertake an independent review of the facts and circumstances surrounding each violation discovered by Compliance staff. They determine whether sufficient evidence supports each possible violation. Risk Assessment and Mitigation staff also work with the registered entity to develop an effective and comprehensive mitigation plan in the event that a violation is confirmed.

Confirmed violations move to the Enforcement department staff, who review recommendations made by Risk Assessment and Mitigation staff, verify all relevant facts, and evaluate appropriate enforcement actions. The factual review conducted by Risk Assessment and Mitigation and Enforcement staff is intended to ensure a consistent, accurate application of the NERC Reliability Standards. Through this segregation of duties, MRO seeks to establish independence among those making the findings, those assessing risk, and those determining and negotiating penalties and sanctions.

MRO has adopted policies and procedures to avoid conflicts of interest in its CMEP work and to ensure the independence of its staff. Those policies and procedures provide that:

(1) No MRO director or member of MRO committees may participate in any way in compliance violation investigations, compliance audits, reports, sanction determinations, or other matters within the CMEP.

(2) An MRO director or member of an MRO committee may engage in actions on behalf of his or her employer regarding a compliance monitoring and enforcement matter undertaken by MRO; however, that director or member of an MRO Committee must recuse himself or herself from any board or committee decisions, meetings, and actions related to that compliance monitoring and enforcement matter. Potential concerns about the participation of a MRO director or member of an MRO committee are brought to the attention of the president and chief executive officer who will seek an appropriate resolution of the matter with the advice and counsel of the independent directors.

[41] *See* Department of Defense Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management" (August 15, 2004) available at: http://www.dtic.mil/whs/directives/corres/dir.html.

Compliance Monitoring Tools and Procedures

MRO uses 32 primary tools to execute its audits, four of which are highlighted in this section. A key guidance source for MRO is GAGAS, which provides a framework for conducting quality audits. MRO's primary audit template tool for documenting audit procedures, testing, findings and reports is its *Audit and Spot Check Process and Procedures* dated May 2012. This document consists of 31 templates and serves as a detailed roadmap and reference tool for MRO's Compliance staff to use during Operations and Planning and CIP audits as well as spot checks. The audit team also uses an FSAW audit workbook which is an MRO-specific tracking tool built on the RSAW for documenting audit work.[42] This tool facilitates evidence requests from registered entities as well as tracking of Reliability Standards to ensure that an audit proceeds in a timely fashion. This tool was updated in 2013 prior to its incorporation into the Auditor Manual.

MRO's web Compliance Database Management System (webCDMS) is also central to its compliance monitoring efforts. WebCDMS assists registered entities in documenting and submitting compliance information. The database provides multiple functionality including:

(1) Viewing Regional Entity and NERC requirements per a registered entity's function(s);

(2) Reviewing compliance information prior to submittal;

(3) Submitting compliance documentation;

(4) Generating compliance reports; and

(5) Tracking mitigation plans.

The webCDMS tool previously required each registered entity to use different logins and passwords. A recent enhancement to webCDMS provides the ability for a registered entity to logon and access webCDMS on behalf of multiple affiliated entities within a particular Regional Entity, using a single username, password, and webCARES digital certificate.

Quality Assurance

MRO relies on a number of tools to assist in its quality assurance efforts. Compliance staff perform peer reviews of audit documentation during audit fieldwork, in addition to reviews conducted by management and by non-Compliance personnel. Such reviews ensure the completeness of audit documentation and that any findings are consistent with the elements of a finding per GAGAS. In addition to audit documentation reviews, Compliance staff rely on "lessons learned" discussions and post-audit surveys of registered entities to help identify opportunities to improve compliance monitoring-related processes and to improve future interactions with registered entities. Finally, Compliance staff review audit findings with Risk Assessment and Mitigation staff to ensure consistent application of the NERC Reliability

[42] FRCC and WECC also have tools that mirror this tool.

Standards among MRO staff and across registered entities in the MRO footprint. All lessons learned are shared internally and, if more broadly applicable outside of MRO, with personnel from NERC and other Regional Entities.

Guidance and Training for Industry Stakeholders

MRO supports industry in developing compliance guidance in the form of Application Guides. Application Guides offer non-binding, training guidance regarding how to meet the requirements of existing and emerging Reliability Standards. They can include the following:

(1) Presentation materials developed by MRO member organizations who volunteer SMEs to the NERC SC;

(2) FERC comments relating to a Reliability Standard;

(3) Documentation and evidence demonstrating compliance; and

(4) References and source documents related to laws, policies, directives, instructions, Reliability Standards and guidelines.

MRO tracks the impact of Application Guides through trend analysis of Reliability Standard violations.

MRO's website contains posted compliance guidance directed to industry stakeholders, including content about internal controls, best practices for internal compliance programs, and aids to assist in compliance for specific and more challenging Requirements. Instructional materials informing stakeholders as to what they can expect and what professional audit standards they should anticipate for their compliance audits is made available on this site. Guidance is also offered to registered entities in their audit notification packets from MRO. With regard to small entities, MRO routinely communicates to the representatives of the applicable trade associations that their members should contact MRO directly with any concerns, including regulatory burden.

MRO holds at least two one-day workshops per year addressing reliability, compliance, and enforcement. In 2013, MRO also held a model building workshop to provide direction and instruction for those who are directly involved in the preparation and submittal of model data. MRO's bi-monthly newsletters have a regular column titled "Tips and Lessons Learned" which covers a wide range of topics from how to use webCDMS more effectively to changes in the procedures for requesting and processing TFEs. Occasionally, "Tips and Lessons Learned" are authored by registered entities covering topics like the CIP Version 5 transition study. MRO conducted its first webinar in 2014 and as part of its review of training initiatives, MRO will be asking its stakeholders for input on the use of webinars. MRO is not participating in any initiative with other Regional Entities to decrease or consolidate the number of announcements published for industry; however, MRO reports that in response to its stakeholder surveys, registered entities have generally encouraged MRO to communicate more, not less.

Maintaining Confidentiality

There are strict confidentiality requirements associated with all CMEP activities.[43] MRO follows the CMEP to maintain the confidentiality of any complaint and has a third-party hotline available to complainants to maintain anonymity. Complainants can contact MRO's chief compliance and ethics officer, who does not do any CMEP work, to maintain anonymity.

All data related to MRO's CMEP activities, particularly registered entity data that may be designated Critical Energy Infrastructure Information, are protected according to §1500 of the NERC ROP to ensure that confidentiality is maintained. Data is stored on a restricted network drive, to which access is granted on a need-to-know basis according to individuals' job responsibilities. Outside of the restricted drive, data may only be stored for limited periods of time on encrypted hard drives or IronKey-encrypted USB drives. When transferring data to or from registered entities, MRO makes use of a secure Enhanced File Transfer (EFT) server, which includes encryption both during transfer and while stored on the EFT server. The EFT server is also utilized for all data transfers involving NERC, FERC, or other Regional Entities.

Participation in RAI

As part of RAI, NERC has assisted with ensuring consistency among audits conducted by the Regional Entities by developing the Auditor Manual. MRO has already taken steps to follow the protocols established in the Auditor Manual. In particular, MRO has changed its protocol regarding independence of audit staff to conform to GAGAS. MRO has also indicated that it will fully adopt the Auditor Manual protocols.

iv. Northeast Power Coordinating Council, Inc.

Department Structure / Staffing / Conflict of Interest Avoidance

Activities performed pursuant to the CMEP are performed within the NPCC Compliance Monitoring and Enforcement and Organization Registration and Certification (CORC) program. In total, NPCC's CORC program area consists of 16 employee positions. The CORC program is divided into two subprograms: (i) an Audits and Investigations subprogram and (ii) a Registration and Enforcement subprogram. The Audits and Investigations subprogram conducts audits, spot checks, and compliance investigations. It is comprised of eight staff employees. The Audits and Investigation subprogram utilizes approximately a dozen independent consultants in addition to NPCC employees. During an audit, spot check, or compliance investigation, the Audits and Investigation team makes a determination of whether a registered entity has any possible violations of NERC Reliability Standards, and provides NPCC enforcement staff with a final report.

The Registration and Enforcement subprogram is comprised of eight staff employees. The Registration and Enforcement subprogram reviews the audit, spot check, or compliance investigation report, and makes an independent evaluation of the facts and circumstances surrounding each possible violation identified in the report. Registration and Enforcement will

[43] *See* NERC ROP §402.8 (NERC Oversight of the Regional Entity Compliance Monitoring and Enforcement Programs — Confidentiality).

determine whether sufficient evidence supports each possible violation and will work with the registered entity to develop an effective and comprehensive mitigation plan. Registration and Enforcement will also evaluate the appropriate enforcement actions, including sanctions and/or penalties.

Many NPCC audit team members individually have over 30 years of industry experience. Two audit team members are NERC-certified system operators and two are registered professional engineers. As described above, NPCC also relies on independent SME consultants who have no other industry obligations or conflicts of interest to perform compliance monitoring activities and to support any increases in its workload. NERC AAO staff recommends that NPCC consider having more audit staff become NERC-certified system operators.

NPCC audit team members participate in various auditor training sessions and workshops. All NPCC auditors attend at least one of the two annual NERC ERO compliance workshops to keep apprised of current topics and NERC initiatives affecting compliance. NPCC itself conducts four in-house auditor training sessions each year. In addition, NPCC auditors augment their training with annual required or suggested NERC training.

With respect to monitoring compliance with the CIP Reliability Standards, NPCC recruits employees with network systems protection experience. Two NPCC auditors have CISSP certifications and one auditor has physical security protection experience. NPCC examines the training that these auditors will need for the upcoming year or other future time frame and assures that its CIP auditors (both employees and consultants) receive the appropriate supplemental training, in addition to the regular training described above.

NPCC has adopted policies and procedures to avoid conflicts of interest in its CMEP work and to maintain the independence of its compliance staff. Those policies and procedures provide that each NPCC director, officer, and employee shall: (i) avoid and refrain from involvement in situations where there is an actual conflict of interest; (ii) disclose any actual or potential conflicts of interest that may arise; (iii) recuse himself or herself from participation in any action involving an actual or potential conflict of interest; and (iv) refrain from voting on any actions where there is an actual or potential conflict of interest.

Compliance Monitoring Tools and Procedures

NPCC utilizes a number of tools to execute its audits, several of which are highlighted in this section. NPCC instituted an improved process in order to facilitate its data reviews in both pre-audit and on-site phases. Its pre-audit process involves several rounds of questions and answers between NPCC and the registered entity relating to a subset of Reliability Standards within the audit scope. The NPCC auditor catalogs the data requests in an evidence tracking spreadsheet. Following this initial evidence review, NPCC provides the evidence tracking spreadsheets to the registered entity prior to on-site activities. During the on-site portion of the audit, the evidence tracking spreadsheets are used by the audit team to direct SME interviews and record additional questions and data requests determined throughout the interview process. NPCC also developed a change management process to ensure the integrity of evidence tracking spreadsheets. At the end of each day of the audit, the NPCC audit team reviews the updated evidence tracking spreadsheets with the registered entity in a debrief.

NPCC's Compliance Data Administration Application (CDAA) is central to its compliance monitoring efforts. All registered entities in NPCC are required to use the CDAA to submit self-certifications and self-reports. Information submitted into the CDAA is automatically placed into CITS. The CDAA database provides multiple functionality, including:

(1) Viewing Regional Entity and NERC requirements per a registered entity's function(s);

(2) Reviewing compliance information prior to submittal;

(3) Submitting compliance documentation;

(4) Generating compliance reports; and

(5) Tracking mitigation plans.

Quality Assurance

NPCC's audit processes are documented in its compliance procedures; these procedures are reviewed on a periodic basis.[44] Following the conclusion of every on-site and off-site audit, NPCC asks registered entities to complete a feedback form. NPCC's audit group reviews comments in order to assess how to improve its processes. NPCC chooses to include detailed information and justification for all audit conclusions in the nonpublic audit reports, including "No Finding" and "Not Applicable." NPCC performs a quality check of draft reports prior to sending them to registered entities for comment. As a result, NPCC does not always meet the 60-day timeline for issuance of audit reports. Additionally, in 2013, NPCC began assigning a minimum of two auditors, in addition to the audit manager, to each off-site audit. This allows the auditors to learn from each other and provides additional quality assurance. Prior to 2013, NPCC assigned a minimum of one auditor, in addition to the audit manager, to each off-site audit.

Guidance and Training for Industry Stakeholders

Since 2009, NPCC has provided the same level of resources for its Training, Education, and Operator Certification program. NPCC dedicated 0.1 FTE to its Training, Education, and Operator Certification program in 2009.[45] For 2013, NPCC also dedicated 0.1 FTE to this program.[46] NPCC utilizes its semi-annual standards and compliance workshops as its main mechanism for outreach to its registered entities, and these activities are budgeted in those respective program areas. NPCC also conducts webinars open to all NPCC registered entities on an as-needed basis. It also posts question-and-answer documents on its website as appropriate. NPCC responds to individual requests from registered entities, but if an individual concern can be applied to all registered entities, NPCC will post a *Compliance Guidance Statement* or clarification

[44] Available at: https://www.npcc.org/Compliance/Compliance%20Procedures/Forms/Public%20List.aspx.

[45] 2009 Business Plan and Budget, Northeast Power Coordinating Council, Inc., June 24, 2008.

[46] 2013 Business Plan and Budget, Northeast Power Coordinating Council, Inc., June 26, 2012.

to address that concern. NPCC hosts regular stakeholder-based Compliance Committee meetings to disseminate the latest information regarding the compliance program to industry stakeholders. Many of these regularly-scheduled meetings are hosted on a web conferencing platform to enable broad and cost-effective participation. NPCC also developed an internal entity guide to assist registered entities in meeting quarterly reporting requirements pursuant to PRC-004 and NERC ALR4-1.

In 2013, NPCC implemented a Physical Security Outreach program. Under this program, NPCC physical security SMEs performed physical security assessments for registered entities that have requested such assistance. NPCC has developed a new Cyber Security Outreach program for 2014.

Maintaining Confidentiality

There are strict confidentiality requirements[47] associated with all CMEP activities. NPCC follows the CMEP and §1500 of the NERC ROP to maintain the confidentiality of all confidential CMEP-related activities. Additionally, NPCC staff involved in CMEP-related activities have signed confidentiality agreements.

Participation in RAI

As part of the RAI initiative described in NERC's *Overview of NERC Activities and Accomplishments in the Five-Year Period*, NPCC participated in efforts to develop the Auditor Manual for the ERO. NPCC also participated in the RSAW Working Group to ensure commonality on audit approaches to the NERC Reliability Standards. NPCC senior management participated in the RAI workgroups charged with developing a framework for Entity Risk Assessment and Internal Control Assessment. NPCC also participates in various Regional Entity compliance and enforcement groups to further consistency in compliance applications across the Regional Entities.

v. ReliabilityFirst Corporation

Department Structure / Staffing / Conflict of Interest Avoidance

During the assessment period, three departments carried out ReliabilityFirst's CMEP functions: (i) Compliance Audits (handling audits and spot checks of compliance with Reliability Standards by registered entities);[48] (ii) Investigations and Compliance Services (handling compliance investigations, registration and certification, self-certifications and periodic data submittals, complaints, and industry training); and (iii) Enforcement (handling all aspects of

[47] *See* ROP §402.8 (NERC Oversight of the Regional Entity Compliance Monitoring and Enforcement Programs — Confidentiality).

[48] Upon the implementation of the CIP Reliability Standards, Compliance Monitoring was subdivided into a CIP Compliance Audit department and an Operations and Planning Compliance Audit department.

enforcement actions, including fact and circumstance review, risk-harm assessment,[49] mitigation plan review and validation, and the negotiation and drafting of settlements and final disposition documents).

At the beginning of 2014, ReliabilityFirst reorganized its compliance structure in order to more clearly focus around risk and to support RAI. Presently, ReliabilityFirst's Compliance Monitoring group handles compliance audits, spot checks, investigations, and complaints, and is subdivided into two departments: (i) a CIP Compliance Monitoring department and (ii) an Operations and Planning Compliance Monitoring department. ReliabilityFirst created a new Reliability Assurance and Monitoring group, which is comprised of three departments: (i) Entity Development (which conducts assist visits, appraisals, certifications, and entity training); (ii) Risk Analysis & Mitigation (which conducts risk-harm assessments, handles mitigation activities, and conducts risk-based assessments, event analyses, and analytics); and (iii) Standards and Services (which is responsible for Reliability Standards, registration, self-certifications and data submittals). ReliabilityFirst's Enforcement group is now housed under Legal & Regulatory Affairs.

ReliabilityFirst's Compliance department (consisting of the Compliance Monitoring and Reliability Assurance and Monitoring groups) consists of 33 positions. Many employees within those positions have at least 15 years of industry experience. Additionally, many of ReliabilityFirst's compliance staff are registered professional engineers, and many are NERC-certified system operators. ReliabilityFirst's CIP auditors have extensive experience in information technology and cybersecurity and hold various security, audit, and IT certifications.

ReliabilityFirst requires regular training for its Compliance staff. ReliabilityFirst's Compliance Audit Procedure has specific training requirements that its audit team members must complete prior to attending an audit. ReliabilityFirst audit team participants and ReliabilityFirst observers must complete all required NERC auditor training courses. All ATLs must complete the *Fundamentals of Auditing for NERC Compliance Team Leaders* and *Gathering Quality Evidence* modules. All other audit team participants must complete the *Fundamentals of Auditing for NERC Compliance Audit Team Members* and *Gathering Quality Evidence* modules. Audit team members participate in various auditor training sessions and workshops. ReliabilityFirst sends its auditors to NERC-led training events whenever they occur. ReliabilityFirst also holds its own staff training week during which it provides on-site training to all staff members, including auditors. For example, during the 2013 ReliabilityFirst training week, ReliabilityFirst's Operations and Planning auditors received training on protection systems, while its CIP auditors received training on various cybersecurity issues. All auditors received training on the evaluation and communication of risk and using risk-based criteria in informed decision-making.

ReliabilityFirst has adopted policies and procedures to avoid conflicts of interest in its CMEP work in order to maintain the independence of its compliance staff. All ReliabilityFirst employees, contractors, and directors are governed by the ReliabilityFirst *Conflict of Interest Policy*, the *ReliabilityFirst Code of Business Conduct and Ethics*, and §1500 of the NERC ROP.

[49] To enhance its risk determination process in enforcement, ReliabilityFirst developed a risk-harm assessment process which, among other things, requests technical experts to answer a series of questions about the risk and harm posed by each violation using a common scale to ascertain a quantified risk assessment.

Its employees and contractors must sign and adhere to nondisclosure and confidentiality agreements and complete conflict of interest forms. ReliabilityFirst does not allow stakeholder participation in its compliance or enforcement activities. Further, ReliabilityFirst does not allow its industry sector directors to participate in settlement discussions with ReliabilityFirst on behalf of their Registered Entity.[50]

Compliance Monitoring Tools and Procedures

ReliabilityFirst utilizes a number of tools to execute its audits, several of which are highlighted in this section. During the assessment period, ReliabilityFirst implemented changes to its compliance monitoring processes and tools to ensure that they are consistent with NERC guidance, other Regional Entities, and GAGAS.

Most entities in the ReliabilityFirst footprint utilize an application called "Color-Code-It" to make evidence submittals which saves audit teams considerable review time and helps ensure a comprehensive and a focused audit or spot check. Use of this application also allows registered entities to organize and monitor their own compliance, maintain internal controls, and reduce the burden of compliance monitoring.

ReliabilityFirst uses a pre-audit review period to review evidence submittals, seek additional information, make compliance determinations, and develop a focused requirement listing to be addressed at the audit review. Audit reviews are typically scheduled two to three weeks prior to the audit. ReliabilityFirst believes that this improvement has provided the time to do a very comprehensive audit and maintain focus on items which need more attention or clarification.

During the assessment period, ReliabilityFirst began to develop and implement an audit management system. This system will allow ReliabilityFirst to manage audits, spot checks, and potentially other monitoring processes of an entity in one application. The software resembles a project management system and has been developed to follow the various steps of an audit checklist, such as planning, pre-audit review, production, reporting and metrics. This system provides auditors with a structured format to follow and help to ensure consistency and completeness in each audit that is performed.

ReliabilityFirst has developed and implemented a risk-based assessment process. This process was initiated in June 2011. During the risk-based assessment process, a designated cross-functional team[51] conducts a risk assessment of a registered entity and makes recommendations to help shape the scope and focus of the registered entity's upcoming compliance audits and/or spot checks. During the assessment, the team evaluates the potential impact of the registered entity on the BPS based upon various factors, including the registered entity's registration, size, location, technical characteristics (e.g., existence of special protection systems), organizational makeup, compliance history and culture, and trends and emerging risks in the industry. ReliabilityFirst implemented this process based on guidance from NERC. ReliabilityFirst will refine the risk-

[50] *See* 2014 Joint Regional Entity Self-Assessment (JRESA) Appendix 2-C at 21.

[51] This cross functional team includes representatives from the ReliabilityFirst engineering, compliance audit, compliance enforcement, and reliability assurance departments.

based assessment process further throughout 2014 to develop a comparable, repeatable process that is aligned with efforts being undertaken under RAI.

ReliabilityFirst's webCDMS system is central to its compliance monitoring efforts. ReliabilityFirst uses webCDMS as its information management tool to collect securely, track, and monitor compliance information from its registered entities. The database provides multiple functionality including:

(1) Linking Regional Entity and NERC requirements to a registered entity's function(s);

(2) Allowing registered entities to review compliance information prior to submittal;

(3) Allowing registered entities to submit compliance documentation, including self-reports, self-certifications, and mitigation plans;

(4) Allowing ReliabilityFirst and registered entities to generate compliance reports; and

(5) Allowing ReliabilityFirst to track mitigation plans.

Quality Assurance

ReliabilityFirst's quality assurance processes are contained within its internal compliance procedures, which ReliabilityFirst reviews on a periodic basis. The ReliabilityFirst Audit Procedure requires ReliabilityFirst to follow a multi-layered quality review process for its draft audit reports, which includes peer reviews and management reviews. The ReliabilityFirst Audit Procedure also requires ReliabilityFirst to ask entities to provide feedback on the audit process and any other concerns they may have, using a feedback form. ReliabilityFirst then uses the feedback and concerns for quality assurance and continuous improvement.

Guidance and Training for Industry Stakeholders

Since 2009, ReliabilityFirst increased its training resources for its Training, Education, and Operator Certification program, which provides continuing education hours through the NERC Continuing Education program. ReliabilityFirst dedicated 0.05 FTE to its Training, Education, and Operator Certification program in 2009.[52] For 2013, ReliabilityFirst increased training resources to 3.1 FTEs.[53]

ReliabilityFirst uses several different methods to communicate with and train its registered entities. ReliabilityFirst has implemented an "Assist Visit" program. Under this program, a registered entity may request a one-on-one or small group meeting where ReliabilityFirst provides guidance on compliance-related activities. Assist Visits can be in the form of a conference call, web meeting, or on-site visit, and topics can range from helping a registered entity become more

[52] 2009 Business Plan and Budget, ReliabilityFirst Corporation, August 13, 2008.

[53] 2013 Business Plan and Budget, ReliabilityFirst Corporation, June 22, 2012.

familiar with general compliance-related material and activities to specific guidance on an area of concern. ReliabilityFirst has prepared and implemented an internal policy and procedure that requires it to internally document Assist Visit training activities to extrapolate and share generic lessons learned where appropriate. The policy and procedure ensures that ReliabilityFirst documents its Assist Visit training activities in a uniform manner, which will help it better distill Assist Visits into useful lessons learned to share with ReliabilityFirst stakeholders where appropriate.

ReliabilityFirst also provides a monthly newsletter to approximately 600 compliance contacts at its registered entities. This newsletter provides registered entities with news and information relating to reliability and compliance activities. In addition, ReliabilityFirst provides a monthly compliance update letter that provides the registered entities with any changes made to the compliance monitoring schedule and the due dates of compliance submittals. ReliabilityFirst's public website provides a number of compliance and technical materials to assist registered entities in their compliance program implementation.

ReliabilityFirst also hosts bi-annual compliance workshops and periodic webinars throughout the year to train registered entities on compliance processes, reliability initiatives, and the Reliability Standards. In addition, ReliabilityFirst holds a monthly conference call with web presentation capabilities for registered entities; this monthly call is an open forum for registered entities to voice concerns, ask questions, and receive information.

Maintaining Confidentiality

ReliabilityFirst has a variety of security measures in place that are designed to protect confidential compliance information. All ReliabilityFirst laptops have encrypted hard drives, minimizing the risk of confidential information being disclosed in the event of a lost or stolen laptop. ReliabilityFirst requires employees to change the passwords on their laptops every 90 days, and requires work phones to be password protected. ReliabilityFirst's offices have physical security measures including badge readers and access badges for all employees. Visitors must be escorted by ReliabilityFirst employees in nonpublic areas of the offices.

ReliabilityFirst uses a confidential and secure extranet website to exchange documents with a registered entity during a compliance monitoring process or an enforcement action. To provide another layer of protection, ReliabilityFirst encrypts sensitive documents.

There are strict confidentiality requirements[54] associated with the investigation of any complaints regarding such potential violations of Reliability Standards. ReliabilityFirst follows the CMEP to maintain the confidentiality of any complainant and maintains a complaint reporting form on its web page.

[54] *See* NERC ROP §402.8 (NERC Oversight of the Regional Entity Compliance Monitoring and Enforcement Programs — Confidentiality).

Participation in RAI

ReliabilityFirst participated in the conceptualization, development, testing, and integration of several RAI programs. ReliabilityFirst led a series of pilot programs to test the evaluation of internal controls at registered entities using an appraisal process. As part of the RAI, ReliabilityFirst participated in efforts to develop the Auditor Manual. ReliabilityFirst also participated in the RSAW Working Group to ensure commonality on audit approaches to the NERC Reliability Standards. In the enforcement area, ReliabilityFirst staff participated in the Aggregation of Minimal Risk Issues pilot program, maintaining the sole MRRE log. Additionally, ReliabilityFirst staff participated in the Enforcement Discretion pilot program and served on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. Further, ReliabilityFirst staff participated in the process to develop improvements for the compliance and enforcement oversight of MRREs. Finally, ReliabilityFirst participates in various Regional Entity compliance and enforcement groups to further consistency in compliance applications across the Regional Entities.

vi. SERC Reliability Corporation

Department Structure / Staffing / Conflict of Interest Avoidance

SERC's CMEP function is split into two departments, (i) Compliance and (ii) Enforcement, each with its own assigned personnel. SERC Compliance staff utilize off-site and on-site audits, spot checks, and other compliance monitoring methods to assess registered entity compliance with NERC Reliability Standards. Compliance is also responsible for registering users, owners, and operators of the BPS and for certifications. Compliance staff prepare detailed reports on each audit and make recommendations to Enforcement about possible violations of NERC Reliability Standards.

SERC Enforcement staff undertake an independent review of the facts and circumstances surrounding each possible violation discovered by Compliance staff or through the other discovery methods. If a sufficient basis exists, then Enforcement staff determine the complete scope of the violation and the actual and potential risk to the reliability of the BPS. The segregation of duties between Compliance and Enforcement staff establishes independence between those making the findings and those determining and negotiating penalties and sanctions.

In 2009, SERC had six Operations and Planning auditors and two CIP auditors. In 2014, SERC has seven Operations and Planning auditors and eight CIP auditors. SERC Operations and Planning audit team members possess the education, industry experience and technical expertise in planning and real-time operations necessary to conduct audits. Several of the Operations and Planning auditors are NERC-certified system operators. Many of the SERC CIP audit team members possess physical security or information security credentials, professional engineering licenses, and/or industry experience. For Operations and Planning audits, SERC audit teams work in two groups. One group reviews audit evidence for NERC operations Reliability Standards and the other group reviews evidence for planning Reliability Standards. For CIP audits, SERC audit teams also work in two groups. One group reviews evidence for physical security Reliability Standards and the other group reviews evidence for cybersecurity Reliability Standards. Each group has a lead moderator and a scribe.

SERC uses industry subject matter experts (ISMEs) from various registered entities that are members of SERC as participants in the audit team. The ISMEs help the audit team to review evidence, and provide insight into issues that the audit team may encounter throughout the audit process. While ISMEs are involved in every aspect of the audit, including interviews of the audited entity's SMEs, they are not voting members of the audit team. ISMEs bring knowledge of the latest changes that are occurring within industry and in the individual ISME's organization. ISMEs are required to sign nondisclosure agreements and complete a conflict of interest form. SERC reviews the conflict of interest forms before assigning ISMEs to audits. If a conflict exists or there is the appearance of a conflict, SERC will assign an ISME to an audit of a different registered entity.

SERC audit team members participate in various SERC internal auditor training sessions, consultant-provided auditor training sessions, NERC auditor training modules, NERC audit team lead training, and ERO auditor workshops. NERC uses training accountability databases to confirm the credentials of audit team members. SERC requires all audit team members to complete "Just-In-Time" training if the audit team member has not completed appropriate training in the last 90 days. The purpose of this training is to refresh fundamental concepts of auditing and thereby supplement that which is required by NERC. This additional training is an excellent method to re-enforce the importance of quality evidence and documentation during the audit process.

Cross-training is also an important feature of auditor training at SERC. Early in the assessment period, SERC utilized CIP auditors as scribes during Operations and Planning audits so that the CIP auditors would have an opportunity to learn the audit process and approach with Operations and Planning Reliability Standards. SERC auditors have also participated on audit teams in other Regional Entity footprints to cross-train and learn.

To determine the skill level required for auditors, SERC relies on feedback from existing audit staff, the input and experiences of NERC and the other Regional Entities, and changes in the Reliability Standards and industry. SERC anticipates training needs by looking at gaps that exist in the audit teams and focuses training on addressing those gaps. SERC considers the direction in which the ERO and other Regional Entities are moving and, if needed, adapts its training plans and desired skill sets to address those needs. SERC also considers new or revised Reliability Standards and the audit approaches associated with them, and provides training if necessary. SERC also listens to what the auditors identify as useful training and development opportunities and allows them to pursue relevant opportunities to strengthen their skills.

SERC has a documented conflict of interest policy which applies to all SERC staff. The conflict of interest policy requires SERC staff to provide an annual update of any employment or director or officer relationships with SERC registered entities, financial interests in any businesses from the energy sector other than SERC, and any business relationships with energy sector businesses other than SERC by the SERC employee or members of the employee's immediate household. SERC personnel with a financial interest in a registered entity or any other current conflict are not allowed to review, discuss, or participate in compliance or enforcement activities.

Compliance Monitoring Tools and Procedures

SERC utilizes a number of tools to execute its audits, several of which are highlighted in this section. As an overarching procedure in completing and tracking the audit progress, SERC uses its audit event tracking spreadsheet. In this spreadsheet, SERC details the actions required to successfully administer an audit and notes the completion of milestones. Registered entities use an internet-based portal for the transmission of audit information and the audit RSAWs and pre-audit questionnaires. During on-site audits and throughout the period leading up to the audit, SERC utilizes email notifications, worksheet summaries, and spreadsheet tables for tracking the review of evidence and for delivering updates to the registered entity and audit team members. SERC also uses established ERO auditor tools, including the RAT-STATS sampling tool and RSAWs. SERC also uses a pre-populated spreadsheet to document the review status for each requirement, including data requests and follow-up questions to be asked on-site. The SERC audit team uses a tool called an audit workbook. This workbook accounts for each of the Reliability Standards and associated requirements that compose the audit scope, any outstanding data requests, and a list of ongoing findings by the audit team.

Until 2013, SERC did not perform formal pre-audit reviews. The absence of a formal pre-audit review is an area of concern because formal pre-audit reviews and the opportunity to thoroughly review documentation would provide SERC with more time to investigate exceptions to audit procedures. It also helps to ensure that sufficient evidence is collected. In 2013, SERC began conducting pre-audit reviews of evidence submittals, which allowed audit teams to better prepare for audits and seek additional information as needed before arriving on-site. Audit reviews are typically scheduled two to three weeks prior to an audit. These efforts have allowed SERC to reduce its time on-site, thereby reducing the burden on the registered entity, and ensure that the on-site audit focuses less on preliminary data collection and more on reviewing higher risk issues and areas where additional clarification is needed.

While SERC has a comprehensive process for registered entity assessment and audit scoping, the associated documentation supporting this process was not thorough until recently. Maintaining thorough audit scoping documentation is an auditing best practice per GAGAS. Adequate scoping helps justify auditng the areas that pose potential risk to the BPS. Starting in mid-2013, SERC conducts an inherent risk assessment and internal controls review (if appropriate) of the registered entity to determine the audit scope and scale. This includes a review of registered entity compliance history, events and misoperations history, registered entity specific data, regional factors affecting reliability, legal or regulatory issues affecting compliance, and public information about the reliability impact of the registered entity. Detailed audit scoping will enable SERC management to better supervise and assess audits. SERC is now actively working to build GAGAS audit principles into its audit process. SERC's sampling methodology could be improved by integrating NERC's *Sampling Methodology Guidelines and Criteria* in order to avoid inconsistency in identifying and quantifying population, sample sizes, sample selection and lack of documentation memorializing sampling procedures and to avoid incorrect conclusions.

SERC tracks mitigation plans in CITS, a compliance information tracking system used by SERC, FRCC, and NPCC. CITS allows SERC to track mitigation plans submitted by registered entities, any revisions requested by SERC, and certifications of mitigation plan completion. SERC works with registered entities to answer questions about SERC's expectations for mitigation plans

and encourages them to submit mitigation plans in a timely manner. SERC occasionally asks registered entities to submit revised mitigation plans when the proposed mitigation plan milestones would result in an extended period of noncompliance that would pose an additional risk to the reliability of the BPS.

SERC presently is unable to consolidate its compliance and reliability assessment portals because they are hosted on separate systems. SERC is exploring an enhancement to these portals that that will provide a registered entity with a summary of all forms (Compliance, Reliability Assessments, and Reliability Services) due for that entity. This will allow users to navigate between both portals to complete the required filings.

SERC develops an annual reporting schedule which identifies required periodic data submittals. Once the matrix is developed, SERC posts it to its website and Compliance Portal, and notifies its registered entities. The Compliance Portal automatically assigns the applicable periodic data submittals to each registered entity's portal site, based on the schedule, identifying the due dates. SERC monitors the submittal of each periodic data submittal using a reporting tool and issues a notification to the registered entity's designated contacts for any periodic data submittals that have not been submitted to SERC. The data received from the periodic data submittals are reviewed and any potential noncompliance issues are documented and reported to Enforcement.

Quality Assurance

SERC's internal process requires a management review within two weeks of an audit engagement, and prior to the audit exit briefings before a decision is made with respect to the registered entity's compliance with NERC Reliability Standards. The management review evaluates the significant judgments made by the audit team and the related conclusions reached in forming the overall conclusion on the engagement. SERC Enforcement staff reviews the audit team's findings of noncompliance and makes a final determination before notifying the registered entity and NERC of any possible violations.

SERC Compliance staff meet weekly and discuss lessons learned after each audit. If appropriate, a plan is developed for any areas that need changes or improvements internally. SERC also develops lessons learned as part of its outreach efforts and these are shared with registered entities. The Operations and Planning and CIP audit groups each have a point of contact for their respective areas who are made aware of any trends or important information that they feel should be communicated to SERC registered entities. A brief description and observations are written and posted quarterly on a dedicated area of the SERC website where registered entities can review it.

SERC has a document retention policy that requires audit documents be maintained for seven years. SERC has a document management system with a retention policy service that allows for the configuration of retention policies. The system also requires administrative permissions to delete documents, files, and folders.

Guidance and Training for Industry Stakeholders

Since 2009, SERC increased its training resources for its Training, Education, and Operator Certification program, which provides continuing education hours through the NERC Continuing

Education program. SERC dedicated 1.4 FTE to its Training, Education, and Operator Certification program in 2009.[55] In 2013, SERC delivered its training program through 2.41 FTEs.[56]

A catalog of all SERC outreach and training has been posted to the home page of the SERC website. Three compliance seminars are held annually with one focused exclusively on CIP topics. In addition, periodic Open Forum WebEx sessions are scheduled along with focused webinars on new and/or revised Reliability Standards and changes in regulatory policy such as the new BES definition process. Specific training on SERC policy changes and enhancement to tools offered to registered entities is also conducted on an as-needed basis. The majority of outreach events are offered via WebEx, and recordings are posted to the SERC website. Select events also offer the opportunity to attend in person and/or earn continuing education hours.

The SERC Training, Education, and Operator Certification program provides education and training necessary to understand and operate the BPS. The target audience of the program is BPS operating personnel – including system operations personnel, operations support personnel (engineering and information technology), supervisors and managers, and training personnel. The program held four system operator conferences in 2013, a wide area restoration drill, and several standard-focused webinars and workshops. The program also supports SERC staff training and development as well as the administration of records necessary to maintain status as a NERC continuing education provider. The majority of outreach events are offered via WebEx, and recordings are posted to the SERC website. Select events also offer the opportunity to attend in person and/or earn continuing education hours.

SERC outreach has conducted small entity workshops specifically focusing on topics of interest to smaller registered entities. An informal group consisting of representatives from four small entities is consulted as to what topics are appropriate and of interest to them. The annual *SERC Filing Due Dates* document is posted to the SERC website in Excel format to make it easy for entities to sort by registered function in order to determine what compliance filings are due and when. An email address (serccomply@serc1.org) is available, and publicized in all outreach materials, for entities to contact SERC with any questions they may have.

Maintaining Confidentiality

SERC has a variety of security measures in place that are designed to protect confidential compliance information. All SERC laptops have encrypted hard drives, minimizing the risk of confidential information being disclosed in the event of a lost or stolen laptop. SERC requires employees to change the passwords on their laptops every 90 days. SERC requires work phones to be password protected and these phones can be remotely wiped. SERC's offices have physical security measures including badge readers, access badges for all employees, and video cameras at all entrances and exits. Visitors must be escorted by SERC employees in nonpublic areas of the offices.

[55] 2009 Business Plan and Budget, SERC Reliability Corporation, July 9, 2008.

[56] 2013 Business Plan and Budget, SERC Reliability Corporation, July 11, 2012.

In addition, SERC implemented a Protected Entity Information (PEI) program in 2012 to handle confidential CIP information and other protected entity information. This PEI program was implemented in order to allow registered entities to provide SERC with CIP and other confidential information without SERC having to visit registered entities' sites. The PEI program protects this information using standards at least as strict as those in the CIP Reliability Standards. Access to PEI information is restricted to those SERC employees with a need to know who have taken cybersecurity awareness training within the past year and have passed SERC-initiated background checks within the previous seven years. In addition, SERC logs and controls physical access to the hardware used for the PEI program. SERC also logs and controls electronic access to the PEI information stored on that hardware, which is encrypted at rest.

Participation in RAI

A key focus of SERC's strategic plan for 2013-2015 is to develop, advocate, and support RAI. SERC has established a plan to implement audit function structural improvements to produce more effective, efficient audits that recognize BPS reliability risk. By incorporating risk principles in the planning and execution of compliance engagements, in conjunction with broader RAI outcomes, the focus of SERC and its registered entities will shift towards identification and mitigation of risks to reliability – preventing uncontrolled, unplanned cascading events. Scoping and timing of monitoring activities will move from a mechanical approach (fixed set of entities monitored for a pre-established set of Reliability Standards on a pre-defined frequency) to a risk-based approach customized around SERC-specific reliability issues and tailored to the specific registered entity. Through more extensive information analysis and dialogue with registered entities, SERC staff will seek to fully understand risk and the registered entity's management practices and controls employed to obtain reasonable assurance of the reliable operation of the BPS. Based on this more proactive review and assessment, SERC will adjust the scope and frequency of its compliance monitoring activities with respect to the specific registered entity.

Throughout 2013, SERC worked with an inter-regional team to develop the *Compliance Auditor Handbook* that describes a uniform process for implementing the *Compliance Auditor Checklist*. In addition, SERC piloted a new approach to risk assessments and auditing practices that permits more focused attention and resources on those issues that present the greatest risk to the BPS. Currently, SERC is working with all eight Regional Entities to develop a common methodology to identify and assess risk in a manner consistent with GAGAS criteria.

vii. Southwest Power Pool Regional Entity

Department Structure / Staffing / Conflict of Interest Avoidance

The SPP RE CMEP is administered by the SPP RE direct staff organized into three groups: (i) Compliance Monitoring - Operations and Planning; (ii) Compliance Monitoring - CIP; and (iii) Enforcement. The Compliance groups are responsible for registering BPS owners, operators, and users, and monitoring and assessing registered entity compliance with the approved Reliability Standards. The Compliance groups make the initial determination of a registered entity's compliance or noncompliance by performing audits, spot checks, and reviews of self-identified violations. The SPP RE Enforcement group reviews the Compliance groups' findings of noncompliance, notifies registered entities and NERC of possible violations, reviews and verifies

registered entity mitigation plans, determines proposed monetary penalties and non-monetary sanctions, and participates in settlement negotiations. To meet its RDA and ROP obligations and its goals, SPP RE has increased its Compliance and Enforcement staff and its budget.

All SPP RE auditors are required to attend various SPP RE internal auditor training sessions, consultant-provided auditor training sessions, NERC auditor training modules, NERC ATL training, and ERO auditor workshops. Out of the ten personnel assigned to the Compliance groups, one is a NERC-certified system operator, five are certified information system auditors, and four are registered professional engineers.

SPP RE requires all auditors participating in an audit to undergo a conflict of interest review to identify any potential conflicts of interest between an auditor and the registered entity. Similarly, SPP RE also created a *Contractor Conflict of Interest Audit Procedure* that establishes due diligence requirements for the review of contractor conflicts of interest, validates and documents requirements concerning gaps in contractor employment, and identifies contract consulting history.

Compliance Monitoring Tools and Procedures

SPP RE utilizes numerous tools to facilitate its audits, several of which are highlighted here. SPP RE's audit teams maintain an audit workbook to facilitate evidence request tracking. SPP RE also uses a compliance pre-audit survey, an audit opening and closing presentation template, an operator interview questions template, and a control center checklist template. For CIP audits, SPP RE has implemented the use of a Network Access Policy Tool (NetAPT), which helps auditors with the visualization of the registered entity's network architecture. SPP RE also utilizes a secure file transfer protocol (FTP) server (EFT server) to facilitate the upload and continuous protection of audit evidence.

Quality Assurance

SPP RE's audit process requires all members of the audit team to participate in the review of evidence and SME interviews. The auditors collectively determine a registered entity's compliance with NERC Reliability Standards. All audit findings are reviewed and approved by SPP RE management. After the Compliance group completes a preliminary screen of a potential noncompliance, it enters the potential noncompliance into SPP RE's webCDMS, and notifies the registered entity and NERC of the potential noncompliance. The Compliance group and the Enforcement group then convene a hand-off meeting to discuss the audit findings. If the Enforcement group determines that sufficient evidence exists to support a possible violation, then the Enforcement group sends the registered entity a notice of a possible violation. The Enforcement group conducts a thorough secondary review of all possible violations before final disposition of a registered entity's noncompliance.

Guidance and Training for Industry Stakeholders

The SPP RE Outreach staff works closely with the SPP Regional Transmission Organization (RTO) Outreach and Training staff to coordinate an array of training opportunities for all of the registered entities in the SPP RE footprint. In 2013, SPP RE and SPP RTO provided approximately 25,000 continuing education hours of training to over 1,800 participants.

Additionally, training related to Reliability Standards and compliance activities was provided to over 700 participants on webinars, over 800 participants at workshops and over 1,200 participants on conference calls.[57] All SPP RE workshops and webinars are free and open to the public. SPP RE frequently provides speakers to industry groups such as the Registered Entity SME conferences, executive conferences, and numerous SPP RTO technical groups and committees.

SPP RE continues to add to its library of training videos,[58] publish e-newsletters, and organize lessons learned educational sessions. SPP RE has worked to refine its workshop logistics and presentations, and continues to update the SPP RE webpages with relevant compliance materials. SPP RE's CIP Compliance team made an effort in 2013 to ensure registered entities undergoing a CIP audit understood that, as permitted by GAGAS, the SPP RE audit teams perform outreach activities during the course of the audit. This practice is communicated in the initial audit notice to the registered entity. The ATL periodically communicates with the registered entity during the pre-audit stage to gauge the effectiveness of outreach activities. If the entity is receptive to the outreach, this practice is reiterated during the opening audit presentation.

Maintaining Confidentiality

The SPP RE audit team strictly follows SPP RE's policies and procedures for the custody of confidential audit material. To ensure that the confidentiality of registered entity audit documents is maintained, SPP RE's uses a secure EFT server for storing the registered entity's data during the audit period. To provide yet another layer of protection, SPP RE stores all evidence documents in encrypted form.

Participation in RAI

SPP RE designated two SPP RE auditors as members of the ECEMG MTF that developed the Auditor Manual. In addition, SPP RE designated one SPP RE auditor as a member of the Pilot Evaluation Committee, and two auditors participated as observers during the ReliabilityFirst entity risk assessment pilot for American Electric Power Service Corporation. SPP RE designated three auditors as members of the RSAW Task Force RAI project, where they assisted in the development of new RSAW templates and a Compliance Application Notice conversion process for the new RSAWs. As a member of the Enforcement Functional Group, SPP RE helped draft the *ERO Enterprise Mitigation Plan Guide* and provided input during the development of the NERC Aggregation and Compliance Exception pilot programs. Internally, SPP RE has taken steps to facilitate the Compliance Exception process by adopting changes to its webCDMS and by implementing a triage process for the screening of incoming compliance issues to identify candidates for compliance exception. A SPP RE registered entity is also participating in the CIP Version 5 transition study to identify issues related to the transition from CIP Version 3 to CIP

[57] *See 2013 Compliance Outreach Report* (December 3, 2013), which was discussion item 3H at the December 10, 2013 SPP RTO Board of Directors/Members Committee meeting, available at: http://www.spp.org/publications/BODAGD&BKGD121013.pdf.

[58] SPP RE's video library received the Bronze Quill Award of Merit from the International Associated of Business Communications, Arkansas Chapter (April 2014), available at: http://vimeopro.com/sppcompliance/re.

Version 5. SPP RE CIP Compliance staff is working closely with the registered entity to identify and document transition compliance issues. SPP RE has provided training on the RAI program during its workshops and continues to support RAI by conducting outreach as RAI unfolds.

viii. Texas Reliability Entity, Inc.

Department Structure / Staffing / Conflict of Interest Avoidance

During the assessment period, Texas RE increased its compliance audit staff from 13 to 19 employees, and increased its registration and certification staff from one to two employees plus a supervising director. Audit teams typically consist of the ATL, a dedicated clerk, and team members auditing a subset of requirements included in the audit scope. Many audit team members have over 20 years of industry experience. In 2012, NERC determined that Texas RE needed to increase its CIP audit staffing levels to ensure its continued ability to perform compliance monitoring activities. Since then, Texas RE has increased its dedicated CIP audit staff from four to five employees and cross-trained several Operations and Planning auditors to assist with the workload.

Texas RE auditors participate in various Texas RE internal auditor training sessions, consultant-provided auditor training sessions, NERC auditor training modules, NERC audit team lead training, and ERO auditor workshops. Texas RE has published an audit procedure manual, which contains procedures for confidentiality, training, conflict of interest, and a procedure related to confirmation that the auditor has completed approved training. Texas RE employees must attend ethics and confidentiality training annually and sign agreements confirming that they will disclose any potential conflicts of interest and maintain the confidentiality of registered entity information. During Texas RE's audits, ATLs confirm that confidentiality and ethics agreements have been signed by all audit team members.

Compliance Monitoring Tools and Procedures

Texas RE utilizes a number of tools to execute its audits, several of which are highlighted in this section. Texas RE's compliance management tools, specifically its audit planning publications, audit procedures, audit agenda, and audit team expectations document, serve to organize the responsibilities of each audit team member, provide audit timelines, and include a comprehensive achievement matrix of audit milestones.

Texas RE audit teams utilize NERC's *Actively Monitored List of Reliability Standards* (AML) to identify requirements applicable to the audited entity and to scope audits. They use NERC's RSAWs and Texas RE's CMEP guidelines, which are sometimes used to expand the scope of an audit and include Regional Entity-specific reliability compliance requirements. They also employ a RAT-STATS statistical tool to select testing samples and create a workbook addressing each audited compliance requirement. Texas RE developed a CIP audit checklist used during the walk-though portions of a CIP audit to identify critical assets, critical cyber Assets, access points, and all other cyber assets within the electronic security perimeter. Texas RE's CIP audit checklist tool ensures that all areas of audit concern are addressed. Additional examples of audit tools used during on-site audits and throughout the period leading up to an audit include

email notifications, worksheet summaries, and spreadsheet tables for tracking evidence, and for delivering updates to the registered entity and to audit team members.

One of the notable improvements in the auditing process was Texas RE's implementation of webCDMS software in 2012, which allowed it to eliminate the manual tracking and reporting processes and synchronize document submission with NERC's database. Texas RE has also updated its audit desk procedures to ensure that auditors are using uniform processes to determine the scope of audits, notify entities of audits, document audit findings, and ensure that draft audit findings are reviewed by management before being sent to registered entities.

Quality Assurance

Texas RE's audits are led by the Texas RE ATLs, who coordinate audit activities and communicate issues pertinent to the performance of the team's work. These teams meet to review the progress of the audit and at the close of the day, the ATL meets with the entity to review audit progress and clarify the status of outstanding data requests and delivery expectations. All audit documentation is saved on a secure server and is subject to a formal document retention schedule. On the last day of the on-site portion of an audit, the audit team provides a summary briefing to the registered entity, describing any possible issues the team identified. The audit manager also reviews the draft audit findings before providing them to the registered entity for comment. At the conclusion of the audit, the audited entity is provided a questionnaire asking for comments on how the audit process could be improved. Questionnaires are reviewed by Texas RE management and lessons learned from the feedback are shared with audit staff.

Guidance and Training for Industry Stakeholders

Since 2009, Texas RE increased its training resources for its Training, Education, and Operator Certification program, which provides continuing education hours through the NERC Continuing Education program. Texas RE dedicated 0.6 FTE to its Training, Education, and Operator Certification program in 2009.[59] Last year, Texas RE delivered its 2013 training program through 1.75 FTEs.[60] Texas RE has an external relations manager and a communications and external relations coordinator who coordinate scheduling of training and development of training materials; however, most training is conducted by auditors from Texas RE's Compliance department. In an effort to improve outreach and training for smaller registered entities with insufficient resources to participate in-person at compliance workshops, Texas RE offers webinar capabilities. On occasion, Texas RE conducts smaller, in-person training presentations for stakeholders unable to attend annual workshops, but that are experiencing compliance issues identified during audits.

Texas RE offers the following additional sources of guidance and training to industry members:

(1) A website with information about Texas RE and its activities, including links to CMEP information and enforcement information;

[59] 2010 Business Plan and Budget, Texas Regional Entity, Inc., June 15, 2009.

[60] 2013 Business Plan and Budget, Texas Regional Entity, Inc., June 27, 2012.

(2) A listserv for distribution of announcements;

(3) Monthly regional stakeholder CIP working group meetings which must be attended in person due to the sensitive nature of the shared information;

(4) "Talk with Texas RE" webinar meetings, which facilitate open discussions of reliability and compliance issues with stakeholders;

(5) Teleconference meetings of the NERC Standards Review Subcommittee (a subcommittee of the Texas RE Reliability Standards Committee) approximately every two weeks, which serve as a forum for discussion of NERC Reliability Standards under development; and

(6) The *Texas REview* a monthly newsletter which includes topics related to NERC compliance (including reminders about compliance deadlines), enforcement, and lessons learned.

Maintaining Confidentiality

Texas RE requires all employees to attend ethics and confidentiality training annually and to sign an agreement requiring them to keep registered entity information confidential. Texas RE also has procedures requiring its employees to keep all compliance information confidential. Texas RE has a hotline and website where anyone can file a complaint regarding a registered entity's compliance with NERC Reliability Standards, and the complainant may remain anonymous. In addition, Texas RE safeguards the confidentiality of registered entity data by using a secure compliance data portal (WebCDMS), using a secure FTP site for data submission, and maintaining data server security through the use of firewalls, system monitoring and penetration testing. All Texas RE staff are also required to complete annual IT and physical security training.

Participation in RAI

Texas RE has been working with NERC and the other Regional Entities to implement RAI. In 2013, Texas RE worked with NERC and the other Regional Entities to develop the *Compliance Auditor Checklist*, and provided significant support toward the development of the *Compliance Auditor Handbook*, as found in the Auditor Manual. In 2014, Texas RE helped evaluate the effectiveness of the RAI pilot programs conducted in other Regional Entities. Texas RE is working to encourage collaboration, emphasize consistency and align proven processes. Texas RE co-hosted an RAI and Internal Controls workshop in February 2014, and a follow-up meeting with Texas RE in March 2014 to answer questions received during and after the workshop.

ix. <u>Western Electricity Coordinating Council</u>

Department Structure / Staffing / Conflict of Interest Avoidance

FERC issued its final orders on February 12, 2014 approving the bifurcation of WECC. Bifurcation resulted in a more focused reliability assurance mission for WECC and Peak

Reliability (Peak) (the new company formed to be the reliability coordinator for the Western Interconnection). WECC will continue as the Regional Entity for the Western Interconnection and focus on RAI activities as it assumes the role of compliance enforcement authority for Peak along with all other registered entities in WECC's footprint. That role includes monitoring and enforcing compliance with mandatory Reliability Standards, as well as having a leadership role in reliability planning and performance assessment of the BPS in the Western Interconnection.

Since January 2009, the Compliance staffing at WECC has increased from 31 to 53 employees, not counting contractors. Staffing increases have occurred throughout Compliance to satisfy the CMEP requirements associated with the increased number of registered entities and registered functions, which to date respectively total 510 and 1,353 respectively, up from the 466 and 1,248 reported in 2009. WECC's number of scheduled audits has almost doubled from 98 in 2009 to 171 in 2013.

WECC's Program Administration department was established in 2008 and restructured in 2012 to ensure the accurate, efficient, and timely exchange of compliance information between registered entities, WECC, and NERC. The department supervises the services and support used by the registered entities and WECC employees to interact with such systems as webCDMS and the WECC EFT server. Staff in this department are currently comprised of one manager and six employees.

Since 2009, the WECC Compliance department has put in place a rigorous training and development program. Like other Regional Entities, WECC struggled initially to fill both Operations and Planning and CIP auditor positions. A recruitment and development plan to recruit, graft and grow expertise included mentoring, cross-training and implementing development milestones programs. WECC also benefits from using industry SMEs as contractors for its audits. These contractors possess operations, planning, and power system knowledge as well as skills and abilities that complement that of WECC's audit staff to fill gaps where specific deficiencies may exist. WECC partners these contractors with less experienced auditors at each audit to provide detailed and in-depth on-the-job training, and educational experiences regarding specific Reliability Standards and requirements. Additionally, all CIP auditors hold at least one relevant certification (e.g. CISA, CISSP).

Audit teams regularly participate in cross-training within their own team through constant rotation in ATL responsibility. In addition, auditors in teams of two are frequently assigned different Reliability Standards and requirements to audit, depending on an audit's scope. This approach provides varied and valuable training opportunities to increase auditor knowledge of and expertise on multiple Reliability Standards. Operations and Planning and CIP SMEs from both Compliance and Enforcement are assigned to participate with auditors on the audit team for at least two audits per year as part of the cross-training effort. This results in a greater understanding of the WECC audit approach by the Enforcement team SMEs, while providing much needed "bench strength" to the audit teams and their ability to satisfy audit staffing requirements. Both Operations and Planning and CIP audit team members in WECC have participated in various WECC internal auditor training sessions, consultant-provided auditor training sessions, NERC auditor training modules, NERC ATL training, and ERO auditor workshops.

WECC conducts conflict of interest checks for its auditors and contractors. WECC's compliance program coordinators (CPCs) are responsible for distributing and collecting these forms. These forms are reviewed by the audit managers and the managing director of compliance at the beginning of every year. In August 2013, WECC included the additional step of having the CPC and the ATL review these forms in connection with every audit, as part of WECC's preliminary audit preparation. This will add an extra layer of review to ensure that the conflict of interest forms are complete and accurate. WECC has also codified these existing and new processes in the CPC informal process manual as part of a basic checklist for audits.

Compliance Monitoring Tools and Procedures

WECC utilizes a number of tools to execute its audits, several of which are highlighted in this section. WECC performs audits in the timeframes anticipated by the CMEP. WECC's Operations and Planning audit teams rely primarily on RSAWs to record audit findings, interview notes, evidence and samples. While WECC did not initially follow GAGAS audit procedures to conduct audits, particularly in the areas of planning, scope, evidence, testing, sampling and documentation, WECC later adopted various professional resources such as the GAGAS, NERC auditor training guidance and other best practices. WECC leverages the *Compliance Auditor Handbook* and associated *Compliance Auditor Checklist* (as found in the Auditor Manual) in addition to the WECC CIP standard operating procedures for documented audit procedures.

The audit teams use a number of secure tools, leveraged by PGP encryption methodologies, to manage the administrative and logistical support for audits. The primary tool used by the audit team is an Audit Remote File server used to expedite the availability of electronic information to auditors during a remote audit. This tool works in conjunction with WECC's EFT server and the WECC internal Sharedrive. When an entity uploads audit evidence to the EFT server, a WECC employee is notified of the change and moves the files to the correct location within the WECC internal Sharedrive. The software then automatically synchronizes the files on WECC's internal Sharedrive with the files on the Audit Remote File server. This system allows all users to access the exact same information from different connection points.

In 2013, WECC launched the Audit Tracking System (ATS) to help manage the tracking, and the timely completion and filing, of audits. The software minimizes rework, helps prevent errors in documentation, and ensures that all related tasks are completed in a timely manner. There are four pieces to the new ATS: audit scheduling, audit metrics, audit library, and audit report task list. Another feature of the ATS is that metrics are now readily and easily available to managers through the system. The system uses an Audit Library to minimize document duplication by tracking the version history on each file and eliminating multiple copies of the same report. Finally the system incorporates an audit task list that reduces manual oversight by electronically tracking task assignments, completions, and notifications.

WECC has been able to greatly reduce the amount of human and budget resources required for compliance support activities. Actual expenditures in 2010 exceeded $1.9 million; in 2012 that number dropped to less than $1.1 million. Starting in 2012, WECC began to concentrate on operational efficiencies that could simplify the growing complexity of managing compliance data and transactions. The single greatest change in that process was upgrading the compliance transaction platform from the WECC Compliance Portal to webCDMS. The new system brought

drastic reductions in the amount of time WECC employees spent on sending data requests, sending reminder notices to registered entities, summarizing compliance data, and transmitting compliance data to NERC.

WECC created an audit report tool that provides readable access to critical data, drives visibility across audit team members and management, and improves the efficiency of the audit report processes. This project streamlines the audit schedule activities and audit report process for audit management, ATLs, and CPCs. The solution minimizes rework, helps prevent errors in documentation, and ensures that all related tasks are completed in a timely manner. This tool also enables management and audit team members to understand workload and prioritize items. Prior to the launch of this tool, significant time and effort was spent on manual oversight.

WECC also created the Compliance Standards Index (CSI). The CSI works by drawing on a number of data sources to place relevant information about Reliability Standards in a single view. The CSI queries NERC's Reliability Standards database, which is the repository for the most current and updated information on Reliability Standards. The system then combines this data with related information such as a link to the WECC RSAW and the WECC AML. Altogether, the CSI allows users to get a more complete view of applicable Reliability Standards.

Quality Assurance

Audit findings are reviewed by the entire audit team, including the ATL, before a possible violation is identified. All possible violations are then reviewed by an Enforcement SME for confirmation. All audit reports and findings are reviewed and approved by senior Compliance management before being sent to the registered entity and NERC. Post audit feedback forms are completed by audited registered entities and reviewed by the ATL, the audit team and senior Compliance management before being discussed in auditor staff meetings. Lessons learned are discussed on an informal basis in both the Operations and Planning and CIP audit team meetings. CIP audit teams document lessons learned and store them on an internal secure WECC server for future auditor review and reference. Audit documents, including evidence, data and reports, are stored on a dedicated drive and SharePoint and archived according to the WECC formal data retention policy of five years.

Guidance and Training for Industry Stakeholders

Beginning in 2009, WECC has offered annual training sessions and workshops for operators, schedulers, and dispatchers. During the assessment period, WECC decreased its training resources for its Training, Education, and Operator Certification program, which provides continuing education hours through the NERC Continuing Education program. WECC dedicated 3.5 FTE to its Training, Education, and Operator Certification program in 2009.[61] Last year, WECC delivered its 2013 training program through 1.5 FTEs.[62]

WECC formalized a compliance outreach program in the fall of 2008 with the hiring of a designated individual to act as a liaison with the registered entities and to coordinate various

[61] 2009 Business Plan and Budget, Western Electricity Coordinating Council, July 9, 2008.

[62] 2013 Business Plan and Budget, Western Electricity Coordinating Council, June 25, 2012.

compliance outreach activities. The director of compliance outreach reported directly to the WECC CEO at that time. This reporting structure assured the separation of Outreach and Compliance Audit and Enforcement. In January 2011, the scope of this position expanded to include outreach to other interested stakeholders. The current position is managing director of stakeholder outreach which reported to the vice president of communications and external affairs during the assessment period and now reports to the vice president and chief administrative officer. This individual is responsible for the coordination of all compliance outreach activities as well as ad hoc outreach for other WECC areas, as appropriate (e.g. BES definitional process).

Below are examples of WECC outreach to registered entities:

(1) WECC hosts three Compliance User Group (CUG)/Critical Infrastructure Protection User Group (CIPUG) meetings annually. These meetings, held over three days, allow time for industry-only Western Interconnection Forum (WICF) sessions. Attendance records (kept electronically since 2011) indicate that participation continues to increase yearly while satisfaction surveys show favorable responses. The CUG/CIPUG agendas cover a wide range of topics including management updates, regulatory actions, industry trends, new Reliability Standards, audit approaches and best user practices. Registration for 2011 through 2013 was 5,717.

(2) WECC hosts open webinars on the third Thursday of most months. These sessions are used to provide time-sensitive updates on topics and issues that arise between CUG meetings and reminders of upcoming events and deadlines. Participation is also very good in this Outreach program with 150 to 250 active ports for each webinar. WECC added real time video streaming capability in 2013.

(3) Starting in January 2011, enforcement SMEs started conducting outreach events to educate registered entities about best practices in submitting information to WECC, and mitigation and prevention of violations. Some of the specific outreach activities include:

(a) Eight Steps for Prevention and Mitigation – The goal of this outreach presentation was to share best practices in creating effective mitigation plans. It provided registered entities eight important elements to consider while creating a mitigation plan for a violation.

(b) Detection and Future Prevention – The goal of this outreach program was to highlight the importance of determining the root cause and implementing strong detection and preventative measures to reduce the likelihood for future recurrence of violations and security issues.

(c) Reliability Standard Specific Outreach – Enforcement SMEs have conducted various events to discuss the audit approach, root cause analysis and effective mitigation solutions for most commonly violated Reliability Standards in the WECC region. Some of these Reliability Standards include: PRC-005; PER-002 and PER-003; PRC-023; VAR-002; and CIP-007.

(4) The WICF is run by and on behalf of entities subject to WECC and NERC compliance requirements. The purpose of WICF is to provide registered functional entities within the Western Interconnection a venue to share knowledge and lessons learned regarding compliance matters, and to collectively develop best practices.

(5) CIP 101 is a two-day class held generally in WECC's Salt Lake City, UT meeting space and is taught by WECC cybersecurity auditors. This class has been offered three times and has sold out each time. Agendas include comprehensive discussions of CIP Reliability Standards, audit approaches, best evidence and interactive work between participants and the WECC auditors.

(6) A "Compliance 101 Webinar" which is a 90-minute session offering an overview of the development of the mandatory compliance program and its major parts. WECC offers this webinar just before each CUG/CIPUG meeting to aid those new to their compliance duties or who may just want refresher training.

(7) WECC hosts compliance systems (EFT/webCDMS) training and webinars providing registered entities with an opportunity to learn about the improvements to these electronic systems.

Maintaining Confidentiality

WECC employs a number of security measures to protect confidential compliance information. WECC laptops with access to confidential information have encrypted hard drives, minimizing the risk of that information being disclosed in the event of a lost or stolen laptop. WECC requires employees to change the passwords on their laptops every 90 days. WECC's offices have physical security measures including badge readers, access badges for all employees, and video cameras which cover the building entrances and exits. There is also an on-site security guard for the building during business hours. Visitors must be escorted by WECC employees in nonpublic areas of the offices. Additionally, WECC uses two secure portals/repositories for registered entity submittals: webCDMS and the EFT server.

Participation in RAI

As part of the RAI, WECC volunteered for the ECEMG MTF that created the Auditor Manual. WECC has also provided its internal training materials to NERC, at its request.

WECC completed its first RAI pilot in 2013 with limited scope and time. WECC provided recommendations to the entity to further consolidate its internal controls. Based on the results, WECC customized the self-certification requirements for the entity. WECC used the entity's feedback to improve its internal controls evaluation process. In May 2014, WECC completed its second RAI pilot. WECC highlighted best practices and recommendations to the entity. A WECC audit team used the results of the controls evaluation to exclude certain requirements from the entity's compliance audit. The entity was also selected for the Compliance Exception pilot. The

entity provided helpful and positive feedback which WECC has used to improve the evaluation process. Currently, the third RAI pilot is in progress.

C. Compliance Investigations

The Compliance Investigations group provides quality assurance of the Regional Entities' compliance evaluations of industry compliance assessments from events that have occurred in their footprints. The Compliance Investigation group's process articulates NERC's technical investigations staff review and facilitates a compliance evaluation of BPS events as they relate to the entities involved in the event. It also outlines subsequent compliance responsibilities under the NERC Reliability Standards.

NERC's Compliance Investigations group works closely with Regional Entity compliance staff to review significant BPS disturbances. These reviews include evaluation of events from a compliance perspective, which includes a review of possible gaps in existing NERC Reliability Standards. During such events, registered entities are encouraged to conduct a compliance self-assessment and submit these assessments to the relevant Regional Entity for review. The registered entity is encouraged to self-report possible violations it identifies during this self-analysis. In its oversight role, NERC reviews and analyzes each compliance self-assessment to ensure consistency and to initiate lessons learned or compliance monitoring follow-up activities.

At the beginning of the assessment period, compliance investigations and event-driven compliance evaluations proved difficult to complete at the Regional Entity level, in part due to the need for more resources. NERC found that the Regional Entities had difficulty determining which BPS events required a more detailed review and in understanding what was required of them in compliance investigations. As further detailed in the *Overview of NERC Activities and Accomplishments in the Five-Year Period*, these issues were addressed through several initiatives including the creation of the ERO Event Analysis program and NERC's development of a compliance investigations leaders training class for NERC and Regional Entity staff compliance investigators. The compliance investigations leaders training material is continuously reviewed and improved based on feedback from compliance investigation experiences and changes to GAGAS, CMEP, and the NERC ROP. As a result of these efforts, the Compliance Investigations group regularly processes over 30 events per year and works with the Events Analysis group to publish relevant NERC alerts.

In addition, the Compliance Investigations group handles all complaints reported to NERC regarding alleged violations of NERC's Reliability Standards. These matters are reported through the compliance hotline or by voice messaging. Between March 2009 and December 2012, NERC in collaboration with the Regional Entities, received, processed and closed all 70 complaints that were received by the ERO.

D. Compliance Enforcement

1. Performance of the ERO Enterprise

a. Overview

During the assessment period, the Regional Entities made remarkable progress in establishing mature, effective enforcement programs consistent with their obligations under the RDAs and the NERC ROP. The RDAs delegate authority over enforcement of compliance with Reliability Standards. The RDAs provide that NERC shall review the Regional Entities' CMEP as often as NERC deems necessary to ensure that: (1) the Regional Entity's program meets all applicable legal requirements; (2) the actual practices of the Regional Entity reflect the requirements; and (3) the program promotes consistent interpretations across North America of Reliability Standards and comparable levels of sanctions and penalties for violations of Reliability Standards constituting comparable levels of threat to the reliability of the BPS.[63] The NERC ROP require the Regional Entities to make initial determinations of compliance or noncompliance and recommend penalties where authorized,[64] apply penalties and sanctions that bear a reasonable relation to the seriousness of a violation and that follow the directives, principles, and processes set forth in NERC's *Sanction Guidelines*,[65] regularly report on the status of the review and assessment of violations of Reliability Standards as well as associated mitigation plan information,[66] and obtain sufficient resources to meet their delegated obligations, including maintaining sufficient staffing.[67] NERC, as part of its oversight role, regularly reviews Regional Entity enforcement activities to ensure that these obligations are being satisfied and to drive the implementation of best practices in enforcement activities throughout the ERO Enterprise. NERC's oversight activities provide an ongoing view of the Regional Entities' effectiveness in executing their compliance enforcement responsibilities.

At the time of the *Three-Year ERO Performance Assessment Report* (mid-2009), the NERC Reliability Standards had been mandatory and enforceable for just over two years. Early in the implementation of the uniform CMEP, the Regional Entities successfully identified some 2,000 violations from the over 2,700 reported possible violations.[68] Additionally, the Regional Entities addressed a large number of self-reported Reliability Standard violations[69] from the period before

[63] Section 6 of each RDA contains the provisions relating to delegation of compliance monitoring and enforcement authority.

[64] NERC ROP §402 (NERC Oversight of the Regional Entity Compliance Monitoring and Enforcement Programs).

[65] NERC ROP §401 (Scope of the NERC Compliance Monitoring and Enforcement Program); *Sanction Guidelines* are Appendix 4B to the ROP.

[66] *See* NERC CMEP, NERC ROP Appendix 4C, at §6.0 (Mitigation of Violations of Reliability Standards).

[67] NERC ROP §403 (Required Attributes of Regional Entity Compliance Monitoring and Enforcement Programs).

[68] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 10-11.

[69] Unless otherwise indicated, "violation" refers to any report of noncompliance submitted to a Regional Entity, regardless of its status as a possible, alleged, or confirmed violation or whether the noncompliance was or will be processed as a "remediated issue" through the Find, Fix, Track and Report (FFT) track.

the Reliability Standards became mandatory and enforceable.[70] NERC recognized in the three-year performance assessment the success of the Regional Entities in the cataloging, processing, and tracking of each violation and the completion of the associated mitigation plans. NERC also recognized that substantial work remained to be done to complete the transition to a more mature enforcement program. In the three-year performance assessment, NERC noted several areas of improvement for the Regional Entities, including increasing the speed of processing violations (and associated mitigation plans) and improving upon the thoroughness and accuracy of the information provided to support each Notice of Confirmed Violation (NOCV) or settlement agreement submitted to NERC for review.[71]

During the current assessment period,[72] NERC and the Regional Entities worked to develop more mature enforcement processes for the ERO Enterprise. NERC and the Regional Entities collaboratively implemented streamlined enforcement processing mechanisms, such as the Spreadsheet Notice of Penalty (SNOP) and FFT enforcement mechanism.[73] NERC and the Regional Entities also worked together to design and build a system for the collection, management, and exchange of compliance-related information between NERC and the Regional Entities. The Regional Entities implemented compliance data systems that interface with NERC's Compliance Reporting, Analysis, and Tracking System (CRATS). These complementary systems are the webCDMS, which is used by MRO, ReliabilityFirst, SPP RE, Texas RE, and WECC, and the CITS, which is used by FRCC, NPCC, and SERC. These systems enable enforcement processing efficiencies and facilitate consistent tracking of violation status across the ERO Enterprise. These systems are continuously evaluated and improved.

For several years, NERC has closely tracked various aspects regarding the overall performance of the ERO Enterprise as it relates to enforcement activities. Beginning in 2013, NERC and the Regional Entities developed and implemented a series of metrics to track and evaluate the performance of the ERO Enterprise and of each Regional Entity. These metrics allow NERC to analyze trends and identify areas where further improvements may be achieved. To facilitate consistent application of these metrics, NERC and the Regional Entities agreed to a set of business rules to govern submission of data to the complementary compliance data systems. For 2014 and beyond, NERC and the Regional Entities have agreed to use some of these metrics to measure achievement of the goals of the *ERO Enterprise Strategic Plan*.[74] Although these metrics were not in place during the entire assessment period, they provide insight into the current status of enforcement processing in the ERO Enterprise, and therefore are used in this evaluation.

NERC recognizes the substantial progress each Regional Entity has made in addressing the enforcement-related issues raised in the three-year performance assessment. NERC also

---

[70] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 12.

[71] *Three Year ERO Performance Assessment Report*, Attachment 3 at 11-12.

[72] For purposes of evaluating the Regional Entities' activities, NERC has used a five-year period of January 1, 2009 to December 31, 2013.

[73] The SNOP and FFT enforcement mechanisms are described in §II.D.b.iv below.

[74] *See ERO Enterprise Strategic Plan 2014-2017*, available at: http://www.nerc.com/gov/Annual%20Reports/ERO%20Enterprise%20Strategic%20Plan%202014-2017%20and%20Performance%20Metrics.pdf.

recognizes the progress each Regional Entity has made in improving consistency and transparency in enforcement-related processes. However, and as explained more fully below, NERC has identified the need for additional improvements with respect to enforcement processing and the Regional Entities' implementation of certain aspects of the CMEP.

This assessment of the enforcement activities of the Regional Entities begins with a discussion of the collective accomplishments of the ERO Enterprise with respect to enforcement processing and a discussion of general recommendations for areas of improvement. Topics that will be covered include ensuring the timely processing and mitigation of older violations, ensuring the quality of data in the compliance data tracking systems, ensuring the quality of submitted information in settlement agreements and NOCV, and NERC's oversight of the performance of the Regional Entities with respect to certain areas of the CMEP. The analysis of the collective accomplishments of the Regional Entities in enforcement is followed by in-depth analysis of the performance of each Regional Entity in executing its compliance enforcement responsibilities.

b. Improvements in Enforcement Processing, 2009-2013

In 2009, at the time of the three-year performance assessment, the Regional Entities had collectively accumulated what was described as a substantial backlog of cases. Of the total 1,926 violations identified by the Regional Entities, only 475 violations had been filed with NERC for its review and for Board of Trustees Compliance Committee (BOTCC) approval as of May 31, 2009. Roughly 75 percent of all violations that had been identified remained to be processed by Regional Entity staff.[75]

During the current assessment period, the Regional Entities have made substantial progress in reducing the number of open violations, despite substantial increases in the numbers of new violations during the assessment period.

i. The Composition of the ERO Enterprise Caseload

As shown by the table below, 10,163 violations were reported to NERC by the Regional Entities during the current assessment period. The Regional Entities reported a significant increase in the number of violations from 2010 through 2012, in large part due to the implementation and enforcement of the CIP Reliability Standards:

[75] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 11.

Violations for all Regional Entities 2009-2013 by Year Reported to NERC
U.S. Violations Only[76]

Regional Entity	2009	2010	2011	2012	2013	Grand Total
FRCC[77]	188	109	141	69	61	568
MRO	60	103	196	166	139	664
NPCC	43	99	130	213	66	551
RFC	123	469	565	505	240	1902
SERC	187	312	309	300	285	1393
SPP RE	132	254	291	173	191	1041
TRE	14	51	430	197	169	861
WECC	571	550	807	818	437	3183
Grand Total	**1318**	**1947**	**2869**	**2441**	**1588**	**10163**

The drop in violations from 2012 to 2013 is attributable to a number of factors.[78] Since the Reliability Standards became mandatory and enforceable, most registered entities have completed at least one full audit cycle and in some instances more than one audit cycle. A number of registered entities have responded to their past compliance audits by improving their management practices, thus decreasing the likelihood of the Regional Entity discovering new violations in recent compliance audits. In addition, the Regional Entities have conducted significant and varied outreach activities. These efforts have included Operations and Planning standards workshops, CIP standards workshops, and training to enhance their registered entities' understanding of the Reliability Standards. Registered entities with better knowledge of the Reliability Standards have improved their compliance cultures, and therefore are less likely to have violated Reliability Standards. The drop in violations is also attributable to an enhancement in the preliminary screening processes as of December 2012. Specifically, this enhancement reduced the likelihood that new potential noncompliance issues were duplicates of issues already being processed.

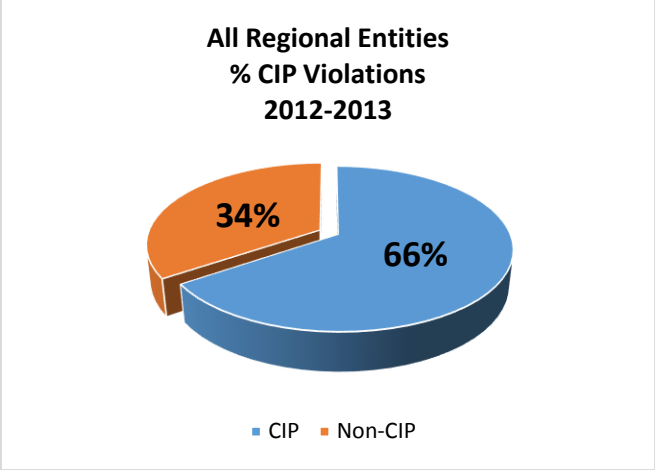
[76] This table reflects all U.S. violations that were submitted via the complementary compliance data systems to NERC's centralized database (CRATS) in 2009, 2010, 2011, 2012, and 2013. This table includes all violations, whether they were later dismissed or were held due to a court, regulator, or appeal. For some violations, the year the violation was discovered and the year the violation was first reported to NERC's centralized database are different. For example, a violation first discovered during an audit in late 2012 may not have been reported to NERC's centralized database until early 2013. Therefore, the total number of violations for a particular Regional Entity or a particular year may vary depending on whether violations are reported by discovery year or by year submitted to NERC's centralized database. To clarify, these differences, where they appear, are attributable to a difference in presentation and reporting rather than an underlying difference in the number of overall violations. For consistency throughout this analysis, the year the violation was first reported to NERC's centralized database is used in this five-year performance assessment unless otherwise specified.

[77] In the JRESA, FRCC reported violations by the year the violations were discovered, rather than the year the violations were submitted to NERC's centralized database. *See* JRESA at 41. As noted above, the differences between the numbers reported by NERC in the table above and the numbers reported by FRCC in the JRESA are attributable to the difference in presentation, rather than an underlying difference in the overall number of violations.

[78] This drop in violations appears whether the number of violations is presented by discovery year or by year reported to NERC's centralized database. When calculated by year of discovery, there was a 12% decline in violations from 2011 to 2012, and a 30% decline in violations from 2012 to 2013.

However, despite the decrease in the overall number of potential noncompliance issues identified, the composition of the ERO Enterprise caseload remained fairly consistent from 2012 to 2013. Since 2010, violations of the CIP Reliability Standards have comprised the majority of violations in each year, with the overall proportion of CIP violations increasing somewhat year over year. CIP violations comprised 66% of the total violations submitted to NERC's centralized database from January 1, 2012 through December 31, 2013.

Type of Violations Reported to NERC by all Regional Entities, 2012-2013

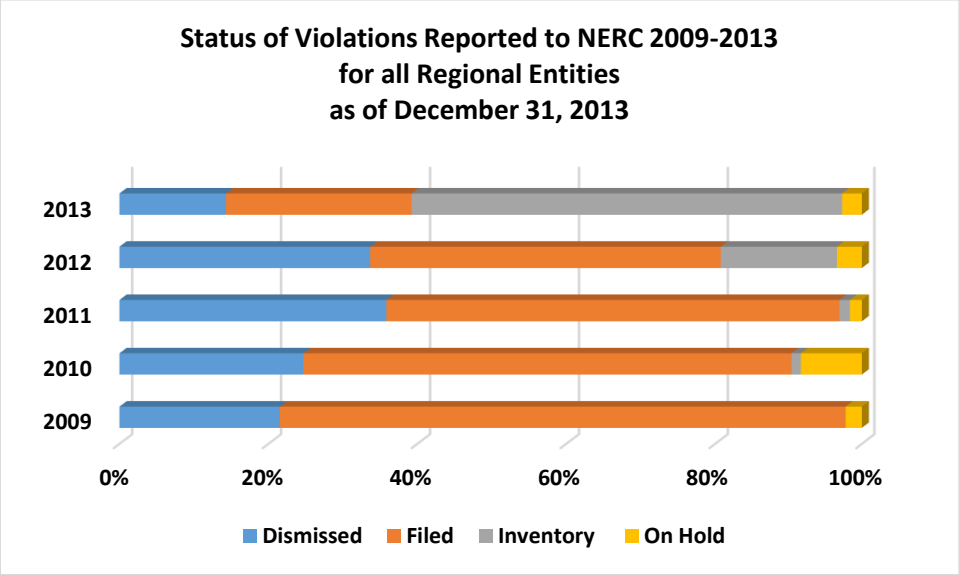


The top five most violated Reliability Standards were CIP-004, CIP-005, CIP-006, CIP-007, and PRC-005. The most violated Reliability Standards were generally consistent across the Regional Entities.

Despite the influx of CIP violations during the assessment period, the Regional Entities actively worked to reduce the number of open violations in their caseloads. As of December 31, 2013, the Regional Entities had processed 100% of the violations available to be processed that were reported to NERC in 2009; nearly 99% of the violations available to be processed that were reported to NERC in 2010 and 2011; and 84% of the violations that were reported to NERC in 2012.[79] Violations reported to NERC in 2012 and 2013 comprised over 95% of the total 1,375 violations available for processing as of December 31, 2013.

[79] NERC recognizes that the Regional Entities are not able to process certain violations because the violations are being held by or due to an appeal, a court, or a regulator. NERC refers to these violations as being "on hold." In evaluating the performance of the Regional Entities with respect to violation processing, NERC excludes any "on hold" violations.

Status of Violations Reported to NERC 2009-2013 for all Regional Entities



As of December 31, 2013, the majority of violations in the ERO Enterprise inventory (67%) consisted of violations reported to NERC in 2013.[80] In addition, during 2013, the Regional Entities processed approximately 39% of the new violations reported to NERC in 2013. By reducing the number of older violations, the Regional Entities are moving toward a caseload consisting primarily of newer violations. The efforts of the Regional Entities to process older violations in their inventories, which has resulted in the reduction in caseload, are described more fully in §II.D.1.b.iii below, Efforts to Reduce Older Caseload.

ii. The Caseload Index

As noted above, NERC and the Regional Entities developed a series of enforcement processing metrics to aid in monitoring and improving the efficiency of enforcement processing throughout the ERO Enterprise. The Caseload Index is one of these metrics. It is used to facilitate planning, coordination, and collaboration between NERC and the Regional Entities.

The Caseload Index is a snapshot of current enforcement processing rates. It measures the amount of time, in months, that it will take the ERO Enterprise (or an individual Regional Entity) to eliminate the existing inventory, assuming no new violations are received. This calculation is based on the processing rate of the previous 12 months. For example, if the Caseload Index is calculated on December 31, 2013, the time to process existing inventory will be based on the processing rate from January 2013 to December 2013. A lower Caseload Index indicates that the ERO Enterprise will need fewer months to clear out its existing inventory of violations available to be processed, based on the processing rate of the previous 12 months. A higher Caseload Index indicates that the ERO Enterprise (or individual Regional Entity) would need more months to clear

[80] The violations in "inventory" refers to identified violations that have not completed processing and are not "on hold."

out its existing inventory. The Caseload Index may fluctuate from month to month as violations are received and processed, but is helpful for evaluating performance over time.

NERC first began monitoring the Caseload Index in 2011 and has targeted achieving a lower average ERO Enterprise Caseload Index in each successive year. As of July 1, 2011, the average ERO Enterprise Caseload Index was 35 months. NERC set a goal to achieve an average ERO Enterprise Caseload Index of 24 months by the end of the year. By the end of 2011, the average ERO Enterprise Caseload Index was 24 months, meeting the goal and marking a substantial improvement from just six months earlier.

In 2012, the calculation of the Caseload Index was refined to account for matters processed through dismissal. The average ERO Enterprise Caseload Index as of December 31, 2012 was 13.3 months.[81] For 2013, NERC sought to achieve an average ERO Enterprise Caseload Index of under 10 months. Throughout 2013, the Caseload Index decreased fairly steadily to approximately 6.5 months at the end of the year.

The overall decrease in the ERO Enterprise average Caseload Index since 2011 reflects the substantial work by NERC and the Regional Entities to implement processing efficiencies and reduce the number of older open violations. These efforts are described more fully in the next section.

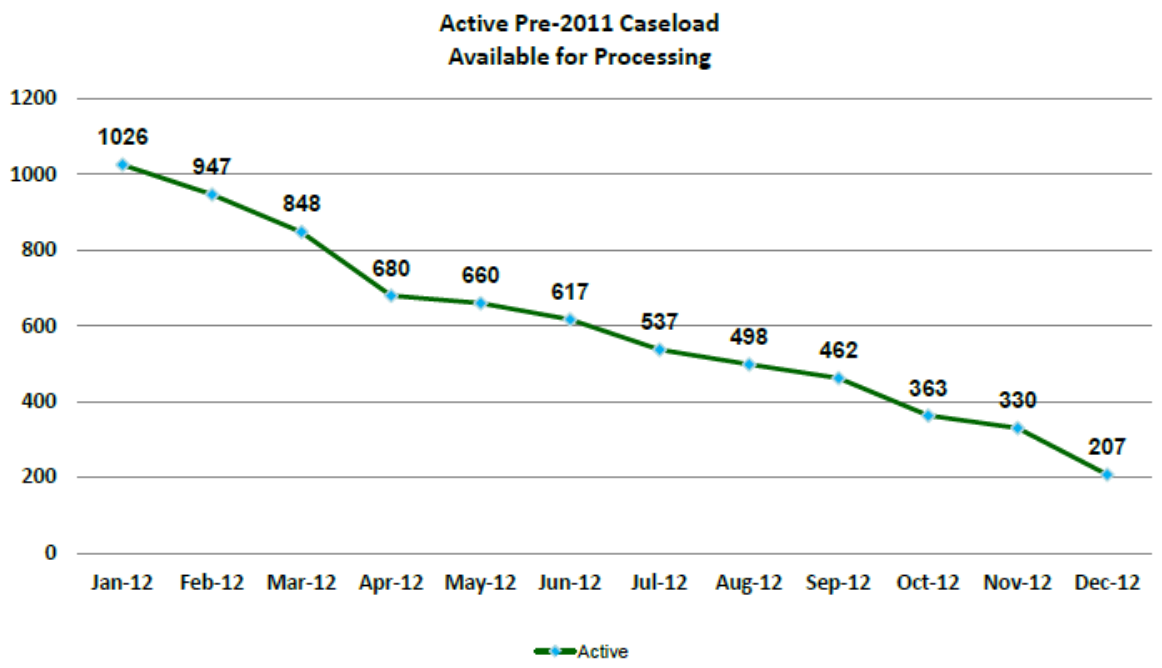
iii. Efforts to Reduce Older Caseload

In the Three-Year Performance Assessment, NERC noted that the Regional Entities needed to make substantial improvements in the processing of violations. NERC noted that the Regional Entities needed to reduce what NERC termed a "backlog" of aging violations. During the current assessment period, the Regional Entities made substantial progress in this regard. Whereas the Regional Entities had processed only about 25% of then-existing violations at the time of the Three-Year Performance Assessment in 2009, the Regional Entities have collectively processed more than 86% of violations reported to NERC from 2009 to 2013. The efforts of the Regional Entities to reduce the number of aging violations have been commendable. These efforts reflect the growth and maturity of enforcement staff across the ERO Enterprise and demonstrate the willingness of the Regional Entities to participate in the development and execution of common goals under NERC leadership and oversight.

In 2012, 2013, and 2014, NERC established corporate goals to reduce the number of older violations remaining to be processed. Working with NERC, the Regional Entities invested significant time and resources in processing the older violations. As a result, the ERO Enterprise reduced the number of open, older violations substantially. For example, during 2012, NERC and the Regional Entities successfully worked to reduce the number of open violations dating from before 2011 (excluding on-hold violations) by 80%, as shown below:

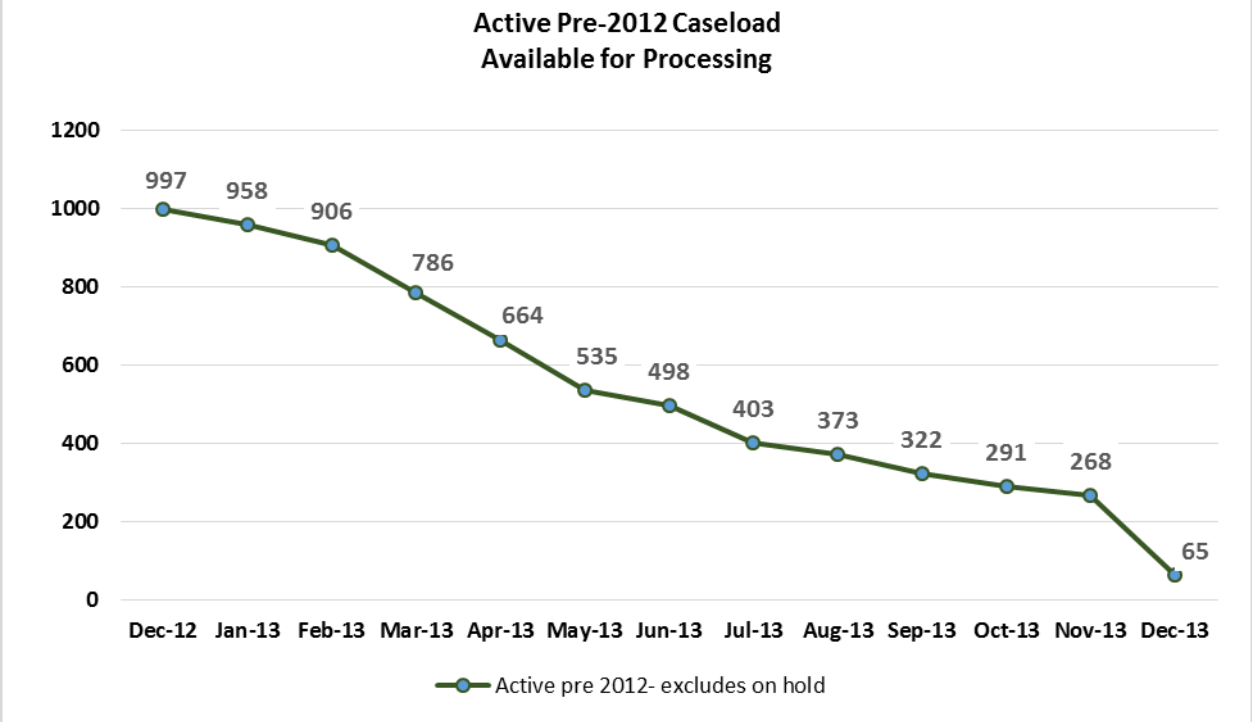
[81] For 2012, NERC established a corporate goal of 12 months for the ERO Enterprise average, with the threshold set at 19 months.

ERO Enterprise Caseload Consisting of Violations Discovered Before 2011 (excluding on hold violations), by Month in 2012



During 2013, the Regional Entities built on the successes of 2012. By December 31, 2013, NERC and the Regional Entities reduced the number of pre-2012 violations (excluding on hold violations) by 93%, as demonstrated below:

ERO Enterprise Caseload Consisting of Violations Discovered Before 2012 (excluding on hold violations), by Month in 2013



Only 65 violations discovered before 2012 remained to be processed as of December 31, 2013, representing less than one percent of total violations discovered from 2007 through 2011 and less than five percent of the violations available to be processed as of December 31, 2013. By working to reduce the number of aging violations while improving the processing speed for newer violations, NERC and the Regional Entities have reduced the average violation age from 11.86 months in 2012 to 11.2 months in 2013 – an improvement of nearly six percent.

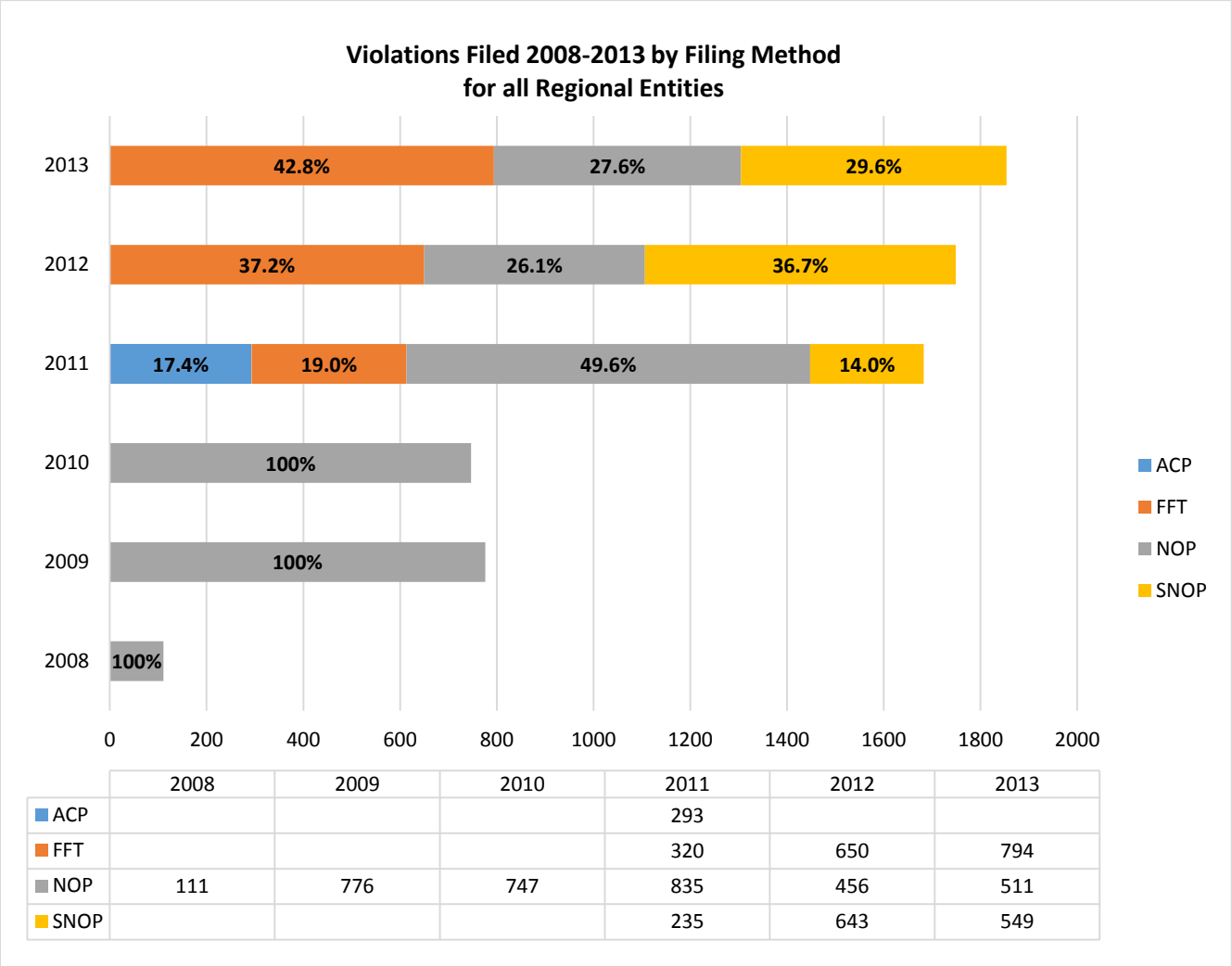
In 2014, NERC and the Regional Entities are continuing to work together to reduce the number of violations in inventory that are older than 24 months. These efforts will ensure that Regional Entities are prioritizing and resolving older violations appropriately. Combined with efforts to decrease processing times through the use of streamlined enforcement mechanisms and enforcement processing process refinements, the Regional Entities will reduce overall processing times and provide finality sooner to registered entities.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

During the five-year assessment period, the Regional Entities worked with NERC to develop, refine, and implement process improvements to ensure the timely processing of new violations while also allowing for the reduction of the number of older violations. Most notable among these process improvements was the development of streamlined enforcement processing mechanisms that simplify the process of filing violations with the Commission. These mechanisms include the SNOP and the FFT program.

At the time of the three-year performance assessment, NERC and the Regional Entities used the NOP mechanism to process all violations. Using only the NOP format, 1,634 violations were filed with the Commission from 2008 through 2010. In 2011, following the implementation of the Administrative Citation Process (ACP) and the FFT and SNOP processes, the Regional Entities collectively filed 1,683 violations – more than the previous three years combined.[82]

Violations Filed per Year by Filing Method, 2008-2013



	2008	2009	2010	2011	2012	2013
ACP				293		
FFT				320	650	794
NOP	111	776	747	835	456	511
SNOP				235	643	549

In 2012, the Regional Entities continued the implementation of the FFT and SNOP processes, which, along with the NOP, are the three enforcement processing mechanisms in use today. During the assessment period, the ERO Enterprise caseload consisted primarily of violations posing a lower risk to the reliability of the BPS. The FFT and SNOP processes proved to be especially useful for processing these lower-risk violations.

[82] The ACP was an alternative enforcement processing mechanism used to process a number of lower risk violations in 2011. The format was similar to the SNOP format currently being used.

In 2012, the number of violations processed by means of SNOP or FFT increased after the Regional Entities developed knowledge and experience with the new mechanisms. These methods accounted for over 70% of the total filed violations in 2012 and 2013. NERC and the Regional Entities continued to use the NOP format for violations that posed a serious and substantial risk to reliability, required the completion of substantial above-and-beyond mitigating activities,[83] or presented other facts and circumstances requiring a detailed presentation. Going forward, NERC expects the proportion and use of the filing mechanisms to evolve as the ERO Enterprise implements the process refinements being developed under RAI.

In 2013, NERC and the Regional Entities worked together to expand the FFT program by implementing the latest round of FFT enhancements, which were approved by the Commission in an order issued June 20, 2013.[84] These enhancements will also reduce the amount of time required to process issues through the FFT program. As a result of these enhancements, FFT treatment is now available for a limited pool of possible violations posing a moderate risk to the reliability of the BPS (in addition to possible violations posing a minimal risk). In addition, certain unmitigated possible violations may be processed through the FFT program, so long as mitigation is completed within 90 days from the date the FFT item is posted.

To streamline processing of FFTs, Regional Entities now submit their FFTs for public posting on NERC's website at the end of each month. This replaces the prior requirement that NERC submit monthly informational filings to the Commission. NERC maintains its enforcement oversight by reviewing a representative sample of FFTs during the 60-day window following the public posting as well as through an annual spot check. NERC's spot checks ensure that issues selected for FFT treatment are appropriate for the program; that the issues are explained sufficiently in the posted documents; that the FFT program is implemented consistently across the regions, and that information about FFT issues is presented consistently across regions.

In addition to feedback provided through the spot check process, NERC provides ongoing training and guidance to the Regional Entities. Risk assessments play a large role in the FFT process and will be important to the success of the risk-based enforcement processes being implemented under RAI. In recognition of the importance of risk assessments, NERC provides ongoing training to the Regional Entities on how to evaluate the risk posed by an issue and how to document the results of the risk assessment in a clear and consistent manner. NERC also developed FFT templates to ensure that information regarding FFT issues, such as issue descriptions, mitigating activities, and other relevant information, is presented in a consistent manner across all Regional Entities. In addition, NERC, working with the Regional Entities, developed and posted an *ERO Self-Report User Guide*.[85] The *ERO Self-Report User Guide*

[83] As described in the evaluations of the individual Regional Entities, "above-and-beyond" activities refers to activities that a registered entity agrees to undertake as part of the resolution of an instance of noncompliance, in addition to completing a mitigation plan or other mitigating activities and/or paying a monetary penalty.

[84] *North American Electric Reliability Corporation*, *Order on Compliance Filing*, 143 FERC ¶ 61,253 (2013).

[85] Drafts of the *ERO Self-Report User Guide* and the companion *ERO Enterprise Mitigation Plan Guide* documents were posted for public comment in January 2014. The final user guides are posted on the RAI page on the NERC website at: http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

provides registered entities with helpful guidance on assessing risk and communicating relevant information to the Regional Entities.

Additional information regarding the FFT process and NERC's oversight of it is provided below.

v. Implementation of Compliance Data Systems

As noted above, the Regional Entities have implemented compliance data systems to collect and track violation data. These systems interface with NERC's centralized database. At the Regional Entity level, these systems have enabled substantial enforcement processing efficiencies. At the NERC level, these systems have enhanced NERC's ability to identify compliance and enforcement trends and compile accurate metrics.

To ensure the quality, integrity, and completeness of the data that is submitted to NERC's centralized database, NERC and the Regional Entities worked together to create a series of business rules. NERC commends the Regional Entities for the resources and effort they have expended in developing these business rules and the associated systems. However, improvements remain to be made in ensuring that data submitted to NERC's centralized database meets the parameters of the business rules. NERC will continue to work with the Regional Entities to address these areas.

vi. Quality of Submitted Information

In the three-year performance assessment, NERC noted that Regional Entities needed to improve the thoroughness and accuracy of the information provided to NERC staff for review to meet NERC expectations and the requirements of Commission orders.[86] Since the filing of the three-year performance assessment in 2009, NERC and the Regional Entities have taken concrete steps to improve the quality, clarity, and consistency of enforcement-related documentation. NERC considers these efforts to have been successful.

NERC developed a series of enforcement processing templates to assist the Regional Entities in ensuring that all required information is presented in a consistent and easily-understood format. Generally, the Regional Entities provide information in the requested format, using the templates, with the record documents that are necessary for filing.[87] The implementation of the various templates has improved the quality of submitted information since the three-year performance assessment.

However, through its regular review of submitted information, NERC has identified opportunities for further improvement. In particular, descriptions of the facts of each violation, assessments of the risk posed by each violation, and descriptions of factors contributing toward the imposition of a certain dollar penalty are not always clear or complete when violations are submitted to NERC for review in settlement agreements or NOCV. Specifically, Regional Entities

[86] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 12.

[87] NERC has advised the Regional Entities to submit all necessary documentation at the time the NOCV or settlement agreement is submitted to NERC for review and BOTCC approval, where possible.

should explain fully what factors were considered aggravating, which factors were considered mitigating, and when previous violations of the same or similar Reliability Standards were or were not considered aggravating (and why). Careful and complete drafting will facilitate greater transparency of Regional Entity decision-making, an area noted for improvement by the commenters.[88] In addition, careful and complete drafting will avoid protracted follow-up periods and processing delays.

Through NERC's outreach efforts and other process improvements and guidance being implemented under RAI, NERC expects that the quality and clarity of risk assessment, violation description information, and other information relevant to enforcement processes will continue to improve. For example, NERC and the Regional Entities have developed two documents to enhance communication between registered entities and the Regional Entities and to facilitate the shift toward a risk-based enforcement approach. The first document, the *ERO Self-Report User Guide*, provides registered entities with additional insight into the information NERC and the Regional Entities need to provide efficient and timely resolution of instances of potential noncompliance. The second document, the *ERO Enterprise Mitigation Plan Guide*, provides guidance on the information that should be considered when developing a mitigation plan and the elements and analysis that should be included. Although targeted specifically to registered entities, the user guides also provide guidance and insight to Regional Entity auditors, new enforcement staff, and other stakeholders.

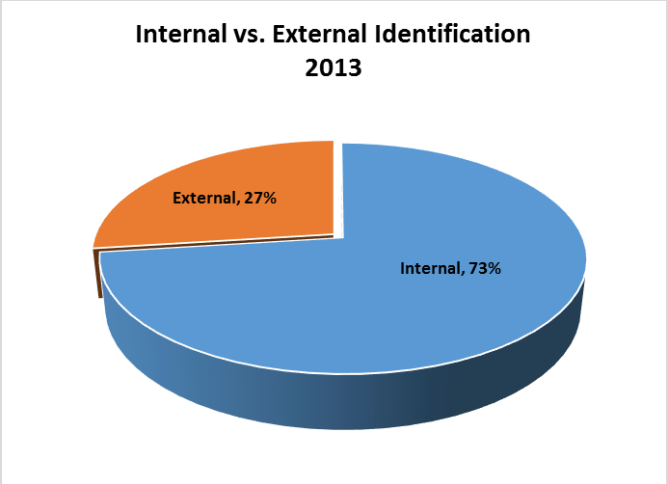
c. Improving Reliability Across the ERO Enterprise

i. Encouraging Internal Discovery of Violations

Regional Entity enforcement programs play an important role in improving the reliability of the BPS. Early self-identification, self-reporting, and mitigation of noncompliance are important steps in improving electric reliability. By deploying incentives to encourage the self-discovery and timely self-reporting of violations, the Regional Entities have encouraged registered entities to take proactive steps to self-identify their noncompliance and thereby promote a more reliable BPS.

[88] *See* the stakeholder comments summarized in the "Enforcement" sections of the comment and response tables in **Attachment 4**.

Percentage of Violations by Method of Identification, 2013



In 2013, internally-discovered (i.e., self-reported) violations comprised the majority of violations identified across the ERO Enterprise.

NERC recognizes that the percentage of self-identified violations necessarily depends on the number of violations identified by the Regional Entities through other compliance monitoring methods (i.e. spot checks and compliance audits). As NERC and the Regional Entities work together to implement efficiency and consistency-enhancing improvements under the compliance components of RAI, NERC expects to gain additional insight into audit finding and self-reporting trends across the Regional Entities. NERC expects that, as the ERO Enterprise gains experience in evaluating the internal controls and management practices of registered entities, it will develop a better understanding of what factors drive internal self-identification of violations. This insight will allow NERC and the Regional Entities to refine self-reporting incentives appropriately.

ii. Ensuring the Timely Mitigation of Violations

NERC monitors all items with ongoing mitigating activities regardless of where the violations are in the enforcement process and expects mitigating activities to be completed in a timely manner.[89] Throughout the assessment period, the Regional Entities worked to ensure that violations, including older violations that have not yet been processed, are mitigated and no longer pose a risk to reliability.

[89] As defined in the NERC ROP, Appendix 2, "mitigating activities" means actions taken by a registered entity to correct and prevent recurrence of a noncompliance, whether or not the actions are embodied in a mitigation plan.

Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation for the ERO Enterprise as of December 31, 2013[90]

Year of Discovery	% Completed	% in Progress
2013	36.0%	64.0%
2012	79.6%	20.4%
2011	92.4%	7.6%
2010	96.4%	3.6%
2009	100.0%	0.0%
2008	99.6%	0.4%
2007	100.0%	0.0%
Grand Total	**84.6%**	**15.4%**

However, as the above chart demonstrates, a small number of older violations remain for which mitigating activities have not been completed. For these violations, mitigating activities may have been started, but not yet completed. Further, some of the older violations with open mitigation relate to registered entities for which violations cannot be processed as a result of a pending court dispute.

In 2014, NERC will continue to focus on the completion of mitigating activities and track this closely. NERC will measure the success of each Regional Entity and the ERO Enterprise as a whole in ensuring that violations are mitigated and no longer pose a threat to reliability.

iii. Promoting Reliability through Enforcement Philosophy and Practices

The Regional Entities have encouraged registered entities to proffer "above-and-beyond" mitigating activities in lieu of, or as an offset to, the full monetary penalties assessed pursuant to the NERC *Sanction Guidelines*. By encouraging registered entities to invest in improvements beyond those necessary to ensure compliance with violated Reliability Standards, this enforcement approach improves reliability and reduces the likelihood of future noncompliance. Examples of such above-and-beyond activities are provided in the individual Regional Entity assessments below.

d. NERC'S Ongoing Monitoring of Specific Regional Entity Processes Under the CMEP

NERC Enforcement staff uses its oversight role to ensure that the Regional Entities are implementing the CMEP effectively, to provide constructive feedback where appropriate, to identify trends, and to drive the implementation of best practices. Over time, as enforcement

[90] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation for all Regional Entities and NERC acting as the CEA as of December 31, 2013. This table excludes dismissed violations and non-U.S. violations.

processes and organizations evolved and matured, NERC's oversight role has evolved and matured. As the Regional Entities have demonstrated the adequacy and maturity of their enforcement-related processes and procedures, NERC has adjusted its oversight activities. For example, whereas NERC formerly reviewed all FFTs before filing with the Commission, NERC now reviews only a representative sample of FFTs that have been posted to NERC's website.[91] In addition, following a 2013 spot check of Regional Entity dismissal procedures, NERC no longer requires preapproval of letters of dismissal for externally-discovered violations (except for violations arising from compliance investigations).

NERC continually looks for ways to exercise its oversight role to drive improvement in Regional Entity processes and its own oversight processes. The results of several of NERC's oversight activities are presented below and in the individual Regional Entity sections of this evaluation.

During the assessment period, NERC conducted spot checks of different aspects of the Regional Entities' implementation of the CMEP. As examples of the types of spot checks it performed, NERC reviewed Regional Entity dismissal procedures in 2013. This spot check provided valuable insight into the reasons why self-reported violations are dismissed.[92] The spot check also gave NERC the opportunity to examine Regional Entity dismissal procedures and documentation in depth. Based on its analysis of the spot check results, NERC concluded that the Regional Entities are preparing letters of dismissals that generally communicate the reasons for dismissal to the registered entities. NERC prepared several letter of dismissal templates to assist Regional Entities in ensuring that the letters of dismissal contain all required information on a consistent basis.

NERC engages in various activities to ensure consistency and exercise oversight over the FFT process. Public and nonpublic versions of the FFTs are submitted by the Regional Entities to NERC, in the NERC-provided template, for posting on a monthly basis. NERC staff reviews moderate risk issues for suitability for FFT filing. If NERC staff determines that the moderate risk issues are not appropriate for FFT filing, staff will discuss concerns with Regional Entity staff. NERC, concurrently with the Commission, reviews a representative sample of FFTs during the 60-day window following the posting of the FFT on NERC's website. NERC also includes moderate-risk FFTs and FFTs with ongoing mitigation as part of its review. Following its review

[91] As noted above, NERC's oversight of the FFT program consists of a review during the 60-day window following the monthly FFT posting as well as an annual spot check.

[92] NERC concluded that 67% of dismissals from its randomly-selected sample were attributable to an expansion of scope or a duplication of already-existing violations. In 22% of dismissals, the registered entity submitted additional information supporting compliance after the initial determination of possible violation was made. Approximately 11% of the dismissals were attributable to changes in the applicable Reliability Standard and requirement, transfer to another CEA, or administrative reasons.

NERC expects the number of dismissals to decrease as a result of the implementation of enhancements to the preliminary screen process in December 2012 (this process requires Regional Entities to review new noncompliance and determine whether it is a duplicate of a violation already being processed) and the issuance of the *ERO Self-Report User Guide*.

of the FFT samples, NERC coordinates any questions or concerns it may have with FERC staff, which conducts an independent sampling and review during the same 60-day period.

In addition to sampling during this 60-day review period, NERC also conducts a separate sampling of the FFTs to gather information related to NERC's annual filing with the Commission. In late 2012, NERC initiated a review of the Regional Entities' FFT programs, the results of which were detailed in NERC's March 15, 2013 compliance filing and report.[93]

During the first quarter of 2014, NERC Enforcement staff performed another review of the Regional Entities' FFT programs, the results of which were detailed in NERC's June 20, 2014 compliance filing and report.[94] In summary, NERC found that the quality of the FFTs submitted by the Regional Entities for posting has continued to improve from the FFTs submitted to NERC for review in prior years. NERC also found that the Regional Entities are appropriately selecting issues for FFT treatment. However, NERC identified additional areas for improvement to promote accuracy and consistency in implementation of the FFT program, as described in detail in that filing.

In addition to its periodic spot checks, NERC performs regular oversight of certain Regional Entity enforcement processes. For example, NERC reviews all SNOP violations and NOP violations before filing these violations with the Commission, and it provides feedback to the Regional Entities as appropriate. As part of this review, NERC reviews all proposed penalties for appropriateness and consistency with monetary penalties assessed for violations of the same Reliability Standard and requirement occurring under similar facts and circumstances, in accordance with the principles contained in the NERC *Sanction Guidelines.*

e. Conclusion

The Regional Entities have made substantial progress during the five-year assessment period in improving the efficiency and timeliness of enforcement processing. Going forward, each of the Regional Entities should focus on continuing to prioritize older violations for completion of processing, ensuring that all violations are mitigated in a timely manner, and ensuring the quality of data and information that is submitted to NERC in the compliance data information systems and in settlement agreements and NOCV. Further, each of the Regional Entities should implement the process improvements recommended by NERC through its oversight activities.

[93] *Compliance Filing and Report on the Compliance Enforcement Initiative and Proposed Enhancements to the Fix, Fix, Track and Report (FFT) Program*, Docket No. RC11-6-004 (Mar. 15, 2013).

[94] *North American Electric Reliability Corporation's Compliance Filing and Report on the Find, Fix, Track and Report Program*, filed June 20, 2014, in Docket No. RC11-6-004.

2. Evaluation of Florida Reliability Coordinating Council, Inc.

a. Overview

In the three-year performance assessment, NERC concluded that FRCC needed to improve its timeliness in enforcement processing in several respects.[95] In response, during the assessment period, FRCC has taken several steps to address the concerns identified by NERC. FRCC added personnel to its enforcement staff and developed a number of processes to support and facilitate the processing of violations. FRCC has also developed checklists, flowcharts, caseload goals, and automated database reporting tools.[96]

During the assessment period, FRCC has increased the number of FTE staff dedicated to enforcement from 0 FTEs in 2009 to 4 FTEs as of December 31, 2013. Based on FRCC's processing speed and efficiency as measured at the end of the assessment period, NERC views FRCC's enforcement staffing to be sufficient to process the number of violations that it receives.

.

FRCC ended the assessment period with a Caseload Index that was consistent with the ERO Enterprise Caseload Index. FRCC processed all violations discovered before 2012, in furtherance of an ERO Enterprise goal. FRCC's caseload tends to consist of more-recent violations, and FRCC has made progress in ensuring the completion of mitigation for older violations. Finally, NERC has reviewed FRCC's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, FRCC generally implements those processes in a satisfactory manner.

In addition, FRCC staff have actively participated in the development of RAI. FRCC staff have participated in the Aggregation of Minimal Risk Issues and Enforcement Discretion pilot programs and served on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

As explained more fully below, based on FRCC's Caseload Index, FRCC's successful processing of its older violations (as facilitated by its effective implementation of streamlined enforcement processing mechanisms), and the results of NERC's oversight activities, NERC concludes that FRCC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. NERC will continue to work with FRCC to ensure that violations are mitigated promptly, with an added emphasis on ensuring the completion of mitigation for older violations.

[95] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 16.

[96] 2014 JRESA Appendix 2B at 1-2.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of FRCC's Caseload

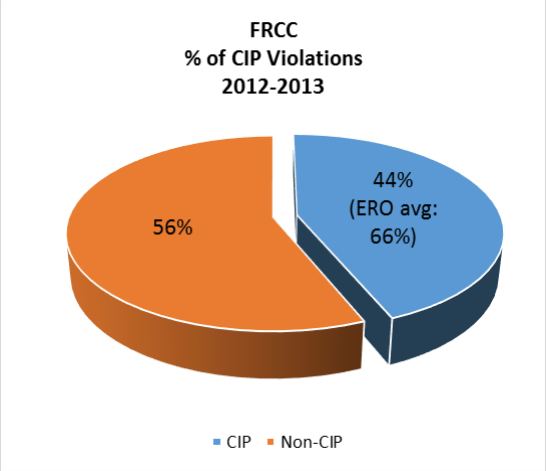
During the assessment period, FRCC reported 568 violations to NERC.

Violations for FRCC 2009-2013 by Year Reported to NERC[97]

Year Reported to NERC	Violations Reported
2009	188
2010	109
2011	141
2012	69
2013	61
Total	**568**

As shown in the table above, FRCC reported a relatively high number of violations in 2009, with a significant drop occurring after 2011. In 2011, over 70% of total violations were of the CIP Reliability Standards. In the years 2012 and 2013, violations of CIP Reliability Standards represented 44% of total violations; this is a substantially lower percentage than the ERO Enterprise average.

Type of Violations Reported to NERC by FRCC, 2012-2013



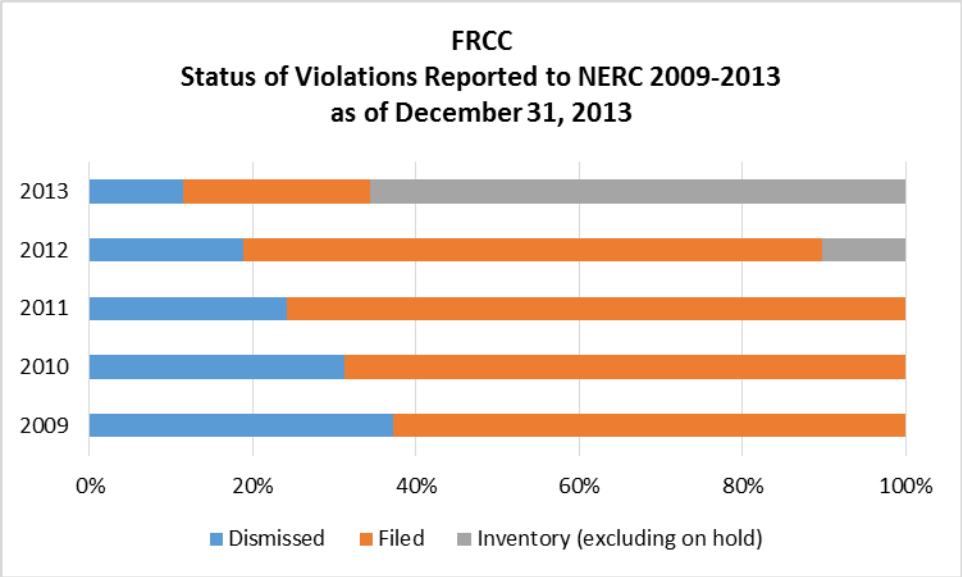
FRCC believes that the lower-than-average ratio of CIP violations in 2012 and 2013 may be due to two factors. During 2011, FRCC performed spot checks on all registered entities within the FRCC region that had critical cyber assets. As a result, FRCC had a high ratio of CIP violations

[97] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 766.

for that year (approximately 75%). In addition, FRCC believes that it has a lower percentage of registered entities with critical cyber assets than other Regional Entities.

Of the total violations reported to NERC by FRCC during the assessment period, 47 violations, or approximately 8%, remained to be processed as of December 31, 2013 (excluding on-hold violations). As shown in the table below, FRCC has processed all violations reported to NERC in 2009, 2010, and 2011. FRCC processed 90% of violations reported to NERC in 2012.

Status of Violations Reported to NERC 2009-2013 for FRCC



FRCC processed 34% of violations reported to NERC in 2013. This was somewhat lower than the ERO 2013 processing rate of 39%. However, violations reported to NERC in 2013 represent approximately 85% of the violations available for processing in FRCC's caseload, which compares favorably to the overall ERO Enterprise average of 67%. FRCC appears to be moving toward a caseload consisting primarily of newer violations.

ii. Caseload Index

The Caseload Index for FRCC is 7.3 months as of December 31, 2013. This is consistent with the ERO Enterprise Caseload Index of approximately 6.5 months.

Based on its achievements in processing its caseload to date and its Caseload Index, it appears that FRCC's efforts to strengthen and streamline its enforcement processes during the assessment period have been effective.

iii. Efforts to Reduce Older Caseload

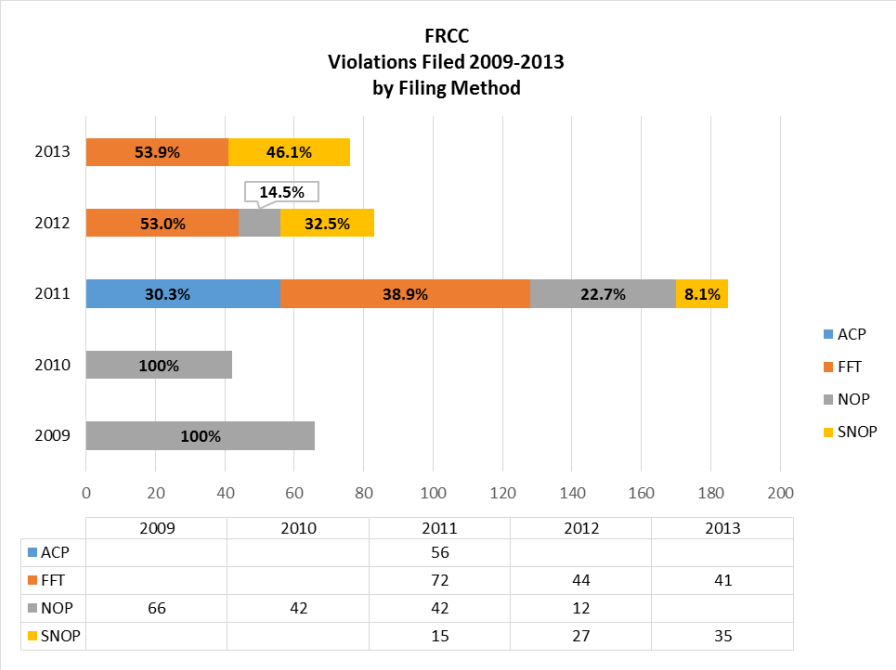
In 2013, FRCC processed all remaining cases in its pre-2012 caseload. NERC commends FRCC for its responsiveness and efforts to achieve this important ERO Enterprise goal.

Based on the current composition of its inventory of violations available to be processed and its successful efforts in processing its older violations, FRCC is especially well-positioned to achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

FRCC effectively used streamlined processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2011, following the implementation of these mechanisms, FRCC filed 185 violations – more than the previous two years combined.

Violations Filed per Year by Filing Method for FRCC, 2009-2013



	2009	2010	2011	2012	2013
ACP			56		
FFT			72	44	41
NOP	66	42	42	12	
SNOP			15	27	35

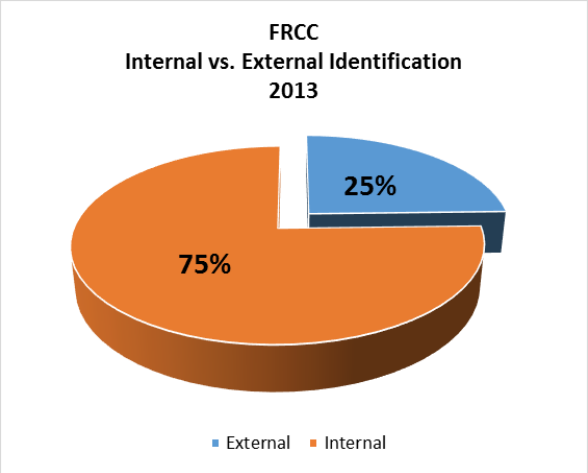
By 2013, FRCC filed all of its violations using either SNOP or FFT. NERC expects that FRCC will continue to reserve the NOP format for violations that require NOP treatment and will take advantage of further process refinements available under RAI. Additional information regarding FRCC's application of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised 75% of total violations in the FRCC region.

Percentage of Violations by Method of Identification for FRCC in 2013



This is consistent with the ERO Enterprise average of 73%.

ii. Ensuring the Timely Mitigation of Violations

FRCC reported that it takes several steps to encourage the prompt submission of mitigation plans or mitigating activities. First, FRCC encourages registered entities to submit the mitigating activities that are planned or which have been completed as part of the registered entity's submission of a self-report or self-certification. FRCC also encourages registered entities to submit mitigation plans early, before the issuance of a Notice of Alleged Violation. Second, FRCC enforcement staff contacts each registered entity to encourage the submission of a mitigation plan approximately ten days after the issuance of a Notice of Possible Violation. FRCC also encourages registered entities to submit draft mitigation plans for review by FRCC staff before formal submission. In evaluating the sufficiency of a registered entity's proposed mitigation, FRCC carefully considers the time it will take to mitigate the violation and the steps taken to prevent reoccurrence of violations. In 2013, FRCC reported that it continued to see some improvement in the timeliness and quality of mitigating activities and mitigation plans submitted by most registered entities, and that most registered entities within its region were willing to work with FRCC staff to create mitigation plans that would be acceptable to FRCC earlier in the mitigation process.

As demonstrated in the table below, FRCC has made substantial progress in ensuring that violations from 2007 through 2010 have been mitigated. However, approximately four violations from 2011 had open mitigation plans at the end of the assessment period. FRCC reported that in those cases, the registered entities had mitigated the violations and completed all milestones required of their mitigation plans; however, they had not yet certified the completion of their mitigation plans and supplied evidence for FRCC to verify completion.

FRCC: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[98]

Year of Discovery	% of Violations with Completed Mitigation Plans or Activities	% of Violations with Mitigation in Progress
2013	25.0%	75.0%
2012	89.3%	10.7%
2011	96.0%	4.0%
2010	100.0%	0.0%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**89.6%**	**10.4%**

In addition, approximately three-quarters of violations discovered in 2013 had open mitigation plans by the end of the year. FRCC reported that in many of these newer cases, the violation had been mitigated, but the registered entity did not yet certify completion or submit completion evidence to FRCC for verification. NERC will continue to work with FRCC to ensure that mitigation of violations is completed in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

FRCC's enforcement philosophy consists of the following components. FRCC provides training and communication to registered entities to help them understand and be more compliant with the Reliability Standards. FRCC strives for efficiency in disposition processing and fairness throughout the enforcement process, and it commits to maintain open communication with registered entities.

In its settlement processes, FRCC has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. FRCC reported that it typically performs a thorough review and critique of a registered entity's internal compliance program as part of settlement discussions, and that registered entities within its region have frequently committed to initiating actions within their organizations to improve their compliance programs. Registered entities in the FRCC region have committed to: (i) implementing software applications; (ii) creating, improving, or disseminating programs relating to internal controls; (iii) creating compliance job positions; (iv) developing and delivering presentations for FRCC compliance workshops; and (v) hiring contractors to evaluate and make recommendations for the development of a sustainability plan

[98] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations.

and training regarding internal control processes. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance. NERC encourages FRCC to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. FRCC'S Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to FRCC.

FRCC has adopted the NERC CMEP as the basis for providing fair and impartial procedures for enforcement. With respect to assessing penalties, FRCC follows NERC guidance.[99] FRCC reviews a registered entity's internal compliance program and its impact on the violations being processed. FRCC includes consideration of the internal controls that a registered entity may have in place as a part of this review. NERC reviews all penalties submitted by FRCC for appropriateness and consistency with monetary penalties assessed by FRCC and by other Regional Entities for violations of the same Reliability Standards and Requirements occurring under similar facts and circumstances. NERC has found that FRCC assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check in 2013, NERC determined that FRCC dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC identified opportunities where FRCC could improve its letters of dismissal and communicated those opportunities to FRCC. By implementing the recommended improvements, FRCC can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of FFT issues filed or posted by FRCC during the assessment period to examine FRCC's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that FRCC's process documents provide clear and concise guidance for FFT processing and drafting and follow the NERC guidance. Further, NERC concluded that FRCC consistently applies the processes set forth in its process documents, and that FRCC applied FFT treatment and evaluated risk in a consistent manner. NERC noted several ways that FRCC could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that FRCC has performed as an effective Regional Entity with respect to enforcement activities during the

[99] 2014 JRESA, Appendix 2-C at 11.

assessment period. FRCC should adopt the recommendations for improvement provided as part of NERC's oversight activities.

3. Evaluation of Midwest Reliability Organization

a. Overview

In the three-year performance assessment, NERC concluded that MRO was an effective Regional Entity as demonstrated by several metrics.[100] At the time NERC noted that MRO needed to improve on providing accurate statements of fact for each violation, assessing penalties according to the facts of each situation as required by FERC orders, and ensuring consistency in its practices with NERC practice and the practice of other Regional Entities.[101]

Consistent with the trends across the ERO Enterprise, the quality of information submitted by MRO for NERC review has improved during the assessment period. Further, MRO believes that its three-step process that segregates duties among its Compliance Monitoring, Risk Assessment and Mitigation, and Enforcement teams, which it established in 2009, provides a "high level of assurance that determinations are accurate, fair and non-discriminatory."[102]

During the assessment period, MRO has increased the number of FTE staff dedicated to enforcement from 2.46 FTEs in 2009 to 4 FTEs as of December 31, 2013. In addition, MRO's Risk Assessment and Mitigation staff consisted of 1 FTE in 2009, and as of December 31, 2013 it consists of 6.25 FTEs (including two open positions). MRO's proposed 2015 Business Plan and Budget anticipates an additional 1.35 FTEs in these two groups. Based on MRO's processing speed and efficiency as measured at the end of the assessment period, NERC views MRO's historic staffing to be insufficient to process the number of violations that it receives in accordance with the performance objectives of the ERO Enterprise. However, MRO has taken steps to increase its staffing throughout the assessment period and beyond into 2014 and 2015.

NERC recognizes the progress MRO has made in enforcement processing during the assessment period. NERC also recognizes that MRO often takes the lead in settlement negotiations to resolve violations from MRREs, and that MRO has demonstrated a commitment to use the enforcement process to promote the reliability of the BPS. Further, NERC has reviewed MRO's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, MRO generally implements those processes in a satisfactory manner. However, MRO ended the assessment period with a Caseload Index that was much higher than the ERO Enterprise Caseload Index. NERC and MRO believe that, with the additional staff MRO expects to add, MRO's processing times (and its Caseload Index) will improve.

In addition, MRO made substantial strides in reducing the portion of its caseload consisting of violations dating to before 2012. While MRO still has older violations in its inventory that must

[100] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 18.

[101] *Id*.

[102] 2014 JRESA, Appendix 2-B at 2-3.

be processed and mitigated, NERC is working with MRO to accomplish the ERO Enterprise goal of having no cases older than 24 months in inventory at the end of 2014.

NERC recognizes the substantial contributions MRO staff have made in the development of RAI and the related enforcement pilot programs. MRO has taken a leadership role in the conceptualization, development, and testing of several programs, and a member of MRO's staff led the multi-region working group on enforcement activities. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

In light of all of the relevant factors, which are explained more fully below, NERC concludes that MRO has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. However, substantial improvement remains to be made with respect to MRO's enforcement processing time as measured by the Caseload Index metric.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of MRO's Caseload

During the assessment period, MRO reported 664 violations to NERC.[103]

Violations for MRO 2009-2013 by Year Reported to NERC[104]

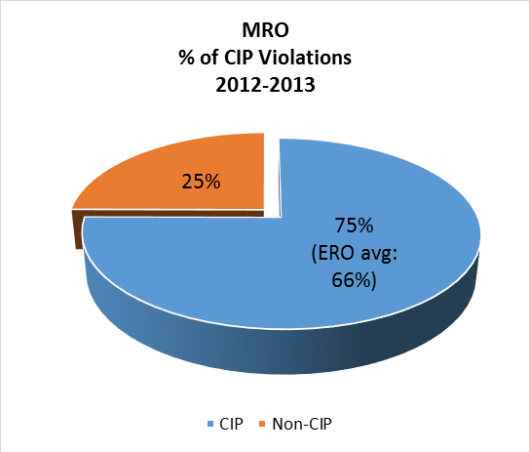
Year Reported to NERC	Violations Reported
2009	60
2010	103
2011	196
2012	166
2013	139
Total	**664**

As noted in the table above, the highest number of violations reported to NERC by MRO was in 2011, with the number decreasing by 29% in 2013. Most of the violations in 2011 were of the CIP Reliability Standards. In the years 2012 and 2013, violations of CIP Reliability Standards represented 75% of total violations; this is a higher percentage than the ERO Enterprise average of 66%.

[103] This table reflects U.S. violations only. When including Canadian violations, MRO received 693 violations for evaluation and processing from 2009 through 2013.

[104] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 766.

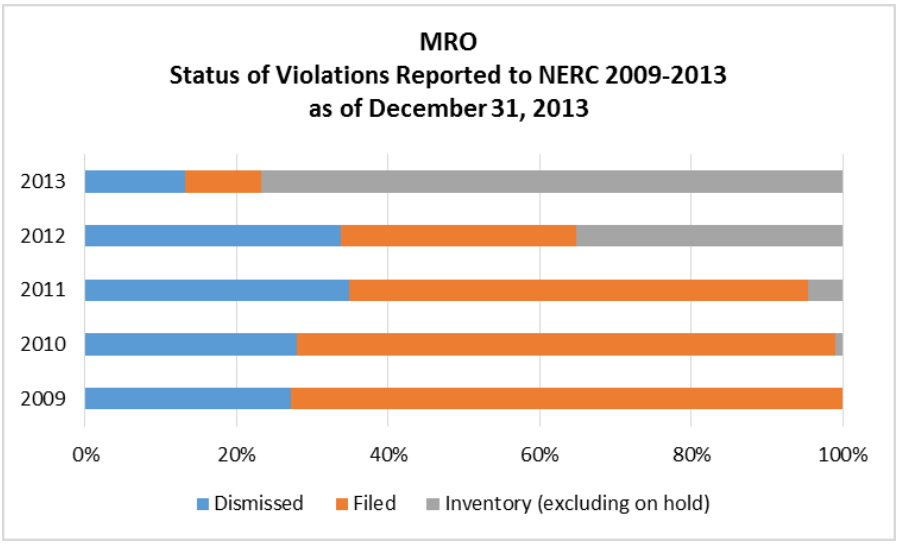
Type of Violations Reported to NERC by MRO, 2012-2013



The discovery method of the CIP violations was fairly evenly split between external and internal methods of identification.

Of the total violations reported to NERC during the assessment period, approximately 159 violations, or 24%, remained to be processed as of December 31, 2013. As demonstrated in the table below, MRO has processed all violations that it reported to NERC in 2009. MRO has processed approximately 99% of violations reported to NERC in 2010, 95% of violations reported to NERC in 2011, and 65% of violations reported to NERC in 2012.

Status of Violations Reported to NERC 2009-2013 for MRO



MRO processed approximately 23% of violations reported to NERC in 2013. This is lower than the ERO 2013 processing rate of 39%. Further, the percentage of MRO's caseload consisting of violations reported to NERC in 2013, approximately 62.3%, is slightly lower than the overall ERO Enterprise average of 67%.

ii. Caseload Index

The Caseload Index for MRO was 14.3 months as of December 31, 2013, compared to the ERO Enterprise Caseload Index of approximately 6.5 months.

MRO believes that its Caseload Index is higher than the ERO Enterprise average due to several factors. MRO states that it places a premium on gaining a comprehensive understanding of the violation and developing mitigation plans that reduce the risk of recurrence, which can be time consuming and increases MRO's Caseload Index. MRO reported a number of violations of CIP-005 and CIP-007, which often require longer processing times due to the need to ensure that the risk is understood and is being comprehensively addressed. Additionally, MRO's risk assessment staff is heavily involved in RAI development efforts.

In light of MRO's Caseload Index and as reflected in the characteristics of its caseload (i.e., MRO's caseload consists of a greater portion of older violations than other Regional Entities), NERC encourages MRO to implement measures so that it is better equipped to process violations as it receives them. MRO currently has two open positions in its Risk Assessment and Mitigation group which, when filled, will help MRO improve its Caseload Index. In addition, MRO created the position of CMEP process principal. This position is responsible for quality assurance and oversight of MRO's business practices related to compliance monitoring and enforcement, including internal transitions among the compliance, risk assessment and mitigation, and enforcement groups. MRO believes it will achieve greater efficiency, enhance communication, and ensure repeatability of its CMEP-related activities through this position. MRO also believes that the increase in staffing will allow it to improve processing times while maintaining its dedication to gaining a complete understanding of violations in its region and examining the best ways to prevent reoccurrence. NERC will work with MRO to evaluate the effectiveness of this and other measures taken to improve efficiency in MRO's enforcement processes.

iii. Efforts to Reduce Older Caseload

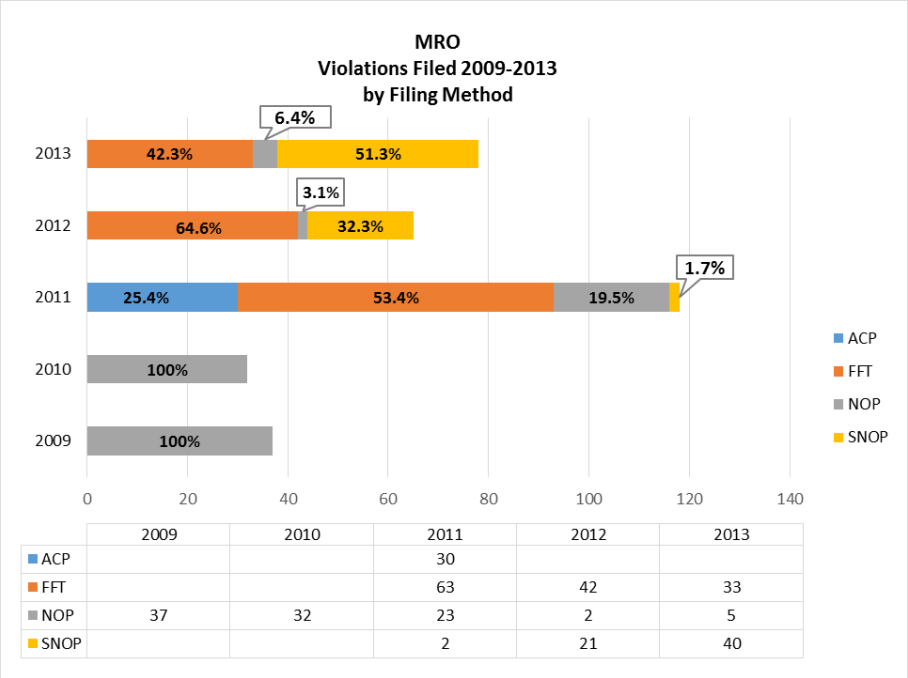
In 2013, MRO reduced the portion of its caseload consisting of violations dating to before 2012 by 89%. NERC commends MRO for its responsiveness and efforts to achieve this important ERO Enterprise goal. MRO states that its remaining inventory consisted of particularly complex violations, and that it is committed to having all 2012 and older cases resolved by the end of 2014.

NERC will work with MRO to ensure that these and other older violations are resolved as soon as is practicable in light of the facts of each violation.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

MRO effectively used streamlined enforcement processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2011, following the implementation of the streamlined enforcement processing mechanisms, MRO filed 118 violations – more than the previous two years combined.

Violations Filed per Year by Filing Method for MRO, 2009-2013



	2009	2010	2011	2012	2013
ACP			30		
FFT			63	42	33
NOP	37	32	23	2	5
SNOP			2	21	40

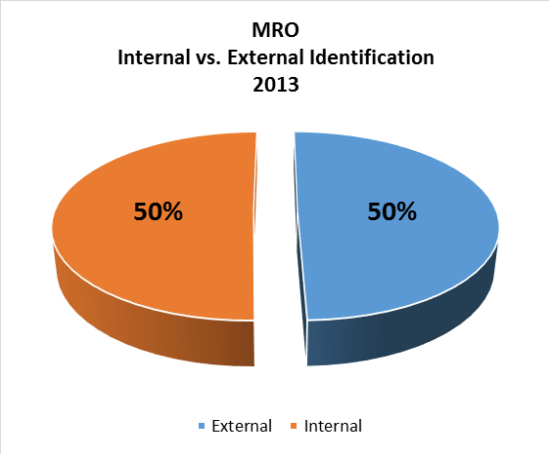
MRO has used the streamlined processing mechanisms to file over 88% of violations since 2011. MRO is using the FFT process to resolve violations posing a minimal risk to the BPS, and it seeks to use the enforcement mechanisms in a manner that promotes consistency. NERC expects that MRO will continue to reserve the NOP format for violations that require it and take advantage of further process refinements available under RAI. Additional information regarding MRO's implementation of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised approximately 50% of total violations in the MRO region. This is lower than the ERO Enterprise average of 73%. Stated differently, during the assessment period, MRO discovered a higher percentage of violations through external methods (i.e., compliance audit and spot check) than other Regional Entities.

Percentage of Violations by Method of Identification for MRO in 2013



As noted above, NERC and the Regional Entities are working to understand the regional variations in the percentages of noncompliances discovered through self-discovery and audits across the ERO Enterprise. Understanding these differences, and how they may relate to registered entity internal controls and management practices, will allow NERC and the Regional Entities to continue to provide the right incentives for discovering and self-reporting noncompliances.

ii. Ensuring the Timely Mitigation of Violations

MRO reported that, upon validation of a violation, MRO mitigation staff conduct a thorough review of the present circumstances at the registered entity to ensure better, more effective corrective actions for prevention. MRO mitigation staff collaborate with the registered entities to develop a thorough, comprehensive, and effective mitigation plan that includes documentation and implementation of controls that are used to monitor performance and correct deficiencies to help prevent recurrence of noncompliance. MRO's position is that while it recognizes that prompt submission or early completion of mitigation plans may be desirable, its overarching goal of preventing recurring issues is of greater concern. MRO uses the webCDMS platform to automate processes for the review, approval, tracking, and certification of mitigation plans, and it participates in efforts across the ERO Enterprise to develop metrics to encourage timely processing of mitigation plans.

As demonstrated in the table below, MRO has made substantial progress in ensuring that older violations have completed mitigation, with 100% of violations discovered from 2007 through 2010 having completed mitigation.

MRO: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[105]

Year of Discovery	% Completed	% in Progress
2013	14.7%	85.3%
2012	58.5%	41.5%
2011	79.5%	20.5%
2010	100.0%	0.0%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**70.4%**	**29.6%**

NERC is working closely with MRO to understand the nature of the violations with open mitigation and ensure that violations are mitigated in a timely manner. Specifically, NERC will work with MRO to understand why just over half of 2012 violations have completed mitigation and less than 15% of 2013 violations have completed mitigation.[106] NERC encourages MRO to continue to seek solutions that will promote reliability and work to ensure that mitigation is completed in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

MRO's enforcement philosophy is to ensure that enforcement determinations match its essential purpose: to improve reliability and address risks to reliability. MRO reserves settlements for more complicated matters and encourages investments in systems and people as an offset for proposed penalties. An important tenet of MRO's enforcement philosophy is to use technical experts with the requisite knowledge and experience to assess actual risk posed by individual violations. MRO's enforcement philosophy considers highly effective reliability organizations to be those that prevent uncontrolled cascading outages through disciplined management practices and are accountable for their performance. As a result, registered entities in the MRO region accept responsibility (or "admit") in 90% of all violations.[107]

Similar to the other Regional Entities, MRO worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards, in lieu of the full monetary penalties

[105] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations and non-U.S. violations.

[106] Although a number of violations from 2011 have open mitigation, most of these violations involve the same registered entity.

[107] JRESA, Appendix 2-C at 13. MRO's Regulatory Philosophy (April 30, 2014) is available at: http://www.midwestreliability.org/01_about_mro/Public%20Awareness/2014/MRO_Regulatory_Philosophy_043014.pdf.

permitted by the NERC *Sanction Guidelines*. MRO states that, during the assessment period, it sought to include above-and-beyond commitments whenever possible. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

As an example of the type of above-and-beyond commitments made by registered entities in the MRO region, one registered entity committed to the hiring of additional compliance personnel, installation of new alarming systems, replacement of electromechanical relays and communication equipment with microprocessor relays and mirrored bit over fiber communications, and the provision of additional training for entity staff. Another registered entity committed to the following activities: (i) sharing its experience and lessons learned related to compliance with PRC-005-1 with at least three industry peer groups such as the North American Generator Forum and the Mid Continent Compliance Forum; (ii) securing NERC Compliance training from an outside consultant for at least six individuals from its Nuclear Business Unit; (iii) coordinating with and benchmarking the adoption of NERC compliance efforts at two nuclear facilities owned and operated by two different entities (one within the MRO region and one outside the MRO region); and (iv) replacing certain solid state relays with microprocessor relays. In another instance, the registered entity accelerated its replacement schedule for aging assets to include replacement of four additional electro-mechanical relay panels with completely digital, self-diagnostic relays, among other above-and-beyond actions over a three year period. NERC encourages MRO to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. MRO'S Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to MRO.

With respect to the appropriateness of monetary penalties, MRO undertook several efforts during the assessment period to ensure consistency of remedies within its region. MRO also participated in various initiatives to increase interaction with other Regional Entities, such as through the various Regional Entity working groups. MRO does not review or track all monetary penalties proposed by other Regional Entities. However, MRO reviews penalty determinations for similar violations in the MRO region and other Regional Entities and, as appropriate, discusses proposed penalties with other Regional Entities and NERC. NERC reviews all penalties submitted by MRO for appropriateness and consistency with monetary penalties assessed by MRO and by other Regional Entities for violations of the same Reliability Standards and Requirements occurring under similar facts and circumstances. NERC has found that MRO assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that MRO dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC

identified opportunities where MRO could improve its letters of dismissal, and communicated those opportunities to MRO. By implementing the recommended improvements, MRO can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of MRO FFT issues filed or posted during the assessment period to examine MRO's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. NERC concluded that MRO's process documents for FFT processing are clear, easy-to-follow, and facilitate consistent application. Further, NERC noted that MRO uses a checklist to ensure that it follows its process by tracking all of the steps that must be taken. NERC concluded that MRO generally assessed the risk posed by an issue in light of all relevant facts and ensured that mitigating activities addressed both mitigation of the issue and prevention of reoccurrence. NERC noted several ways that MRO could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that MRO has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. In addition, NERC commends MRO for its substantial efforts in the development of RAI. MRO should adopt the recommendations for improvement noted above. In particular, based on MRO's performance in several enforcement processing metrics, MRO should work to identify and implement solutions so that it is better equipped to ensure that violations are processed as quickly as is practicable consistent with the circumstances of each violation. MRO should also adopt the other recommendations for improvement provided as part of NERC's oversight activities.

4. Evaluation of Northeast Power Coordinating Council, Inc.

a. Overview

In the three-year performance assessment, NERC concluded that NPCC was a relatively effective Regional Entity in that it processed and completed identified violations in a timely manner. However, NERC indicated its concern that NPCC may not be identifying all violations that are occurring.[108]

NPCC believes that, during the assessment period, it has built a very cost-effective compliance program through the use of independent contractors. NPCC's level of alleged violations per registered reliability function remains low, but in line with other Regional Entities. NPCC believes its low level of violations per registered reliability function is a product of its thorough outreach and communication with registered entities in its region.[109]

[108] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 19-20.

[109] 2014 JRESA, Appendix 2-B at 3.

During the assessment period, NPCC has increased the number of FTE staff dedicated to enforcement from 2 in 2009 to 4 as of December 31, 2013. Based on NPCC's processing speed and efficiency as measured at the end of the assessment period, NERC views NPCC's enforcement staffing to be sufficient to process the number of violations that it receives.

NPCC ended the assessment period with a Caseload Index that was somewhat better than the ERO Enterprise Caseload Index. NPCC processed all violations that were discovered before 2012, in furtherance of an ERO Enterprise goal. NPCC's caseload now consists of more-recent violations, and NPCC has made progress in ensuring that older violations are mitigated. Finally, NERC has reviewed NPCC's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, NPCC generally implements those processes in a satisfactory manner.

In addition, NPCC staff have actively participated in the development of RAI. Specifically, NPCC staff have participated in the Aggregation of Minimal Risk Issues and Enforcement Discretion pilot programs and served on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. NPCC also participated in several compliance-based programs. In addition, NPCC staff have participated in the process to develop improvements for the compliance and enforcement oversight of MRREs. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

As explained more fully below, based on NPCC's Caseload Index, NPCC's successful processing of its older violations (as facilitated by its effective implementation of streamlined enforcement processing mechanisms), and the results of NERC's oversight activities, NERC concludes that NPCC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. Going forward, NERC will work with NPCC to ensure that violations are mitigated promptly.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of NPCC's Caseload

During the assessment period, NPCC reported 551 violations to NERC.[110]

Violations for NPCC 2009-2013 by Year Reported to NERC[111]

Year Reported to NERC	Violations Reported
2009	43
2010	99
2011	130

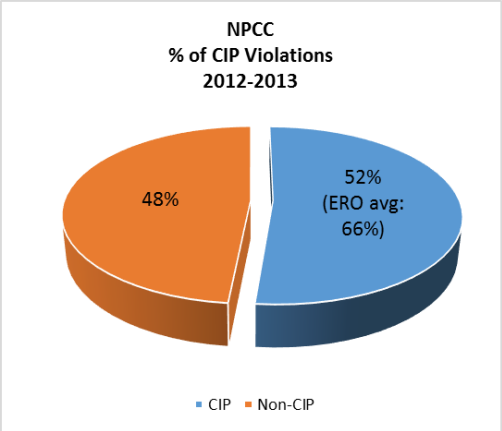
[110] This table reflects U.S. violations only. When including Canadian violations, NPCC reported 670 violations from 2009 through 2013.

[111] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 766.

2012	213
2013	66
Total	**551**

As noted in the table above, NPCC reported the highest number of violations in 2012, with a substantial decline in 2013. In the years 2012 and 2013, violations of CIP Reliability Standards represented 52% of total violations; this is a lower percentage than the ERO Enterprise average of 66%.

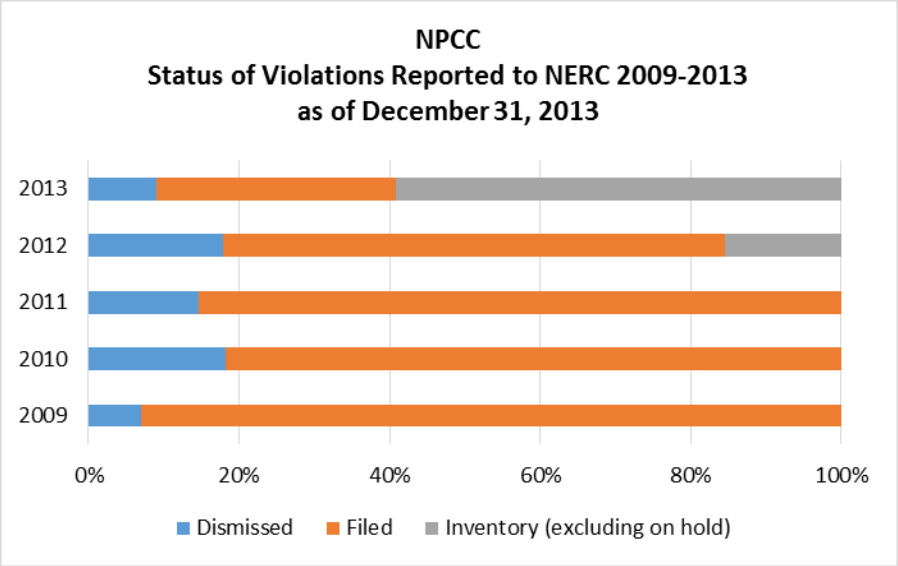
Type of Violations Reported to NERC by NPCC, 2012-2013



Over the assessment period, CIP violations made up 54.6% of total violations in NPCC, compared to the ERO Enterprise average of 59.4%. Approximately 70% of the CIP violations were self-identified. NERC will work with NPCC to understand what factors may have caused NPCC to have a lower percentage of CIP violations than other Regional Entities in 2012-2013.

Of the total violations reported to NERC during the assessment period, approximately 72 violations, or 13%, remained to be processed as of December 31, 2013 (excluding violations that are held by appeal, a court, or a regulator). As demonstrated in the table below, NPCC has processed all violations that were reported to NERC in 2009, 2010, and 2011. NPCC has processed approximately 85% of violations reported to NERC in 2012.

Status of Violations Reported to NERC 2009-2013 for NPCC



NPCC processed approximately 41% of violations that it reported to NERC in 2013. This is consistent with the ERO 2013 processing rate of 39%. Approximately 54% of the violations available for processing in NPCC's inventory consist of violations reported to NERC in 2013. This is lower than the overall ERO Enterprise average of 67%.

ii. Caseload Index

The Caseload Index for NPCC is 6.7 months as of December 31, 2013. This is consistent with the ERO Enterprise Caseload Index of approximately 6.5 months.

In light of NPCC's Caseload Index and as reflected in the general characteristics of its caseload (i.e., NPCC's caseload consists entirely of violations reported to NERC in 2012 and 2013), NPCC continued to process violations in a timely manner during the assessment period.

iii. Efforts to Reduce Older Caseload

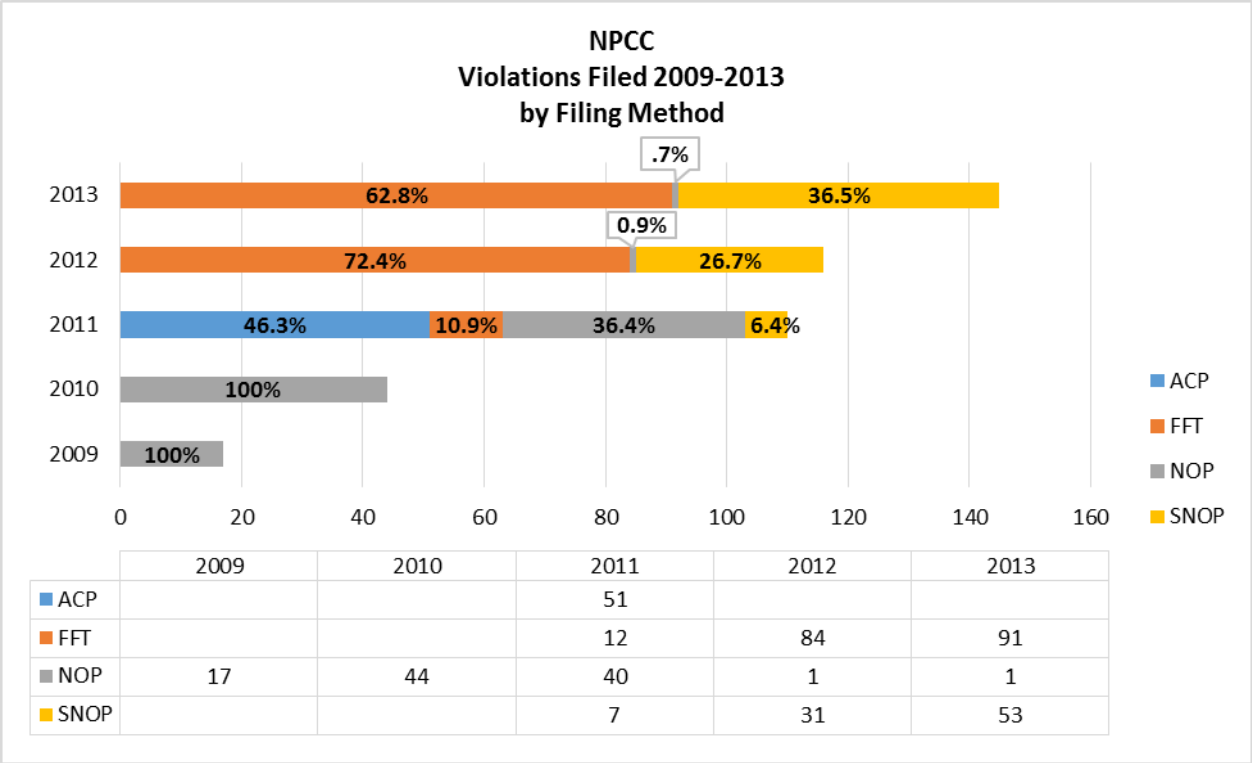
In 2013, NPCC completed processing of all pre-2012 violations. NERC commends NPCC for its responsiveness and efforts to achieve this important ERO Enterprise goal. Based on the current composition of its inventory of violations available to be processed, NPCC is well-positioned to achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

NPCC effectively used streamlined processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2011, following the implementation of the

streamlined enforcement processing mechanisms, NPCC filed 110 violations – more than the previous two years combined.

Violations Filed per Year by Filing Method for NPCC, 2009-2013



	2009	2010	2011	2012	2013
ACP			51		
FFT			12	84	91
NOP	17	44	40	1	1
SNOP			7	31	53

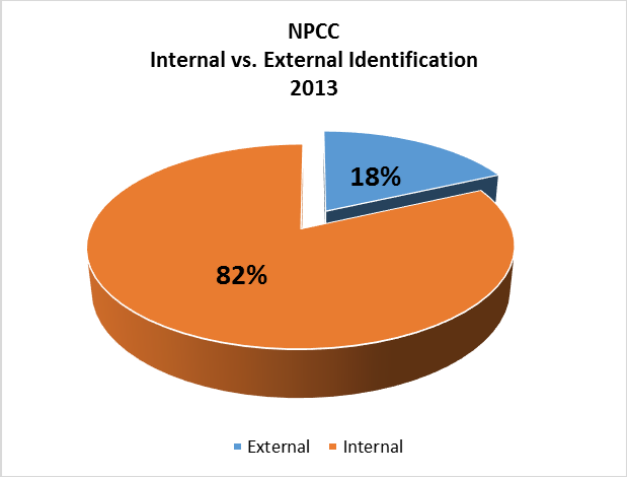
By 2012, NPCC filed nearly all of its violations using either SNOP or FFT. NPCC reported that it discusses the application of FFT and SNOP with other Regional Entity representatives to ensure consistency. NERC expects that NPCC will continue to reserve the NOP format for violations that require it and to take advantage of further process refinements available under RAI. Additional information regarding NPCC's application of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised 82% of total violations in the NPCC region. This is somewhat higher than the ERO Enterprise average of 73%.

Percentage of Violations by Method of Identification for NPCC in 2013



ii. Ensuring the Timely Mitigation of Violations

NPCC has enhanced its self-report form to include data fields that allow registered entities to supply details of mitigation plans or mitigating activities when submitting a self-report. NPCC believes that use of these new data fields has resulted in earlier implementation of mitigation, thereby promoting improved reliability. NPCC works closely with each registered entity to process mitigation plans in a timely manner.

As demonstrated in the table below, NPCC has made substantial progress in ensuring that pre-2012 violations have been mitigated.

NPCC: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[112]

Year of Discovery	% Completed	% in Progress
2013	37.5%	62.5%
2012	86.3%	13.7%
2011	100.0%	0.0%
2010	100.0%	0.0%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**89.0%**	**11.0%**

[112] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations and non-U.S. violations.

Approximately 22 violations from 2012 remain to be mitigated, along with 62.5% of violations from 2013. NERC is working closely with NPCC to ensure that violations are mitigated in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

NPCC's enforcement philosophy is to develop relationships with the registered entities in its region to: (1) educate them on the aspects of the CMEP and its implementation; (2) inform them of the changes to the enforcement process during biannual workshops; and (3) promote RAI.

In its settlement processes, NPCC has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

As an example of above-and-beyond activities, one registered entity within the NPCC region committed to establish an enterprise-wide compliance program, with resources dedicated to implementing that program. Another registered entity committed to implement software systems (rather than manual record-keeping) to track protection system devices and their associated maintenance intervals. On one occasion, a registered entity committed to implement Light Detection and Ranging (LiDAR)-based Power Line Systems as a supplemental tool to identify site conditions. NERC encourages NPCC to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. NPCC'S Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to NPCC.

NPCC reported that, in addition to using the NERC *Sanction Guidelines* as a guide for assessing monetary penalties, NPCC reviews the monthly enforcement filings. Specifically, NPCC compares the penalties that other Regional Entities assess for violations of Reliability Standards and Requirements and contacts other Regional Entities to discuss penalties where appropriate. NERC reviews all penalties submitted by NPCC for appropriateness and consistency with monetary penalties assessed by NPCC and other Regional Entities for violations of the same Reliability Standards and Requirements occurring under similar facts and circumstances. NERC has found that NPCC assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that NPCC generally dismisses violations for appropriate reasons, and generally includes the required information when issuing letters of dismissal. NERC identified opportunities for NPCC to improve its letters of dismissal and communicated those opportunities to NPCC. By implementing the recommended improvements, NPCC can improve the quality and clarity of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of NPCC FFT issues filed or posted during the assessment period to examine NPCC's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that NPCC maintains process documents governing the application of the FFT process. NERC noted that NPCC ensures that mitigating activity is completed. NPCC's issue descriptions are generally adequate to describe the issue. NERC noted several ways that NPCC could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that NPCC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. NPCC should adopt the recommendations for improvement provided as part of NERC's oversight activities.

5. Evaluation of ReliabilityFirst Corporation

a. Overview

In the three-year performance assessment, NERC concluded that, consistent with the overall findings for the ERO Enterprise, ReliabilityFirst needed to improve its efficiency with respect to conducting enforcement activities.[113] ReliabilityFirst has taken several steps to increase its efficiency with respect to conducting enforcement activities during the assessment period, including setting internal violation processing goals that are tied to corporate goals and training enforcement staff on how to become more efficient in their fact-gathering efforts. In 2013, ReliabilityFirst implemented a practice of consolidating multiple violations of the same standard with similar facts into a single docket number and consolidating multiple docket numbers with similar violations into a single settlement agreement or FFT. ReliabilityFirst believes this practice furthers its approach to resolving violations, an approach which it described as "holistic." ReliabilityFirst has also focused its efforts on those violations that pose the greatest risk to reliability and expedited its processing of lesser-risk violations through the FFT process.[114]

During the assessment period, ReliabilityFirst increased the number of FTE staff dedicated to enforcement from 8 in 2009 to 12 as of December 31, 2013.

---

[113] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 21-22. NERC also noted that an independent audit of ReliabilityFirst's compliance program found no material deficiencies.

[114] 2014 JRESA, Appendix 2-B at 6.

NERC recognizes the progress ReliabilityFirst has made in enforcement processing during the assessment period. ReliabilityFirst made significant progress in reducing the number of open violations, despite substantial increases in new violations during the assessment period. Moreover, during the assessment period, ReliabilityFirst worked with and resolved a number of complex matters concerning registered entities with significant BPS operations. When resolving each of these complex matters, ReliabilityFirst encouraged registered entities to implement actions above and beyond baseline compliance to improve the reliability and security of the BPS. Examples of these above-and-beyond actions are presented below.

NERC also recognizes that ReliabilityFirst often takes the lead in settlement negotiations to resolve violations from MRREs. ReliabilityFirst has routinely demonstrated a commitment to use the enforcement process to promote the reliability of the BPS. Further, NERC has reviewed ReliabilityFirst's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, ReliabilityFirst generally implements those processes in a satisfactory manner. However, ReliabilityFirst ended the assessment period with a higher-than-average Caseload Index. In addition, while ReliabilityFirst made substantial strides in reducing the portion of its caseload consisting of violations dating to before 2012, ReliabilityFirst had a number of older violations in its inventory that needed to be mitigated and processed by the end of the assessment period. As is discussed in more detail below, ReliabilityFirst is working closely with the registered entities to complete mitigation and processing of these older violations.

NERC recognizes the contributions ReliabilityFirst staff have made in the development of RAI and the related enforcement pilot programs. ReliabilityFirst has taken a leadership role in the conceptualization, development, testing, and integration of several programs, and a member of ReliabilityFirst's staff led the multi-region working group on enforcement activities during the assessment period. ReliabilityFirst staff participated in the Enforcement Discretion pilot program and served on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. ReliabilityFirst staff have also participated in the process to develop improvements for the compliance and enforcement oversight of MRREs. ReliabilityFirst also maintained the sole MRRE log during the Aggregation of Minimal Risk Issues pilot program. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

In light of all the relevant factors, which are explained more fully below, NERC concludes that ReliabilityFirst has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. However, ReliabilityFirst should consider exploring and implementing solutions that will assist ReliabilityFirst in processing the substantial number of violations that it receives on a yearly basis while meeting the performance objectives of the ERO Enterprise.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of ReliabilityFirst's Caseload

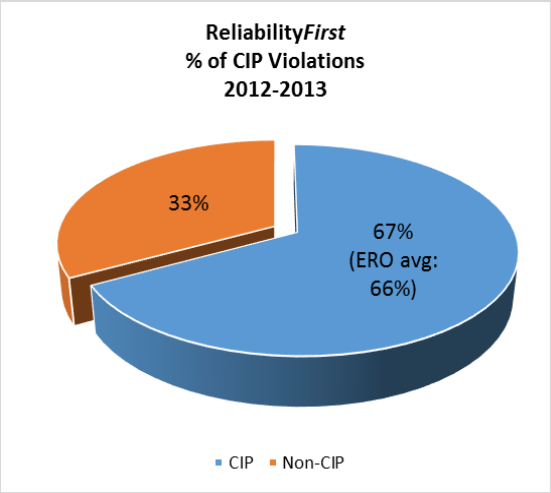
During the assessment period, ReliabilityFirst reported 1,902 violations to NERC, the second highest number among the Regional Entities.

Violations for ReliabilityFirst 2009-2013 by Year Reported to NERC[115]

Year Reported to NERC	Violations Reported
2009	123
2010	469
2011	565
2012	505
2013	240
Total	**1902**

As shown in the table above, ReliabilityFirst reported the highest number of violations in 2011, with a gradual decrease in 2012 and a substantial decrease in 2013. Approximately two-thirds of the violations in 2011 were of the CIP Reliability Standards. In the years 2012 and 2013, violations of CIP Reliability Standards represented 67% of total violations; this percentage is consistent with the ERO Enterprise average of 66%.

Type of Violations Reported to NERC by ReliabilityFirst, 2012-2013

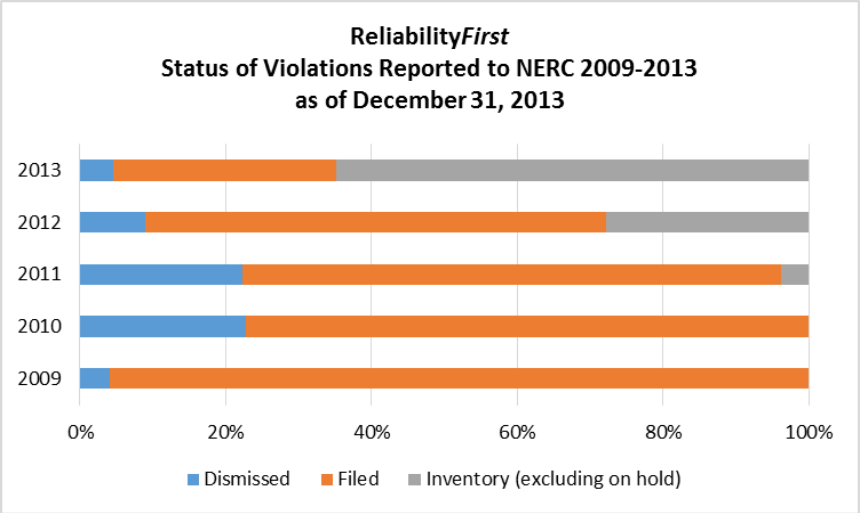


Approximately 76% of the CIP violations were discovered through internal means.

Of the total violations reported to NERC during the assessment period, approximately 316 violations, or approximately 17%, remained to be processed as of December 31, 2013 (excluding violations that are held by appeal, a court, or a regulator). As demonstrated in the table below, ReliabilityFirst has processed all violations that were reported to NERC in 2009 and 2010 (excluding on hold violations). ReliabilityFirst has processed approximately 96% of violations reported to NERC in 2011 (excluding on hold violations), and approximately 72% of violations reported to NERC in 2012.

[115] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 766.

Status of Violations Reported to NERC 2009-2013 for ReliabilityFirst



ReliabilityFirst processed approximately 35% of violations reported to NERC in 2013 (excluding on hold violations). This is slightly lower than the ERO 2013 processing rate of 39%. Further, the percentage of ReliabilityFirst's caseload consisting of violations reported to NERC in 2013 (approximately 49%), is substantially lower than the overall ERO Enterprise average of 67%.

ii. Caseload Index

The Caseload Index for ReliabilityFirst was 9.8 months as of December 31, 2013. Although this is higher than the ERO Enterprise Caseload Index of approximately 6.5 months, NERC notes that ReliabilityFirst performed well, relative to the ERO Enterprise average, for the majority of the assessment period. NERC also recognizes that in 2014, ReliabilityFirst has resolved a significant number of the current set of cases and is on track to resolve the remaining cases that are responsible for the higher-than-average Caseload Index at the end of the assessment period. The majority of these cases are large, multi-regional matters.

iii. Efforts to Reduce Older Caseload

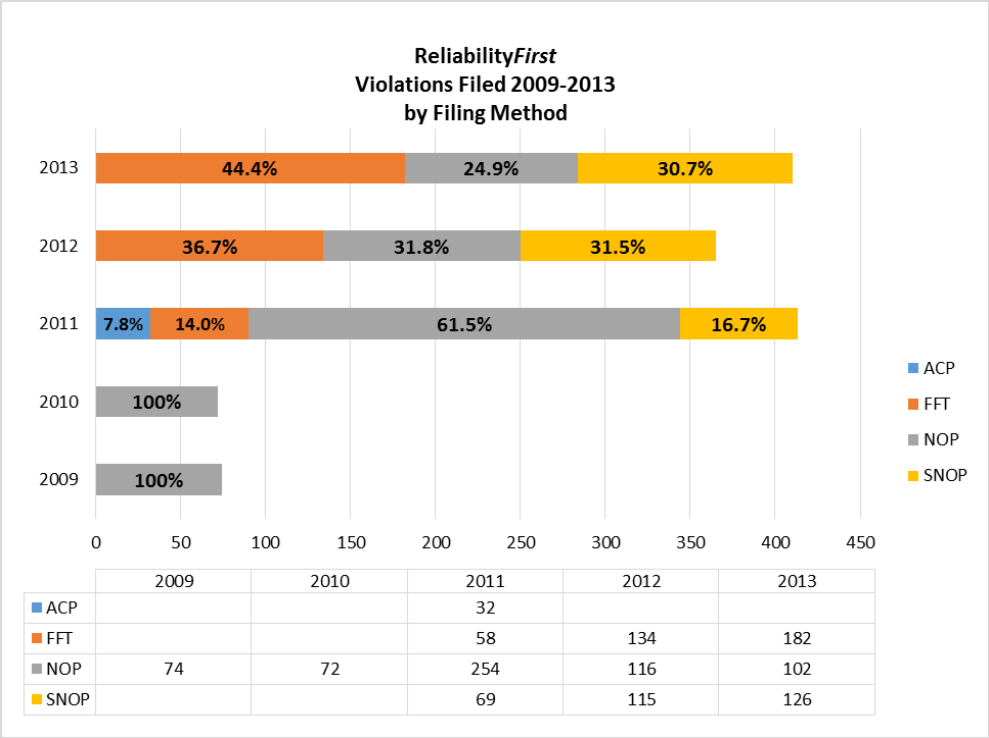
In 2013, ReliabilityFirst reduced the portion of its caseload consisting of violations dating to before 2012 by 88%. NERC commends ReliabilityFirst for its responsiveness and efforts to achieve this important ERO Enterprise goal. ReliabilityFirst reported that its remaining inventory consisted of particularly broad and complex violations that are part of large settlement agreements in the process of being negotiated. ReliabilityFirst also reported that it has been closely monitoring and working with the registered entities to ensure effective and holistic mitigation for these older, more complex violations.

NERC will continue to work with ReliabilityFirst to prioritize the processing of these violations and other older violations so that ReliabilityFirst may achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

ReliabilityFirst effectively used streamlined enforcement processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2011, following the implementation of the streamlined enforcement processing mechanisms, ReliabilityFirst filed 413 violations – more than two-and-a-half times the total of the previous two years combined.

Violations Filed per Year by Filing Method for ReliabilityFirst, 2009-2013



	2009	2010	2011	2012	2013
ACP			32		
FFT			58	134	182
NOP	74	72	254	116	102
SNOP			69	115	126

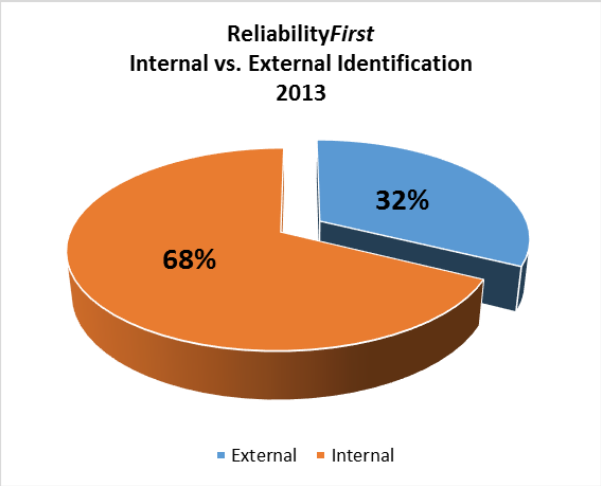
ReliabilityFirst uses the FFT process for minimal or moderate risk violations where it seeks to encourage certain entity behavior (or conversely, where there is there is an absence of behavior that ReliabilityFirst wishes to discourage). ReliabilityFirst prepares NOPs where there are important mitigating actions, above-and-beyond commitments, or reliability concerns that may not be adequately presented in the SNOP format. ReliabilityFirst also confers with other Regional Entities through an enforcement activities working group to ensure that each of the Regional Entities develops consistent documentation for the FFT process and makes consistent risk determinations when deciding whether to grant FFT or SNOP treatment for a violation. NERC expects that ReliabilityFirst will continue to take advantage of further process refinements available under RAI. Additional information regarding ReliabilityFirst's implementation of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised 68% of total violations in the ReliabilityFirst region. This is slightly lower than the ERO Enterprise average of 73%.

Percentage of Violations by Method of Identification for ReliabilityFirst in 2013



ii. Ensuring the Timely Mitigation of Violations

ReliabilityFirst reported that it encourages the prompt submission of mitigation plans in its notices of possible violation, in compliance audit exit briefings, and as part of its enforcement process. ReliabilityFirst considers the prompt submission of mitigation plans when making its penalty determinations and the prompt identification of mitigating activities in its determination of FFT eligibility. ReliabilityFirst has processes in place for the review, acceptance, and verification of mitigation plans, and it has tracking systems in place to help ensure that mitigation plans are submitted, reviewed, and accepted in a timely manner. ReliabilityFirst does not require formal mitigation plans for some minimal and moderate risk violations, but rather requires submission of a formal mitigation plan based on the risk posed by each violation. ReliabilityFirst sends notifications to registered entities when necessary to ensure that they submit mitigation plans promptly and meet associated deadlines. Acceptance and verification of mitigation plans passes through a multi-layer review and approval process. During this process, ReliabilityFirst works closely with the applicable registered entity to ensure that the proposed mitigating activities address the underlying cause of the violation, the time to complete the mitigating activities is reasonable, and effective steps are taken to prevent reoccurrence of violations.

NERC is working closely with ReliabilityFirst to ensure that violations are mitigated in a timely manner. As demonstrated in the table below, ReliabilityFirst has made notable progress in ensuring that older violations have been mitigated, with 100% of violations discovered from 2007-

2009, 98.1% of violations discovered in 2010, and 89.1% of violations discovered in 2011 having completed mitigation.

ReliabilityFirst: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[116]

Year of Discovery	% Completed	% in Progress
2013	24.5%	75.5%
2012	68.3%	31.7%
2011	89.1%	10.9%
2010	98.1%	1.9%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**79.6%**	**20.4%**

ReliabilityFirst reported that it is working closely with registered entities to ensure the completion of effective mitigating activities for these violations. NERC will continue to work closely with ReliabilityFirst to ensure that violations are mitigated in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

ReliabilityFirst has taken a proactive approach to developing a detailed enforcement philosophy. ReliabilityFirst's enforcement philosophy consists of several overarching themes governing enforcement and a series of philosophies governing particular aspects of the enforcement process. ReliabilityFirst's philosophy is to not see the enforcement process as adversarial, but rather as an opportunity to work collaboratively with registered entities to craft forward-thinking resolutions designed to enhance reliability. ReliabilityFirst's philosophy is to use the enforcement process as a tool to shape and encourage desired registered entity behavior, and to only assess monetary penalties where the penalty is appropriate to encourage or discourage behavior and where the justification is supported by sound, consistent, and risk-based reasoning. ReliabilityFirst encourages the development of strong internal controls and other steps taken to improve compliance.

In its settlement processes, ReliabilityFirst has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

[116] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations.

ReliabilityFirst has worked with registered entities to include commitments in their mitigation plans going beyond those actions necessary to mitigate the underlying violations. Several notable examples are presented here. One registered entity committed to an aggressive timeline for the completion of mitigating actions, including completing certain activities faster than required by NERC guidance. To resolve a violation involving facility ratings, one registered entity committed to perform a broad review and verification of system components, to implement a new ratings software application, and to use LiDAR-based Power Line Systems – Computer Aided Design and Drafting (PLS-CADD) modeling as a supplemental tool to identify site conditions that may indicate potential ratings issues. One registered entity committed to perform an ongoing risk analysis of its cybersecurity policies and procedures using a Failure Modes Effects Analysis tool (a continuous improvement tool to improve the quality of process outputs by identifying and removing the cause of defects and errors and minimizing variability in processes). Another registered entity committed to conduct an evaluation of the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and create and implement an action plan with the goal of increasing the entity's maturity indicator level in domains related to the CIP Reliability Standards. ReliabilityFirst has also imposed the non-monetary sanction of conducting an unscheduled audit before the next six-year scheduled audit to ensure that a registered entity's implementation of a new compliance program improved and better positioned the registered entity's compliance posture prospectively. NERC encourages ReliabilityFirst to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. ReliabilityFirst's Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to ReliabilityFirst.

With respect to assessing monetary penalties, ReliabilityFirst reported that it has implemented a multi-step internal process for making penalty determinations. First, an assigned case manager makes all penalty recommendations (subject to senior executive review and approval) for his or her assigned registered entities, including the application of the adjustment factors set forth in the NERC *Sanction Guidelines*. Second, ReliabilityFirst has implemented what it calls the "Risk-Harm" process, whereby technical experts answer a series of questions about the risk and harm posed by each violation using a common scale which results in a quantified risk assessment for each violation. Third, ReliabilityFirst analyzes the risk assessment produced from the Risk-Harm process and checks to ensure that the penalty is consistent with the risk posed by the violation. Fourth, ReliabilityFirst looks at previously assessed penalties for comparable violations in the ReliabilityFirst region and in other regions, to ensure the internal and external consistency of its penalties. Finally, ReliabilityFirst requires senior management approval for each settlement agreement or Notice of Alleged Violation and Penalty, to ensure that the penalty is consistent with the risk posed by the violations at issue and is consistent with the enforcement philosophy it wishes to convey to other entities in the region. NERC reviews all penalties

submitted by ReliabilityFirst for appropriateness and consistency with monetary penalties assessed by ReliabilityFirst and other Regional Entities for violations of the same Reliability Standards and requirements occurring under similar facts and circumstances. NERC has found that ReliabilityFirst assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that ReliabilityFirst dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC identified opportunities for ReliabilityFirst to improve its letters of dismissal and communicated those opportunities to ReliabilityFirst. By implementing the recommended improvements, ReliabilityFirst can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of ReliabilityFirst FFT issues filed or posted during the assessment period to examine ReliabilityFirst's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that ReliabilityFirst has clear FFT processes that follow the directives, principles, and processes of the NERC guidance and the directives issued by the Commission regarding FFTs. NERC found that ReliabilityFirst applies its processes consistently. NERC noted several ways that ReliabilityFirst could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that ReliabilityFirst has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. ReliabilityFirst should adopt the recommendations for improvement noted above and the recommendations provided as part of NERC's oversight activities. In particular, based on ReliabilityFirst's recent performance in several enforcement processing metrics, ReliabilityFirst is encouraged to continue to identify and implement solutions so that it is better equipped to ensure that violations are processed as quickly as practicable consistent with the circumstances of each violation.

6. Evaluation of SERC Reliability Corporation

a. Overview

In the three-year performance assessment, NERC concluded that SERC was an effective Regional Entity.[117] Consistent with the overall findings for the ERO, NERC noted a need to improve the efficiency of enforcement processes. During the assessment period, SERC made a number of organizational and process improvements to streamline its enforcement process and elevate enforcement within the SERC organizational structure.[118] In particular, SERC has expanded its CIP capabilities based on the increase of CIP violations reported to the region.

[117] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 26.

[118] 2014 JRESA, Appendix 2-B at 5.

During the assessment period, SERC has increased the number of FTE staff dedicated to enforcement from 4.25 FTE in 2009 to 7 FTE as of December 31, 2013. Based on SERC's recent improvements in its processing speed and efficiency (as measured at the end of the assessment period), NERC views SERC's enforcement staffing to be sufficient to process the number of violations that it receives.

SERC ended the assessment period with a Caseload Index that was notably better than the ERO Enterprise Caseload Index. SERC processed a substantial number of violations discovered before 2012 in furtherance of an ERO Enterprise goal and in so doing, improved its performance and shifted the composition of its caseload to newer violations. NERC has reviewed SERC's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, SERC generally implements these processes in a satisfactory manner.

In addition, SERC staff have actively participated in the development of RAI. SERC staff have participated in the Aggregation of Minimal Risk Issues and Enforcement Discretion pilot programs, and have provided input and feedback during the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* development processes. In addition, SERC staff have participated in the process to develop improvements for the compliance and enforcement oversight of MRREs. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

As explained more fully below, NERC concludes that SERC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. However, work remains to be done to ensure that violations are mitigated in a timely manner. Going forward, NERC will work with SERC to ensure that violations are mitigated promptly, with an added emphasis on ensuring the completion of mitigation for older violations.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of SERC's Caseload

During the assessment period, SERC reported 1,393 violations to NERC.

Violations for SERC 2009-2013 by Year Reported to NERC[119]

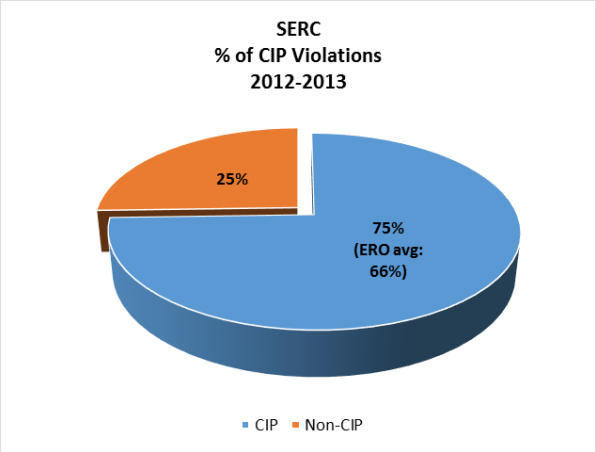
Year Reported to NERC	Violations Reported
2009	187
2010	312
2011	309
2012	300
2013	285

[119] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 76.

Total	**1393**

As shown in the table above, SERC reported a fairly steady number of violations from 2010-2013. In the years 2012 and 2013, violations of CIP Reliability Standards represented a higher percentage (75%) of total violations in the SERC region than the ERO Enterprise as a whole.

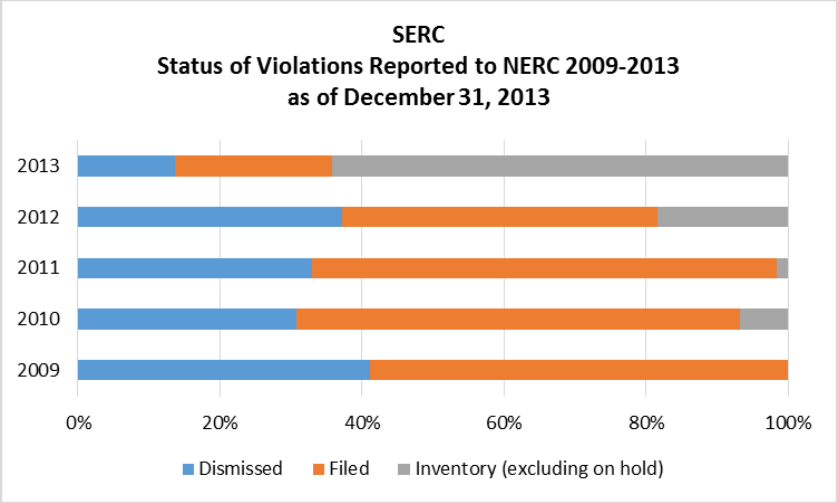
Type of Violations Reported to NERC by SERC, 2012-2013



Over two-thirds of CIP violations received from SERC in 2012 and 2013 were self-identified. SERC's recent expansion of its CIP capabilities should assist SERC in ensuring the timely evaluation and processing of the CIP violations it has received as well as the CIP violations it is likely to receive in the future.

Of the total violations reported by SERC to NERC during the assessment period, approximately 264 violations, or 19%, remained to be processed as of December 31, 2013 (excluding violations that are held by appeal, a court, or a regulator). As demonstrated in the table below, SERC has processed all violations reported to NERC in 2009, 93% of violations reported to NERC in 2010, 98% of violations reported to NERC in 2011, and 82% of violations reported to NERC in 2012 (excluding on hold violations).

Status of Violations Reported to NERC 2009-2013 for SERC



SERC processed approximately 36% of violations it reported to NERC in 2013. This is slightly lower than the ERO 2013 processing rate of 39%. However, violations reported to NERC in 2013 represent approximately 69% of the violations available for processing in SERC's caseload, which is consistent with the overall ERO Enterprise average of 67%.

ii. Caseload Index

The Caseload Index for SERC is 5.1 months as of December 31, 2013. This is better than the ERO Enterprise Caseload Index of approximately 6.5 months and represents a significant improvement in SERC's performance from earlier in the assessment period.

Through 2013, SERC improved its pace of enforcement processing in a dedicated effort to process its older violations. SERC reduced the average age of violations in its inventory by approximately three months from the end of the first quarter of 2013 to the end of 2013. SERC's processing efforts are reflected in the Caseload Index and the other informational measures described in this assessment.

iii. Efforts to Reduce Older Caseload

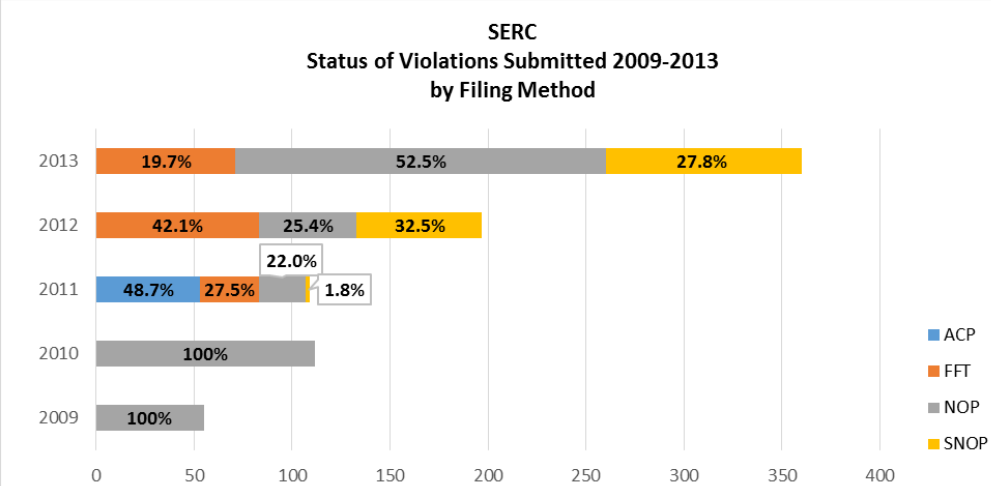
In 2013, SERC reduced its pre-2012 caseload by 92%. Over 90% of these pre-2012 violations were of the CIP Reliability Standards. NERC commends SERC for its responsiveness and efforts to achieve this important ERO Enterprise goal. SERC's remaining pre-2012 violations were in the settlement process or scheduled for processing in early 2014. NERC will work with SERC to ensure that these older violations are resolved and that future accumulations of older violations in the SERC region does not occur.

Based on the current composition of its inventory of violations available to be processed and its recent success in processing its older violations, SERC is positioned to achieve the ERO Enterprise goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

SERC believes that its processing of violations has improved because of increased resources and improved tools such as FFT and the SNOP filing mechanisms.[120] As demonstrated in the table below, SERC effectively used streamlined enforcement processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2010, SERC filed an exceptionally high number of violations using the NOP format; in subsequent years, it used the streamlined enforcement processing mechanisms to file 50% or more of violations. In 2013, SERC had a higher percentage of violations processed as an NOP than most Regional Entities, based in large part on SERC's efforts to reduce the number of older, higher-risk CIP violations in its inventory.

Violations Filed per Year by Filing Method for SERC, 2009-2013



	2009	2010	2011	2012	2013
ACP			53		
FFT			30	83	71
NOP	55	112	24	50	189
SNOP			2	64	100

SERC generally uses the FFT process for minimal risk issues, the SNOP process for minimal and moderate risk issues and medium-scale compliance failures, and the NOP process for serious risk issues or large-scale compliance failures. SERC reviews previously-filed violations by SERC and other Regional Entities as part of its process for determining the appropriate enforcement processing mechanism. NERC expects that SERC will continue to reserve the NOP format for violations that require it and take advantage of further process refinements available under RAI. Additional information regarding SERC's implementation of FFT is presented later in this assessment.

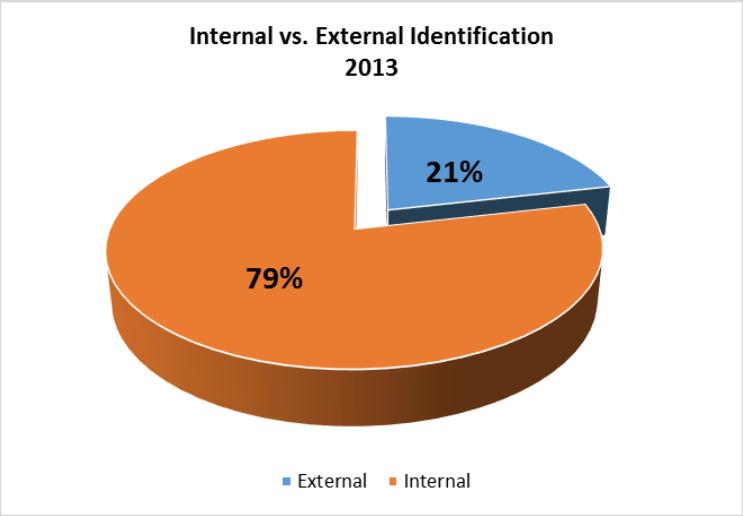
[120] 2014 JRESA, Appendix 2-C at 24.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised 79% of total violations in the SERC region. This is somewhat higher than the ERO Enterprise average of 73%.

Percentage of Violations by Method of Identification for SERC in 2013



ii. Ensuring the Timely Mitigation of Violations

SERC reported that it has taken several steps to encourage the timely mitigation of violations. First, SERC encourages and discusses the benefits of prompt submission of mitigation plans during its compliance seminars, open forum web conferences, and its compliance program updates to its board of directors. SERC requires a registered entity, when submitting a self-report form, to provide the status of its mitigating activities, detailed information on mitigating activities that are in progress or are completed, and the registered entity's efforts to prevent reoccurrence. To ensure timely follow-up and completion of mitigation plans, SERC has dedicated a staff member to mitigation processing for operations and planning violations, and several staff members share responsibility for CIP mitigation processing. SERC believes that the efforts of its enforcement staff to discover the complete scope of each violation are likely to result in the creation of mitigation plans that fully address each violation and reduce the likelihood of reoccurrence. SERC tracks mitigation plan information and documents in its compliance information tracking system, including mitigation plans submitted by entities, mitigating activities submitted through self-reports or other means, any revisions requested by SERC, and certifications of mitigation plan completion. If a registered entity does not include mitigating activities in its self-report form, SERC enforcement staff will contact the registered entity to ensure that mitigating activities are occurring. SERC may accept the mitigating activities and details to prevent reoccurrence, through the self-report form, as an informal mitigation plan. The review and acceptance process is similar for both mitigating activities and a formal mitigation plan. In the

case of mitigating activities, SERC does not send a formal notification of its review to the registered entity, but SERC reviews and confirms completion. SERC reported that it works with registered entities to answer questions about SERC's expectations for mitigation plans, and that it has occasionally requested that a registered entity revise a mitigation plan when proposed milestones would result in an extended period of noncompliance posing an additional risk to the BPS.

Many of the mitigation plans in the SERC region from 2010 and 2011 that are still in progress are for issues where SERC has combined more recent instances of noncompliance into the older enforcement action. In many of those cases, the registered entities have completed mitigating activities for the older occurrences but are still completing the mitigating activities for the newer occurrences.

SERC: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[121]

Year of Discovery	% Completed	% in Progress
2013	27.8%	72.2%
2012	75.9%	24.1%
2011	81.7%	18.3%
2010	83.8%	16.2%
2009	100.0%	0.0%
2008	96.9%	3.1%
2007	100.0%	0.0%
Grand Total	**74.6%**	**25.4%**

As shown in the table above, as of December 31, 2013, SERC had a small number of 2008 violations for which mitigating activities had not been completed. These violations involve a single registered entity, and the violations are currently on hold due to a pending court case involving a similarly-situated registered entity. SERC reported that the pending court case has impacted its ability to verify the timely completion of mitigation for these violations. .

NERC will continue to work with SERC to ensure that newer violations are mitigated in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

SERC's enforcement philosophy is to manage all enforcement activities in an unbiased, fair, transparent, and consistent manner, affording registered entities appropriate due process. SERC strives to manage all enforcement actions in such a way to ensure consistent application of penalties for violations of Reliability Standards. SERC's view of the enforcement process is that

[121] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations.

it should be used to assist registered entities in assessing, understanding, and managing risk to the BPS and deploying innovative solutions to not only restore compliance, but also mitigate risk, increase reliability, and prevent reoccurrence. SERC believes that it is important to leverage relationships with registered entities and other Regional Entities to promote effective collaboration, cooperation, and communication around significant risks to the reliability of the BPS to produce outcomes that effectively manage risk.

In its settlement processes, SERC has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

As examples of above-and-beyond activities, SERC has accepted the following commitments as formal conditions of settlement. To address a series of CIP violations, a registered entity committed to centralize physical monitoring activities by implementing a new access control and video monitoring system and establishing a central security monitoring station.[122] To settle another series of CIP violations, a registered entity committed to conduct an evaluation of the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and share the evaluation with SERC; create and implement an action plan with the goal of increasing the entity's maturity indicator level in domains related to the CIP Reliability Standards; provide SERC with quarterly updates regarding its progress in implementing the action plan; and provide SERC with notification and evidence upon completion of activities.[123] NERC encourages SERC to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. SERC's Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to SERC.

With respect to the assessment of monetary penalties, SERC reviews previously-filed violations by SERC and other Regional Entities as part of its process to determine appropriate monetary penalties for violations. SERC seeks to apply a uniform process for determining monetary penalties that ensures that they are both (i) appropriate in light of the scope of, and risk posed by, the violations, and (ii) reasonable in light of monetary penalties levied by SERC and other Regional Entities for similar violations. NERC reviews all penalties submitted by SERC for appropriateness and consistency with monetary penalties assessed by SERC and other Regional Entities for violations of the same Reliability Standards and requirements occurring under similar

[122] *Unidentified registered entity*, NP14-18-000 (Dec. 30, 2013).

[123] *See Unidentified registered entity*, NP14-21-000 (Dec. 31, 2013).

facts and circumstances. NERC has found that SERC assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that SERC dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC identified opportunities for SERC to improve its letters of dismissal and communicated those opportunities to SERC. By implementing the recommended improvements, SERC can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of SERC FFT issues filed or posted during the assessment period to examine SERC's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that SERC's documented FFT process was adequate and that SERC follows its process. NERC noted that SERC generally provides all relevant information in its issue description, ensures the completion of mitigating activities, and considers violation history appropriately. NERC noted several ways that SERC could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that SERC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. SERC should adopt the recommendations for improvement provided as part of NERC's oversight activities.

7. Evaluation of Southwest Power Pool Regional Entity

a. Overview

In the three-year performance assessment, NERC expressed concerns about SPP RE's ability to process violations to completion in a timely manner.[124] During the current assessment period, SPP RE developed and streamlined enforcement procedures and increased enforcement staff in an effort to reduce processing times.[125] SPP RE now also has internal performance metrics in place to encourage the processing of violations as quickly as possible.

During the assessment period, SPP RE increased the number of FTE staff dedicated to enforcement from one FTE in 2009 to ten FTEs and one part-time employee as of December 31, 2013. Based on SPP RE's processing speed and efficiency as measured at the end of the assessment period, NERC views SPP RE's enforcement staffing to be sufficient to process the number of violations that it receives in accordance with ERO Enterprise performance objectives.

SPP RE closed the assessment period with a Caseload Index consistent with the ERO Enterprise average. SPP RE also made remarkable progress in meeting older caseload reduction goals for 2012 and 2013. Finally, NERC has reviewed SPP RE's enforcement-related processes

[124] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 24.

[125] 2014 JRESA, Appendix 2-B at 5.

as part of its oversight role and found that, while areas for improvement remain, SPP RE generally implements those processes in a satisfactory manner.

SPP RE staff have actively participated in the development of RAI. SPP RE staff participated in several NERC working groups that are developing, testing, and implementing the Aggregation of Minimal Risk Issues and Enforcement Discretion pilot programs. SPP RE staff took a leadership role in the development of the *ERO Enterprise Mitigation Plan Guide*. In addition, SPP RE staff also participated in various RAI projects and programs falling under the compliance function. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

In light of all of the relevant factors, which are explained more fully below, NERC concludes that SPP RE has performed as an effective Regional Entity during the assessment period with respect to enforcement activities. NERC will continue to work with SPP RE to ensure that violations are processed and mitigated promptly, with an emphasis on ensuring the completion of mitigation for older violations.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of SPP RE's Caseload

During the assessment period, SPP RE reported 1,041 violations to NERC.

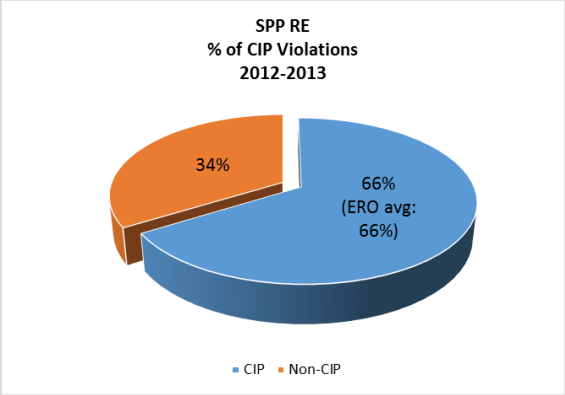
Violations for SPP RE 2009-2013 by Year Reported to NERC[126]

Year Reported to NERC	Violations Reported
2009	132
2010	254
2011	291
2012	173
2013	191
Total	**1041**

As shown in the table above, SPP RE reported its highest number of violations in 2010 and 2011. CIP violations were the majority of those violations. In the years 2012 and 2013, violations of CIP Reliability Standards comprised 66% of total violations. This is consistent with the ERO Enterprise average.

[126] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 76.

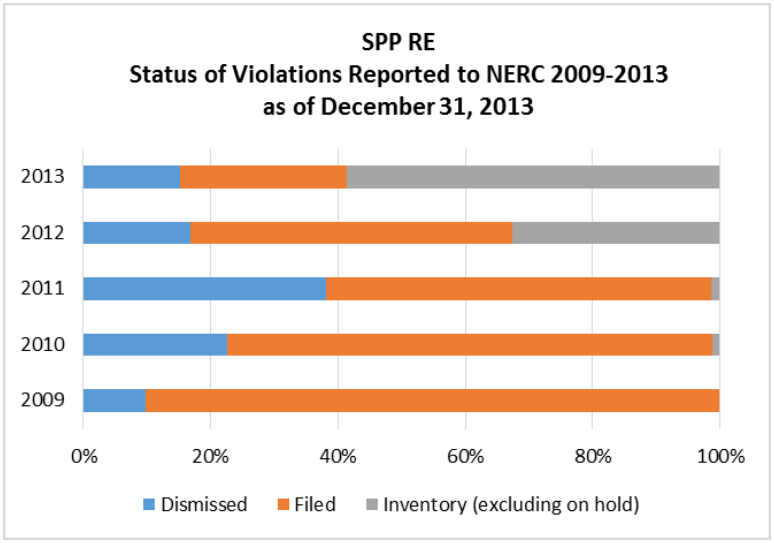
Type of Violations Reported to NERC by SPP RE, 2012-2013



Approximately 56% of CIP violations were discovered through internal mechanisms.

Of the total violations reported by SPP RE to NERC during the assessment period, approximately 175 violations, or about 17%, remained to be processed as of December 31, 2013 (excluding on-hold violations). As demonstrated in the table below, as of December 31, 2013, SPP RE had processed all violations that were reported to NERC in 2009; 98.8% of violations reported to NERC in 2010; 98.6% of violations reported to NERC in 2011; and 67.4% of violations reported to NERC in 2012 (excluding on hold violations).

Status of Violations Reported to NERC 2009-2013 for SPP RE



SPP RE processed approximately 41% of violations reported to NERC in 2013. This is consistent with the ERO 2013 processing rate of 39%. The percentage of SPP RE's caseload consisting of violations reported to NERC in 2013 (64%) is also consistent with the overall ERO Enterprise average of 67%.

ii. Caseload Index

The Caseload Index for SPP RE is 8.3 months as of December 31, 2013. This is slightly higher than the ERO Enterprise Caseload Index of approximately 6.5 months, but nevertheless lower than the 2013 ERO Enterprise average goal of 10 months.

In light of SPP RE's Caseload Index and as reflected in the characteristics of its caseload (i.e., the percentage of SPP RE's caseload consisting of older violations is consistent with the ERO average), it appears that SPP RE's efforts to streamline its enforcement processes and increase its enforcement staffing during the assessment period have been effective.

iii. Efforts to Reduce Older Caseload

In 2013, SPP RE reduced its pre-2012 caseload by 96%.[127] NERC commends SPP RE for its responsiveness and efforts to achieve this important ERO Enterprise goal. SPP RE states that several factors specific to the remaining violations caused delays in processing, but SPP RE expects to resolve those issues in 2014.

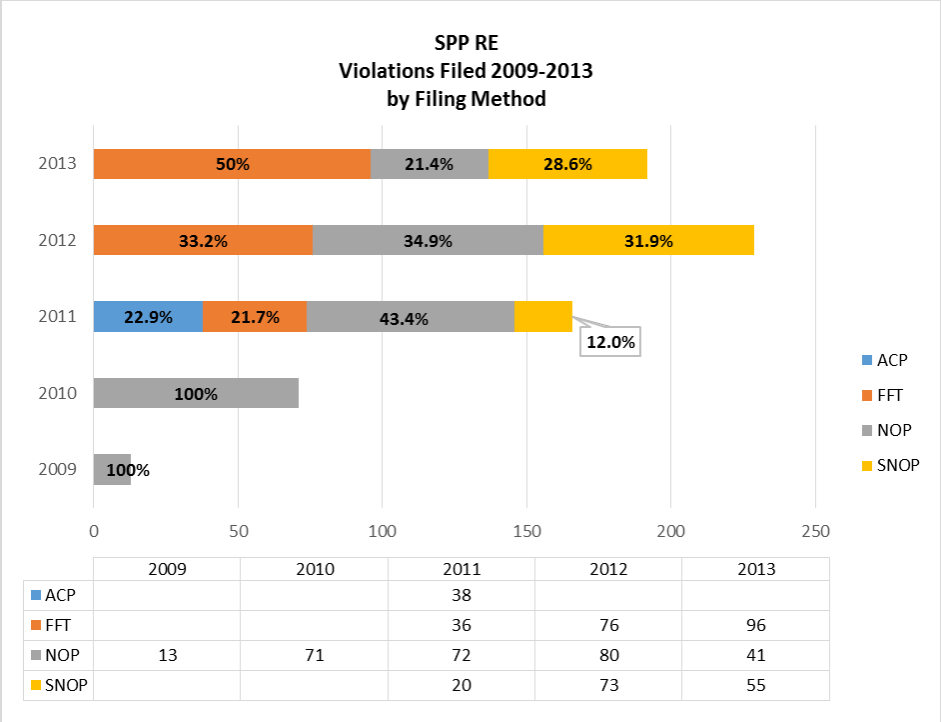
Based on the current composition of its inventory of violations available to be processed and its largely successful efforts in processing its older violations, SPP RE is positioned to achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

From 2007 through 2010, SPP RE filed a total of 89 violations. In 2011, SPP RE filed a total of 166 violations, almost double the total number of violations from the previous three years combined. SPP RE credits its success in improving its violation processing rate to several factors. SPP RE developed internal enforcement procedures, streamlined its enforcement processes, and dedicated resources to increasing both the number and maturity of its enforcement staff. For example, SPP RE decreased the time it spends drafting CMEP required and related documents by utilizing its compliance database to automate the issuance of a number of documents. In addition, SPP RE effectively implemented alternative enforcement processing mechanisms, including using FFT to process its lower-risk violations, as demonstrated in the table below.

[127] All but four pre-2012 violations were processed before the end of 2013. Of the four violations, two were MRRE violations for which another Regional Entity took lead responsibility. One violation was being held pending an interpretation of the associated Reliability Standard.

Violations Filed per Year by Filing Method for SPP RE, 2009-2013



	2009	2010	2011	2012	2013
ACP			38		
FFT			36	76	96
NOP	13	71	72	80	41
SNOP			20	73	55

SPP RE filed the majority of violations using FFT or SNOP in 2012 and 2013. In 2013, the percentage of FFTs relative to SNOPs increased notably. SPP RE generally limits the use of the FFT process to minimal risk issues, and it uses the SNOP process for those violations that do not represent a serious or substantial risk to the BPS and do not qualify for FFT disposition. Every FFT and SNOP is reviewed by the SPP RE sanction review team to ensure consistency and uniform application. Going forward, NERC encourages SPP RE to continue its review processes and consider increasing the use of FFT for moderate risk issues that qualify for FFT.

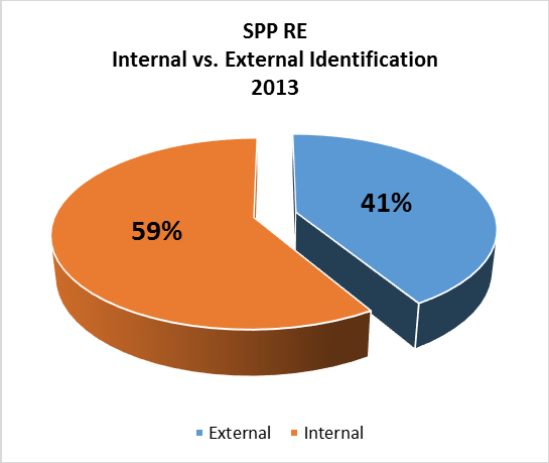
c. Improving Reliability

i. Encouraging Internal Discovery of Violations

SPP RE regularly encourages the value of self-reporting, and it gives presentations on how to self-report effectively during its regional workshops. Additionally, SPP RE discusses the value of self-reporting when it gives penalty determination presentations at workshops.

In 2013, violations discovered by registered entities through internal mechanisms comprised 59% of total violations in the SPP RE region. This is lower than the ERO Enterprise average of 73%. Stated differently, during the assessment period, SPP RE discovered a higher percentage of violations through external methods (i.e., compliance audit and spot check) than other Regional Entities.

Percentage of Violations by Method of Identification for SPP RE in 2013



As noted above, NERC and the Regional Entities are working to understand the regional variations in the percentages of noncompliance discovered through self-discovery and audits across the ERO Enterprise. Understanding these differences, and how they may relate to registered entity internal controls and management practices, will allow NERC and the Regional Entities to provide the right incentives for discovering and self-reporting noncompliance.

ii. Ensuring the Timely Mitigation of Violations

SPP RE has undertaken a number of efforts to encourage the timely mitigation of violations. It has implemented internal metrics to: (i) encourage enforcement staff to solicit mitigation plans as soon as possible for higher-risk violations; (ii) measure whether mitigation plans are accepted or rejected within 30 days of submission; and (iii) measure whether mitigation plan completion evidence is reviewed by SPP RE staff within 30 days of when the registered entity's certification of mitigation plan completion and associated evidence are submitted. SPP RE tracks mitigation plan information in its webCDMS. SPP RE has put standardized processes in place for the review and approval of registered entity mitigation plans, and the associated forms become part of the violation case record.

SPP RE requires registered entities to complete mitigation plans for all compliance issues identified for FFT treatment, and it requires each registered entity desiring to remain in settlement negotiations to submit an acceptable mitigation plan. SPP RE typically requires mitigation plans to be completed before it will execute a settlement agreement and file it with NERC. [128]

SPP RE has strengthened its active monitoring of mitigation plans by increasing its communication with registered entities since 2010. SPP RE issues email reminder notices to registered entities as due dates approach. SPP RE staff has continued to communicate and give

[128] SPP RE does not yet accept completion of mitigating activities in lieu of a formal mitigation plan; however, SPP RE reported that will accept mitigating activities as soon as appropriate changes are made to the webCDMS system.

presentations to registered entities regarding best practices for submitting and managing information associated with self-reports, self-certifications, and mitigation plans.

As demonstrated in the table below, SPP RE has made substantial progress in ensuring that older violations have been mitigated, with 100% of violations discovered from 2007-2009 having completed mitigation.

SPP RE: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[129]

Year of Discovery	% Completed	% in Progress
2013	43.6%	56.4%
2012	77.8%	22.2%
2011	96.7%	3.3%
2010	96.0%	4.0%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**84.0%**	**16.0%**

NERC is working closely with SPP RE to understand the nature of the violations with open mitigation, particularly the older violations. NERC is also working with SPP RE to ensure that violations are mitigated in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

SPP RE reported that it has been its experience that most registered entities desire to be as reliable and as compliant as possible, and that avoiding or minimizing penalties and sanctions is only a secondary motivation. SPP RE reported that it has undertaken a number of efforts to improve the efficiency of its enforcement processes and encourage the prompt mitigation of violations. For instance, SPP RE has supplied registered entities with online training videos covering topics such as evidence submission, mitigation processing, and self-reporting. SPP RE was recently awarded the Bronze Quill Award of Merit from the International Association of Business Communicators, Arkansas Chapter for the quality of its video library. SPP RE developed a flow diagram that is used for small group discussions at regional workshops. The diagram facilitates conversation about the enforcement process with registered entities and provides a visual aid for how violations and mitigation plans move through the enforcement process. SPP RE has also conducted on-site visits with several registered entities to discuss internal compliance program improvements following negative audit findings.

[129] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations.

SPP RE's enforcement group tracks various metrics on a monthly basis, including: (i) the expediting of high risk violations; (ii) caseload processing time: (iii) mitigation plan acceptance review time; (iv) mitigation plan completion review time; (v) processing of pre-2013 violations; (vi) incoming compliance issue triage time; and (vii) case record review and close-out time. To facilitate transparency, SPP RE posts a monthly metrics tracking dashboard covering these areas on its web page.[130]

The FFT process has enabled SPP RE to improve its processing efficiency substantially. As a result, SPP RE reported that it has been able to devote a substantial portion of the efforts of its personnel toward evaluating and processing higher-risk violations.

In its settlement processes, SPP RE has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. For example, SPP RE has considered a registered entity's initiatives to audit and improve its internal compliance program to be a mitigating factor in SPP RE's penalty determination. NERC encourages SPP RE to continue deploying such solutions that promote reliability and insight into processes that can manage risk.

d. SPP RE's Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to SPP RE.

With respect to the assessment of monetary penalties, SPP RE requires its case managers to follow the penalty guidance established by NERC and the Commission. Each violation and its associated penalty must be approved by the SPP RE sanction review team. When presenting a violation and proposed penalty to the sanction review team, an SPP RE case manager will provide the basis for the proposed penalty and a comparison to similar violations and the penalties assigned to those violations. The SPP RE sanction review team will then review the violation and proposed penalty to determine whether the proposed penalty is justified, reasonable, and consistent with penalties assessed for similar violations by SPP RE and by other Regional Entities. NERC reviews all penalties submitted by SPP RE for appropriateness and consistency with monetary penalties assessed by SPP RE and other Regional Entities for violations of the same Reliability Standards and requirements occurring under similar facts and circumstances. NERC has found that SPP RE assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that SPP RE dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC

[130] *See* http://www.spp.org/section.asp?group=2754&pageID=27.

identified opportunities where SPP RE could improve its letters of dismissal and communicated those opportunities to SPP RE. SPP RE has already implemented at least one of the recommended improvements. These improvements will ensure SPP RE has access to the information it needs to process each violation properly. Such efforts will also assist NERC in its oversight role and allow the Commission to evaluate the efficiency and effectiveness of the dismissal process.

As part of its ongoing FFT review processes, NERC reviewed a sample of SPP RE FFT issues filed or posted during the assessment period to examine SPP RE's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. NERC noted that SPP RE developed a checklist which delineates the steps that need to be taken by each SPP RE staff member and indicates that the final document will be attached to the record for tracking purposes. If completed on a regular basis, this checklist could provide valuable insight into SPP RE's determination of FFT treatment and facilitate future review by NERC and the Commission. NERC recommended several areas in which SPP RE could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that SPP RE has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. SPP RE should adopt the recommendations for improvement provided as part of NERC's oversight activities.

8. Evaluation of Texas Reliability Entity, Inc.

a. Overview

In the three-year performance assessment, NERC concluded that Texas Regional Entity was an effective Regional Entity, and it praised Texas Regional Entity's processing efficiency and focus on identifying higher-risk violations that result from failure to comply with Reliability Standards.[131] At the time, NERC noted questions regarding the contrast between the high percentage of "failure to perform" violations and the low number of violations recommended for a zero-dollar penalty. Texas RE reported that it recommended zero-dollar penalties in 2007 and 2008 for most cases as the Reliability Standards were new, and registered entities were still learning how to comply with them. Texas RE reported that it began recommending more monetary penalties for "failure to perform" violations in 2010 in an effort to deter noncompliance. As the streamlined enforcement mechanisms were developed and implemented, Texas RE began using these mechanisms to process violations posing a low risk to reliability and that had been mitigated.[132] Texas RE also made organizational changes related to its enforcement processes in late 2013 to provide for a clear delineation between processing tasks; Texas RE believes that these changes have resulted in efficiency gains and decreased processing time.

[131] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 26.

[132] 2014 JRESA, Appendix 2-B at 6.

During the assessment period, Texas RE increased the number of FTE staff dedicated to enforcement from 3 in 2009 to 11 as of December 31, 2013. Based on Texas RE's processing speed and efficiency as measured at the end of the assessment period, NERC views Texas RE's enforcement staffing to be sufficient to process the number of violations that it receives.

Texas RE ended the assessment period with a Caseload Index that was the lowest among all Regional Entities. Texas RE processed all violations discovered before 2012 in furtherance of an ERO Enterprise goal. Texas RE's caseload tends to consist of more-recent violations, and generally, Texas RE has made progress in ensuring that older violations have completed mitigation. Finally, NERC has reviewed Texas RE's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, Texas RE generally implements those processes in a satisfactory manner.

In addition, Texas RE staff have actively participated in the development of RAI. Many Texas RE employees worked on various aspects of RAI in collaboration with NERC and the other regions. Texas RE staff participated in the Aggregation of Minimal Risk Issues and Enforcement Discretion pilot programs and served on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. Texas RE staff also participated in several compliance-related programs under RAI. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

As explained more fully below, based on Texas RE's performance in several enforcement processing metrics and the results of NERC's oversight activities, NERC concludes that Texas RE has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. NERC will continue to work with Texas RE to ensure that violations are mitigated promptly.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of Texas RE's Caseload

During the assessment period, Texas RE reported 861 violations to NERC.

Violations for Texas RE 2009-2013 by Year Reported to NERC[133]

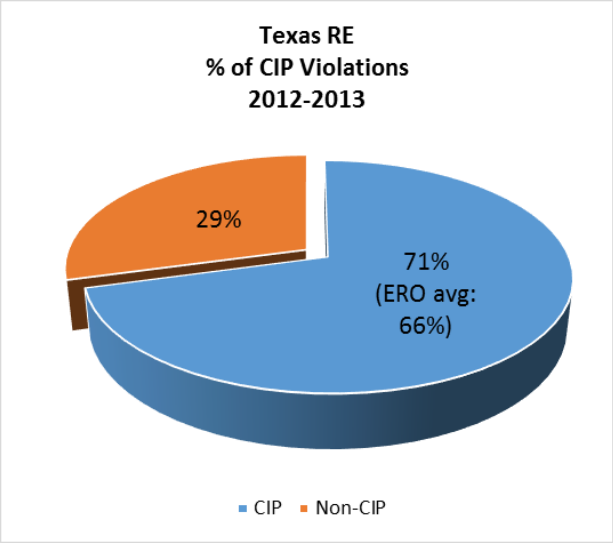
Year of Submission	Violations Reported
2009	14
2010	51
2011	430
2012	197
2013	169

[133] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 76.

Total	**861**

As shown in the table above, Texas RE reported a spike in violations in 2011..[134] The violations reported to NERC in 2011 were split almost evenly between CIP and non-CIP violations and internal and external methods of discovery. In the years 2012 and 2013, violations of CIP Reliability Standards represented a higher percentage of total violations in the Texas RE region than the ERO Enterprise as a whole.

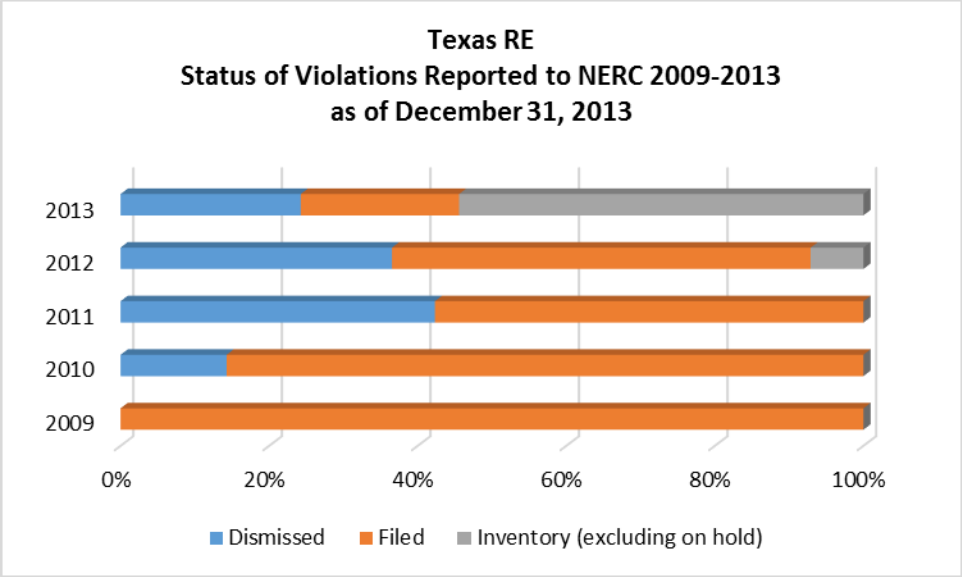
Type of Violations Reported to NERC by Texas RE, 2012-2013



Of the total violations reported to NERC during the assessment period, 106 violations, or approximately 12%, remained to be processed as of December 31, 2013 (excluding violations that are held by appeal, a court, or a regulator). As demonstrated in the table below, Texas RE has processed all violations reported to NERC in 2009, 2010, and 2011 (excluding on hold violations). Texas RE processed approximately 93% of violations reported to NERC in 2012.

[134] When adjusted for year of discovery, 157 violations were discovered in 2010, and 298 violations were discovered in 2011.

Status of Violations Reported to NERC 2009-2013 for Texas RE



Texas RE processed approximately 46% of violations reported to NERC in 2013, which is better than the ERO Enterprise average 2013 processing rate of 39%. Approximately 87% of the violations available for processing in Texas RE's inventory consist of violations reported to NERC in 2013. This greatly exceeds the overall ERO Enterprise average of 67%. Texas RE appears to be moving toward a caseload consisting primarily of newer violations.

ii. Caseload Index

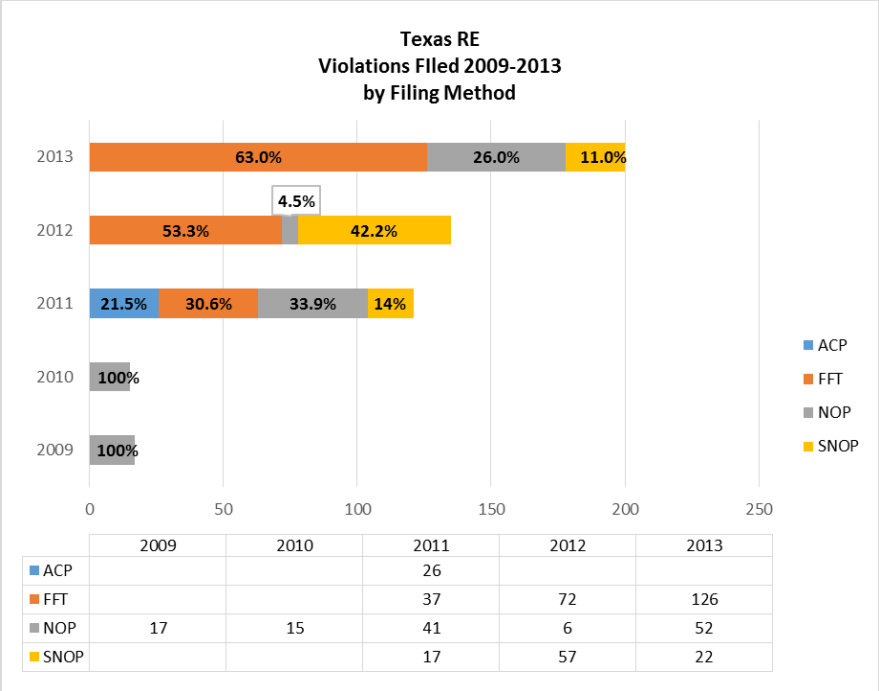
The Caseload Index for Texas RE is 3.8 months as of December 31, 2013. This is the lowest of all Regional Entities and notably better than the ERO Enterprise Caseload Index of approximately 6.5 months.

Based on the current composition of its inventory of violations available to be processed and its success in achieving the timely processing of violations to date, Texas RE is well-positioned to achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iii. Implementation of Streamlined Enforcement Processing Mechanisms

A number of factors are responsible for Texas RE's successes in processing its caseload. As demonstrated in the table below, Texas RE effectively used alternative processing mechanisms to process a substantial portion of its caseload during the assessment period. In 2011, following the implementation of the streamlined enforcement processing mechanisms, Texas RE filed 121 violations – almost quadruple the number of violations filed in the previous two years combined.

Violations Filed per Year by Filing Method for Texas RE, 2009-2013



	2009	2010	2011	2012	2013
ACP			26		
FFT			37	72	126
NOP	17	15	41	6	52
SNOP			17	57	22

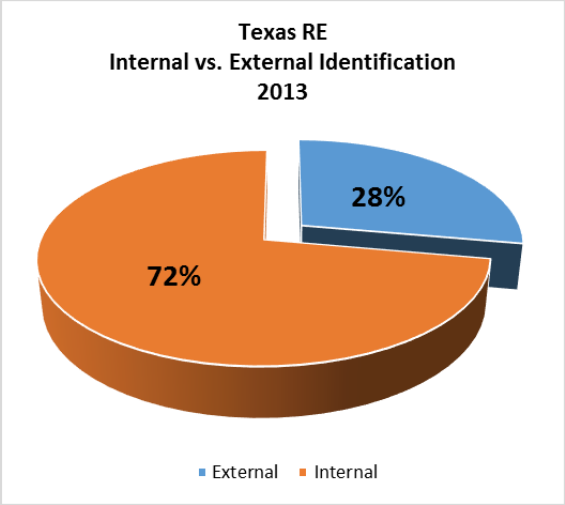
Texas RE reviews posted FFT and SNOP filings before determining the disposition method it will use for a particular violation, and it coordinates all FFT and SNOP-related issues with NERC. These methods help ensure the consistent application of FFTs and SNOPs across the Regional Entities. In 2011 and in every year since, Texas RE filed the majority of its violations using the streamlined enforcement processing mechanisms, including using FFT to file lower-risk violations of the CIP Reliability Standards. NERC expects that Texas RE will continue to reserve the NOP format for violations that require it and take advantage of further process refinements available under RAI. Additional information regarding Texas RE's application of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, violations discovered by registered entities through internal mechanisms comprised 72% of total violations in the Texas RE region. This is consistent with the ERO Enterprise average of 73%.

Percentage of Violations by Method of Identification for Texas RE in 2013



ii. Ensuring the Timely Mitigation of Violations

During the assessment period, Texas RE reported that it implemented a number of measures to ensure the timely mitigation of violations. Texas RE stressed the importance of prompt mitigation in workshops and other communications with registered entities and encouraged early completion of mitigation. Texas RE modified its self-report form to require a description of mitigating activities, preventative measures, and a date of mitigation. As a result of this modification, Texas RE began receiving more information regarding mitigation earlier in the enforcement process. Texas RE has also strengthened processes and documentation standards for the review, approval, tracking, and certification of mitigation plans. When reviewing a mitigation plan, Texas RE determines if the completion date is reasonable, considering the nature of the violation. Texas RE has requested that mitigation plans be revised because Texas RE determined that the completion date was unreasonable. Texas RE tracks the mitigation plan or mitigation activities completion date and has informed registered entities that violations cannot be closed until the mitigation is complete. Texas RE also tracks mitigation plan milestones in webCDMS and provides notifications to registered entities for upcoming milestones. In an effort to hold registered entities accountable, Texas RE will only discuss settlement and suspend deadlines if the entity submits a mitigation plan, or Texas RE has verified that the entity has mitigated the violation.

As demonstrated in the table below, Texas RE has made substantial progress in ensuring that older violations have completed mitigation. Only three violations from 2010 through 2011 remained to be mitigated at the end of the assessment period.

Texas RE: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[135]

Year of Discovery	% Completed	% in Progress
2013	28.1%	71.9%
2012	91.2%	8.8%
2011	99.4%	0.6%
2010	98.1%	1.9%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**82.5%**	**17.5%**

NERC will continue to work closely with Texas RE to ensure the completion of mitigating activities.

iii. Promoting Reliability through Enforcement Philosophy and Practices

Texas RE's enforcement philosophy is to abide by the requirements of the NERC ROP, reserve the enforcement process for those violations posing a serious or substantial risk to the reliability of the BPS, and encourage the development of strong internal compliance programs and internal controls. As part of encouraging strong internal controls, Texas RE encourages registered entities to address the results of internal controls by self-reporting and mitigating violations promptly. Texas RE may consider the method of discovery, presence of internal compliance programs, and the prompt mitigation of violations among the factors in determining how to dispose of a violation (i.e., FFT, SNOP, or NOP) and in assessing potential penalties.

In its settlement processes, Texas RE has worked with registered entities, where appropriate, to accept the completion of certain activities above-and-beyond those required to ensure compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

As examples of above-and-beyond activities, registered entities in the Texas RE region have committed to hire additional compliance staff, install new software to track maintenance and testing intervals, contribute to future compliance efforts (such as making an entity's SME available for a compliance workshop), develop additional training for staff, perform additional technical modifications beyond those required to achieve compliance, and upgrade physical security measures. NERC encourages Texas RE to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

[135] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations.

d. Texas RE's Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity executes its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to Texas RE.

Texas RE calculates penalties using the NERC *Sanction Guidelines* and reviews its determinations in relation to similar penalties assessed by Texas RE and by other Regional Entities. NERC reviews all penalties submitted by Texas RE for appropriateness and consistency with monetary penalties assessed by Texas RE and other Regional Entities for violations of the same Reliability Standards and requirements occurring under similar facts and circumstances. NERC has found that Texas RE assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that Texas RE dismisses violations for appropriate reasons and generally includes the required information when issuing letters of dismissal. NERC identified opportunities for Texas RE to improve its letters of dismissal and communicated those opportunities to Texas RE. By implementing the recommended improvements, Texas RE can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of Texas RE FFT issues filed or posted during the assessment period to examine Texas RE's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that Texas RE maintains adequate documentation and written procedures for its FFT process. NERC noted that Texas RE developed a process checklist which could prove to be a useful tool for FFT processing, provided the checklist is completed on a consistent basis. NERC further concluded that Texas RE generally provides an adequate description of the issue in its FFT postings. NERC noted several ways that Texas RE could improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that Texas RE has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. Texas RE should adopt the recommendations for improvement provided as part of NERC's oversight activities.

9. Evaluation of Western Electricity Coordinating Council

a. Overview

In the three-year performance assessment, NERC concluded that WECC was one of the less effective Regional Entities in carrying out its compliance obligations, but noted that WECC was starting to make significant strides in reducing the portion of violations described as its "backlog" in the first half of 2009. NERC encouraged WECC to create a stronger separation of its compliance encouragement efforts from its enforcement activities and to maintain its focus on processing violations to completion.[136]

During the assessment period, WECC has taken several steps to address the concerns identified by NERC in the three-year performance assessment. WECC reported that it has enhanced, streamlined, and documented all of its enforcement processes with the assistance of dedicated enforcement SMEs. Further, WECC has implemented the alternative enforcement processing mechanisms. WECC calculated its processing time (from intake through submittal to NERC) to be less than five months, on average. WECC also has enhanced its compliance encouragement activities while maintaining separation from its enforcement activities.[137]

During the assessment period, WECC increased the number of FTE staff dedicated to enforcement processing from 6 in 2009 to 8 as of December 31, 2013.[138] Based on WECC's processing speed and efficiency as measured at the end of the assessment period, NERC views WECC's enforcement processing staffing to be sufficient to process the number of violations that it receives.

WECC ended the assessment period with a better-than-average Caseload Index. In addition, WECC made substantial progress in processing the especially large number of violations that it received during the assessment period, including processing almost all of its older caseload. NERC notes that WECC has a few older violations that still need to be mitigated and processed. In addition, NERC has reviewed WECC's enforcement-related processes as part of its oversight role and found that, while areas for improvement remain, WECC generally implements those processes in a satisfactory manner.

NERC recognizes the contributions WECC staff have made in the development of RAI. WECC staff participated in the Enforcement Discretion pilot program and served in leadership roles on the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide* drafting teams. This participation is vital as the ERO Enterprise shifts toward a risk-based model of compliance and enforcement.

In light of all of the relevant factors, which are explained more fully below, NERC concludes that WECC has performed as an effective Regional Entity with respect to enforcement

---

[136] *Three-Year ERO Performance Assessment Report*, Attachment 3 at 26.

[137] 2014 JRESA Appendix 2B at 6-7.

[138] WECC has additional staff dedicated to reviewing violations from a technical perspective and reviewing and approving mitigation plans.

activities during the assessment period. NERC will continue to work with WECC to ensure that violations are mitigated and processed promptly.

b. Evaluation of Caseload Processing Efficiency

i. The Composition of WECC's Caseload

During the assessment period, WECC reported 3,183 violations[139] to NERC.

Violations for WECC 2009-2013 by Year Reported to NERC[140]

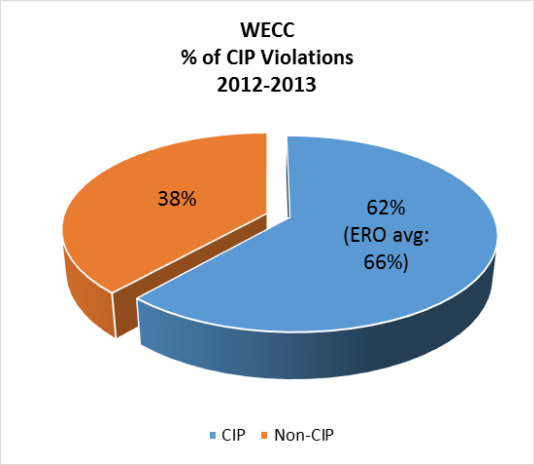
Year Reported to NERC	Violations Reported
2009	571
2010	550
2011	807
2012	818
2013	437
Total	**3,183**

As shown in the table above, WECC reported the most violations to NERC in 2011 and 2012. CIP violations comprised more than half of total violations in 2011 through 2012. In the years 2012 and 2013, violations of CIP Reliability Standards represented a slightly lower percentage of total violations in the WECC region (62%) than the ERO Enterprise as a whole.

[139] This table reflects U.S. violations only.

[140] For an explanation of the methodology used to calculate the data in this table and throughout this §II.D, *see supra* n. 76.

Type of Violations Reported to NERC by WECC, 2012-2013

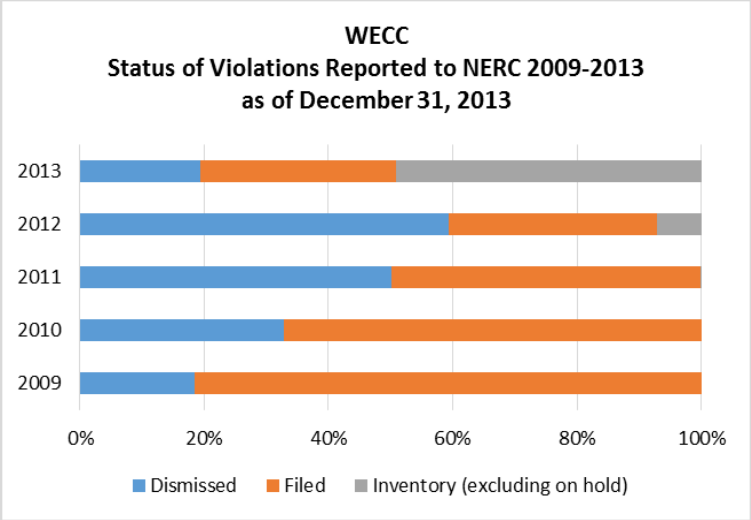


More than 85% of the total number of CIP violations reported by WECC to NERC in 2012 and 2013 were identified through internal means; nearly half of these CIP violations were later dismissed.[141]

Of the total violations reported by WECC to NERC during the assessment period, approximately 254 violations, or approximately 9%, remained to be processed as of December 31, 2013 (excluding violations that are held by appeal, a court, or a regulator). As demonstrated in the table below, WECC has processed 100% of violations reported to NERC in 2009 and 2010 and 99.9% of violations reported to NERC in 2011 (excluding on hold violations). WECC has processed approximately 93% of violations reported to NERC in 2012.

[141] WECC had a larger number of dismissals than other Regional Entities during the assessment period as a result of duplicate self-reporting. In early 2012, WECC had a number of violations where an entity submitted both a self-report and a self-certification. Since that time, WECC implemented a process to check for duplicate violations. In addition, the NERC ROP were amended to add several enhancements to the preliminary screen process; part of this process requires Regional Entities to confirm that new violations are not duplicates of violations already in process.

Status of Violations Reported to NERC 2009-2013 for WECC



WECC processed nearly 51% of violations reported to NERC in 2013. This is notably higher than the ERO 2013 processing rate of 39%. Approximately 78% of the violations available for processing in the WECC region consist of violations reported to NERC in 2013. This is notably better the overall ERO Enterprise average of 67%. WECC appears to be moving toward a caseload consisting primarily of newer violations.

ii. Caseload Index

The Caseload Index for WECC is 5.7 months as of December 31, 2013. This compares favorably to the ERO Enterprise Caseload Index of approximately 6.5 months.

Based on its achievements in processing its caseload to date and its Caseload Index, it appears that WECC's efforts to enhance and streamline its enforcement processes have been effective.

iii. Efforts to Reduce Older Caseload

In 2013, WECC processed 98% of remaining cases in its pre-2012 caseload. NERC commends WECC for its responsiveness and efforts to achieve this important ERO Enterprise goal.

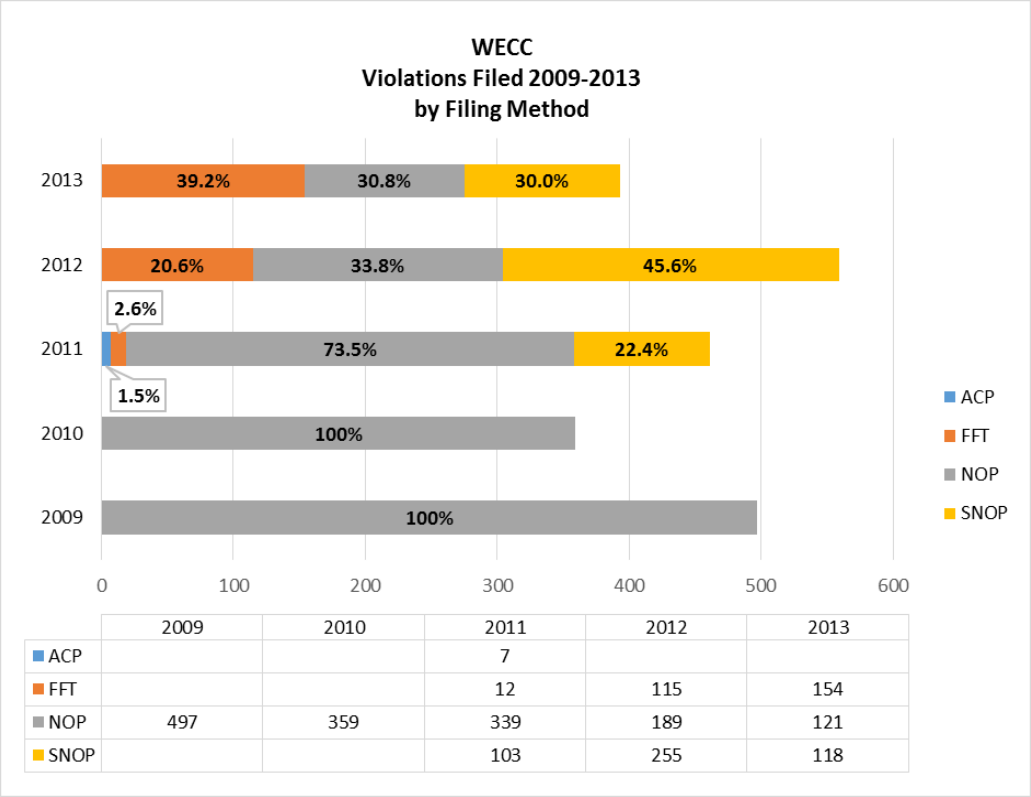
Based on the current composition of its inventory of violations to be processed and its successful effort in processing its older violations, WECC is well-positioned to achieve the goal of ensuring that violations are processed before reaching 24 months in age.

iv. Implementation of Streamlined Enforcement Processing Mechanisms

A number of factors are responsible for WECC's successes in processing its caseload. As

demonstrated in the table below, WECC effectively used streamlined processing mechanisms to process a substantial portion of its caseload during the assessment period. WECC did not implement streamlined processing mechanisms as quickly as some other Regional Entities, but by 2012, WECC was using the streamlined processing mechanisms to file nearly two-thirds of its violations.

Violations Filed per Year by Filing Method for WECC, 2009-2013



	2009	2010	2011	2012	2013
ACP			7		
FFT			12	115	154
NOP	497	359	339	189	121
SNOP			103	255	118

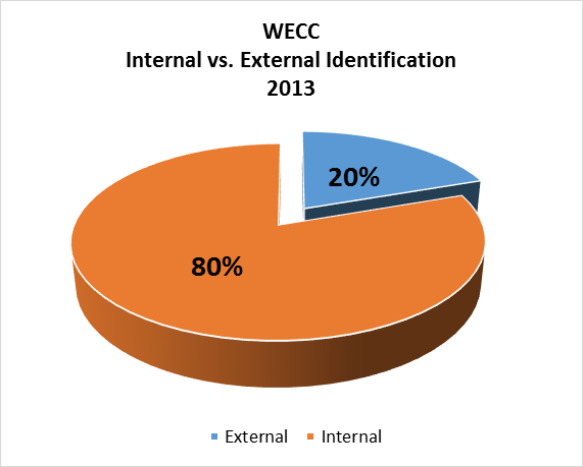
WECC has enhanced, streamlined, and documented all of its enforcement processes; WECC believes that these efforts will help ensure effective and consistent use of the enforcement processing mechanisms (including FFT and SNOP). NERC encourages WECC to continue its utilization of alternative enforcement processing mechanisms. Going forward, NERC expects that WECC will continue to use the NOP format for violations that require it and take advantage of further process refinements under RAI. Additional information regarding WECC's implementation of FFT is presented later in this assessment.

c. Improving Reliability

i. Encouraging Internal Discovery of Violations

In 2013, self-identified violations comprised 80% of total violations in the WECC region. This is somewhat higher than the ERO Enterprise average of 73%.

Percentage of Violations by Method of Identification for WECC in 2013



ii. Ensuring the Timely Mitigation of Violations

During the assessment period, WECC increased relevant staffing, enhanced relevant processes and procedures, and strengthened metrics to help ensure timely mitigation plan and completed mitigation plan processing. These actions were taken to address certain concerns regarding WECC's mitigation plan processing that were identified in a 2010 FERC audit report.[142] Specifically, WECC created two SME teams, one to review mitigation plans associated with violations of the CIP Reliability Standards, and the other to review mitigation plans associated with Operations and Planning Reliability Standards. WECC also implemented several internal process improvements, including establishing a priority review process for mitigation plans associated with violations posing a high risk to reliability or otherwise requiring prompt attention. WECC now tracks its mitigation plan review efficiency through the use of an internally-developed metric.

WECC has strengthened its active monitoring of mitigation plans by increasing its communication with registered entities. These increased efforts began in 2013. WECC now issues email reminder notices to registered entities as due dates approach. WECC staff also continue to communicate with and give presentations to registered entities regarding best practices for submitting and managing information associated with self-reports, self-certifications, and mitigation plans. WECC now accepts mitigating activities in lieu of a formal mitigation plan for a limited number of cases.

As demonstrated in the table below, WECC has made substantial progress in ensuring that violations from 2007 through 2009 have been mitigated. Only about 11 violations from 2010 and 2011 remained to be mitigated by the end of the assessment period.

[142] *See Order Approving Audit Report, Determining Issue of Separation of Functions, and Directing Compliance and Other Corrective Actions*, 132 FERC ¶ 61,149 (Aug. 10, 2010) at Appendix A.

WECC: Status of Mitigating Activity for Violations Discovered from 2007-2013 and Requiring Mitigation as of December 31, 2013[143]

Year of Discovery	% Completed	% in Progress
2013	56.6%	43.4%
2012	92.0%	8.0%
2011	98.5%	1.5%
2010	98.7%	1.3%
2009	100.0%	0.0%
2008	100.0%	0.0%
2007	100.0%	0.0%
Grand Total	**93.2%**	**6.8%**

WECC has made progress in ensuring that newer violations have been mitigated, with over half of violations discovered in 2013 having completed mitigation by the end of the year. NERC will continue to work with WECC to ensure that all violations are mitigated in a timely manner.

iii. Promoting Reliability through Enforcement Philosophy and Practices

WECC's enforcement philosophy is to use the enforcement process as a tool to influence and encourage desired behavior by registered entities. To that end, WECC Enforcement has adopted risk-based processes and projects that it believes will promote, foster, and influence a reliable BPS. WECC Enforcement seeks opportunities to work collaboratively with and educate registered entities in the enforcement space. WECC Enforcement also recognizes its obligation to ensure fair and reasonable outcomes.

WECC created a new violation assessment process to improve its ability to assess the impact and the root cause of violations, and to determine effective solutions to address the root causes. WECC calls this process a Violation Risk Assessment Methodology (vRAM). This framework is used to assist WECC Enforcement staff in determining the risk posed by a violation, as well as the level of resource allocation that must be dedicated to each violation. During a violation review, WECC Enforcement staff use a four-step process to assess the risk of each violation. This process consists of a severity analysis, controls analysis, likelihood analysis, and risk analysis. This new risk characterization allows a more granular reflection of the risk. In addition, this process considers an entity's connectivity, internal controls, and functions when determining the severity of a violation. WECC believes that this process helps WECC process lesser-risk violations more quickly than in the past.

In its settlement processes, WECC has worked with registered entities, where appropriate, to agree to the future completion of certain activities above-and-beyond those required to ensure

[143] This table reports the percentage of violations discovered from the years 2007 through 2013 with completed or open mitigation. This table excludes dismissed violations and non-U.S. violations.

compliance with one or more Reliability Standards in lieu of the full monetary penalties permitted by the NERC *Sanction Guidelines*. These efforts allow registered entities to allocate their resources to those projects that can increase overall reliability and reduce the likelihood of future noncompliance.

As an example of above-and-beyond activities, registered entities in the WECC region have committed to implement improvements to enhance their ability to comply with Reliability Standards. Examples of compliance-related improvements included developing a process to mitigate violations in a timely manner, implementing meetings and programs to increase awareness of compliance issues, and developing processes to identify the full scope of violations promptly. NERC encourages WECC to continue deploying solutions such as these that promote reliability and insight into processes that can manage risk.

d. WECC's Implementation of Various Aspects of the CMEP

As noted in §II.D.1.a above, NERC conducts ongoing oversight activities to evaluate the effectiveness of each Regional Entity's implementation of the CMEP. These activities include regular reviews and periodic spot checks of specific Regional Entity processes. NERC's oversight activities give NERC an ongoing view into how effectively and efficiently the Regional Entity is executing its enforcement responsibilities. Below is a summary of some of NERC's more recent oversight activities specific to WECC.

With respect to the assessment of monetary penalties, WECC tracks and reviews penalty information to ensure that penalties are applied consistently. Responsibility for penalty tracking analysis lies with WECC's compliance enforcement case management team, which works with WECC management to determine appropriate penalties. NERC reviews all penalties submitted by WECC for appropriateness and consistency with monetary penalties assessed by WECC and other Regional Entities for violations of the same Reliability Standards and requirements occurring under similar facts and circumstances. NERC has found that WECC assesses monetary penalties that are appropriate and consistent with penalties assessed for similar violations.

Based on a spot check, NERC determined that WECC dismisses violations for appropriate reasons. NERC identified opportunities where WECC could improve its letters of dismissal and communicated those opportunities to WECC. By implementing these improvements, WECC can improve the quality of its compliance guidance to registered entities.

As part of its ongoing FFT review processes, NERC reviewed a sample of WECC FFT issues filed or posted during the assessment period to examine WECC's procedures for FFT processing and the application of those procedures to the FFT issues in its caseload. Following its review, NERC concluded that WECC's procedures generally followed FFT requirements and guidance. NERC noted that WECC's Notice of FFT Treatment was very useful and included details on the factors WECC considers, such as the description of the issue, risk statement, and mitigating activities, when considering whether to afford FFT treatment. The WECC sample set contained several instructive examples where the risk statement adequately addressed the issue and the minimal risk to the reliability of the BPS. NERC noted several ways that WECC could

improve its FFT postings and related documentation to provide additional transparency to its determinations.

e. Conclusion

Based on NERC's review of the factors described above, NERC concludes that WECC has performed as an effective Regional Entity with respect to enforcement activities during the assessment period. WECC should adopt the recommendations for improvement provided through NERC's ongoing oversight activities.

III. RELIABILITY ASSESSMENTS

A. Overview of Regional Entity Responsibilities

One of the ERO's responsibilities, as set forth in §215(g) of the FPA, 16 U.S.C. §824o(g), and 18 C.F.R. §39.11, is to conduct periodic assessments of the reliability and adequacy of the BPS in North America.[144] These assessments are conducted by the NERC Reliability Assessment and Performance Analysis (RAPA) department. Pursuant to the RDAs, the Regional Entities help to assess reliability and to provide performance assessment and event analysis of the BPS in their footprints.[145] Section 804 of the NERC ROP specifies that the Regional Entities are to provide data and information to support NERC's annual long-term and seasonal assessments of the reliability of the BPS and any special reliability assessments. In addition, the Regional Entities are to conduct self-assessments of resource adequacy and transmission constraints within their footprints.

Throughout the assessment period, the Regional Entities have supported the RAPA program area by providing Regional Entity-specific data and information for the development of NERC's seasonal, long-term, probabilistic and special reliability assessments. These continent-wide assessments are developed annually by NERC through ongoing coordination between the RAPA department and the NERC Reliability Assessment Subcommittee (RAS), a subcommittee of the NERC Planning Committee (PC).[146] The assessments are primarily based on information and data submitted by a variety of registered entities within the Regional Entities.[147] Data includes

[144] Section 39.11(b) of the U.S. FERC's regulations provide that: "The Electric Reliability Organization shall conduct assessments of the adequacy of the Bulk-Power System in North America and report its findings to the Commission, the Secretary of Energy, each Regional Entity, and each Regional Advisory Body annually or more frequently if so ordered by the Commission."

[145] Assessment of the Regional Entities' performance in the event analysis function is provided in §IV on Reliability Risk Management, below. This §III is focused on the reliability assessment function.

[146] Information on the Reliability Assessment Subcommittee can be found at: http://www.nerc.com/comm/PC/Pages/Reliability-Assessment-Subcommittee-(RAS)-2013.aspx.

[147] Prior to 2011, data was collected and presented based on the political boundaries of each Regional Entity. Following approval by the NERC PC, assessment areas were introduced in 2011. These assessment areas were based on planning coordinator boundaries (or groups of planning coordinators), which more accurately reflect the planning and operational activities of the BPS. The eight Regional Entities are still responsible for providing reliability assessment data to NERC, but data is collected on an assessment area basis.

peak load (demand) forecasts, projected availability of capacity and demand-side management (DSM) resources, and existing and future transmission.[148]

The Regional Entities provide technical input to support the objectives of the RAPA department through the following ERO committees, subcommittees, and working groups:

- PC: The PC is a stakeholder committee chartered by the NERC Board to proactively support the ERO Enterprise mission[149] and associated NERC program areas by carrying out a broad array of technical activities and responsibilities focused on the reliable planning and assessment of the interconnected BPS of North America. The PC's mission is to promote the reliability of the interconnected BPS in North America and to assess and encourage resource and transmission adequacy. The PC also provides a forum where industry representatives and subject matter experts can address reliability, planning and adequacy issues. The PC supports NERC's reliability mission by executing the policies, directives, and assignments from the NERC Board and by advising the NERC Board on matters related to bulk electric system transmission planning, reliability, and resource adequacy.

- RAS: The RAS reviews, assesses, and reports on the overall reliability (adequacy and security) of existing and planned BPS. Six meetings are held annually to support the peer review and information verification necessary for the development of seasonal, long-term, and probabilistic (biennial) assessments. These peer reviews ensure that each assessment area conforms to its own planning criteria, guides and the applicable NERC Reliability Standards. The RAS reports directly to the NERC PC.

- Performance Analysis Subcommittee (PAS): The PAS provides input to and supports the objectives of the NERC RAPA department. The PAS reviews, assesses, and reports on the state of reliability based on historical performance of BPS. The key findings and recommendations of the PAS serve as technical input to NERC's Reliability Standards and project prioritization, compliance process improvements, reliability assessments, event analysis, and CIP, and ultimately support the *State of Reliability* report.

- Reliability Assessment Data Working Group (RADWG): The RADWG (formerly known as the Data Coordination Working Group), operates at the direction of the RAS. The primary function of the RADWG is to facilitate existing data collection

[148] Additional information about the assessment development process is provided in *NERC Reliability Assessment Guidebook*, version 3.1 (NERC Guidebook), available at: http://www.nerc.com/pa/RAPA/rg/ReliabilityGuidelines/Reliability_Assess_Guidebook_3_1Final.pdf.

[149] The ERO's mission is to ensure the reliability of the North American BPS. NERC achieves this mission by facilitating: industry awareness and management of risks to reliability; developing clear, reliability-focused standards; providing reliability assurance and excellence; assessing reliability performance; identifying and improving reliability models; and providing firm and fair enforcement of compliance with mandatory Reliability Standards.

efforts of the Regional Entities for NERC's seasonal and long-term reliability assessments. Additionally, this working group provides a platform for collaborative enhancements of current data collection processes to improve the accuracy, consistency, transparency, and efficiency of NERC's reliability assessment processes. Finally, the RADWG collaborates with the Department of Energy Energy Information Administration and other governmental/regulatory agencies that conduct similar data collection efforts. The goal of the RADWG is to reduce duplicative reporting requirements while promoting consistent data definitions.

B. Regional Entity Responsibilities in the Preparation of Assessment Reports

NERC annually prepares two seasonal (summer and winter), one long-term (10-year), and one probabilistic (biennial) assessment under the direction of NERC's PC and with support from the RAS. To support these assessments, each Regional Entity conducts reliability assessments for its footprint (assessment area, as described above) in accordance with guidelines provided in the NERC Guidebook. The NERC Guidebook is a "living document" which aims to improve consistency and transparency, to enhance granularity, and to establish a core framework for conducting independent assessments. While inherent differences in the way that the BPS is planned and operated across North America result in different approaches in conducting reliability assessments, NERC maintains a consistent framework for how the BPS is assessed in different areas. This framework includes a common set of definitions and measures for demand, resources, transfers, transmission, and resource adequacy.

Ongoing coordination between NERC and the Regional Entities occurs throughout the assessment development process. This is accomplished through monthly calls with each Regional Entity to identify Regional Entity-specific challenges in the collection of assessment data and information.

1. Reliability Assessment Data Collection

NERC collects seasonal and long-term electricity supply and demand data for the assessments areas through the Regional Entities. The data is collected through a series of forms that are developed and distributed by the RAPA department, in coordination with the RAS and RADWG. Specific seasonal and long-term data collected for the reliability assessments include: (i) peak load (demand) forecasts; (ii) on-peak capacity (including DSM); and (iii) transmission facilities. Although these metrics have been collected by NERC since 1968, the level of detail for each metric has grown, especially during the last decade. The data collection activities for each assessment require ongoing coordination between NERC and the Regional Entities. This coordination is executed through the RADWG and RAS to ensure that the data are accurate and consistently reported at the assessment area level.

The underlying data collection processes and planning methods also vary by assessment area or Regional Entity. These variances exist due to the inherent complexity, different corporate structures and unique history of the industry. More importantly, different attributes within each assessment area (e.g., climate, resource mix, market structures) require Regional Entity-specific or assessment area-specific planning considerations. These issues are identified and addressed

through the RAS and RADWG. More recently, in 2012, NERC's RAPA department instituted the development of individual Methods and Assumptions reports[150] for the long-term, seasonal, and probabilistic assessments. These reports, updated annually, provide detailed documentation of the planning activities and special considerations applicable to each assessment area or Regional Entity and ensure consistency across all Regional Entities.

2. Reliability Assessment Narratives

NERC's seasonal, long-term reliability, and probabilistic assessments include information from each assessment area (or Regional Entity if prior to 2011). Similar to the data collection process (described above), the NERC RAPA department coordinates the collection of assessment information through the RAS. Specifically, narrative guides (or questionnaires) are developed annually, with RAS input, to assess future resource adequacy and identify potential NERC-wide or Regional Entity-specific reliability issues. Narrative guides for the seasonal, long-term, and probalistic assessments are distributed to each Regional Entity several months prior to the data submittal due date to NERC.

The assessment areas submit their self-assessments (in response to the narrative guides) to NERC through the Regional Entities. Each Regional Entity's self-assessment is then distributed to RAS members from other Regional Entities for an in-depth and comprehensive review of the data and information. Peer reviewer comments are discussed with Regional Entity and assessment area representatives, and refinements and adjustments are made, as needed. The Regional Entity self-assessments are then subjected to scrutiny and review by the entire RAS. This peer review process provides an essential check and balance to ensure the validity of the information provided for each assessment. It also provides a mechanism for the members of the RAS to become fully convinced that each Regional self-assessment is accurate, thorough, and complete. Regional Entity representatives are able to examine and better understand planning methods and assumptions in other Regional Entities while also critiquing these processes or identifying potential gaps or shortfalls. Finally, the peer review also ensures consistency of methods and assumptions so that reliability evaluations are uniform.

Following the peer review process, the NERC RAPA compiles all Regional self-assessments into a single draft report, which is reviewed by the NERC Operating Committee (OC), the Member Representatives Committee (MRC), and NERC senior management. The report ultimately requires NERC PC approval before it is submitted to the NERC Board for final approval. This comprehensive vetting process promotes the development of independent assessments with heavy coordination among Regional Entity stakeholders.

C. Regional Entity Responsibilities in the Preparation of *State of Reliability* Reports

NERC annually produces a *State of Reliability* report that provides NERC's independent view of ongoing BPS trends to objectively present an integrated view of reliability performance. The key findings and recommendations serve as technical input to NERC's processes for risk assessment, Reliability Standards projects prioritization, compliance process improvements, event

[150] Methods and Assumptions reports are available at: http://www.nerc.com/pa/RAPA/ra/Pages/default.aspx.

analysis, and CIP activities. The analysis of BPS performance developed as part of the report provides an industry reference of historical reliability, offers analytical insights regarding industry action, and enables the identification and prioritization of specific steps that can be taken to manage risks to reliability. The data that are analyzed to produce the *State of Reliability* report are submitted by entities across North America. Each Regional Entity is responsible for reviewing the data submitted by entities in its respective region for completeness and accuracy. Once this review is complete, the Regional Entity staff informs NERC staff that the data are ready for analysis.

D. Regional Entity Responsibilities in the Collection of Data for NERC Reliability Databases

The NERC Board has approved mandatory data reporting concerning conventional generating units, transmission outages, and demand response availability. NERC collects this data using its Generating Availability Data System (GADS), Transmission Availability Data System (TADS), and Demand Response Availability Data System (DADS) databases. This unique series of databases is used to collect, record, and retrieve operating information tracking, reporting, analyzing, and improving the reliability performance of the BPS. Regional Entity staff work with NERC staff to ensure the data submitted by entities is timely, complete, and accurate.

E. Regional Entity Resources Budgeted for Reliability Assessment and Performance Analysis During the Assessment Period

During the assessment period, each Regional Entity increased its budgeted direct expenses and its budgeted FTE staffing for its RAPA program. The following table shows the amounts of direct expense budgeted by each Regional Entity for its RAPA program in its 2009 and 2014 business plans and budgets as filed with the Commission:[151]

Regional Entity	2009 Budget	2014 Budget	Percent Increase
FRCC	$918,744	$1,270,439	38.3%
MRO	$982,029	$1,329,480	35.4%
NPCC	$1,446,942	$1,888,972	30.5%
RFC	$985,605	$2,213,282	124.6%
SERC	$976,109	$1,398,882	43.3%
SPP RE	$432,558	$1,345,065	211.0%
Texas RE	$365,180	$1,055,983	189.2%
WECC	$2,742,063	$6,516,514	137.7%

The following table shows the direct FTE staffing budgeted by each Regional Entity for its RAPA program in its 2009 and 2014 business plan and budget as filed with the Commission:

[151] WECC amounts include spending to perform work under DOE grants.

Regional Entity	2009 Budget	2014 Budget	Percent Increase
FRCC	3.67	5.29	44.1%
MRO	4.75	6.49	36.6%
NPCC	3.90	5.83	49.5%
RFC	5.50	10.00	81.8%
SERC	4.50	7.60	68.9%
SPP RE	3.40	7.13	109.7%
Texas RE	2.20	4.75	115.9%
WECC	14.00	23.60	68.6%

F. Evaluation of Regional Entity Performance in Reliability Assessment Activities and Areas for Improvement

As the discussion in §§III.B, C, and D above makes clear, the quality of NERC's reliability assessments depends heavily on the collaborative efforts of the Regional Entities, working through the RAS. The ability of the NERC RAPA staff to identify NERC-wide highlights and key findings is heavily dependent on the submittal of on-time, complete, and accurate data and information from each assessment area and Regional Entity.

NERC has assessed the performance of the Regional Entities during the assessment period against the following criteria pertaining to the Regional Entities' roles and responsibilities:

(1) Regional Entities interface with registered entities to support and assure overall alignment with wide-area, ERO-formulated, reliability assessments and performance analyses, program design and structure, and to undertake support functions for wide-area studies and analyses and the development of specific region-centric assessments initiated by the Regional Entity to gather greater insight into a particular reliability issue.

(2) Regional Entities evaluate and provide seasonal, long-term reliability, and probabilistic assessments of the planning coordinator within their regions (assessment areas) including the data supporting the various analyses and evaluations of anticipated reliability conditions.

(3) Regional Entities compile interconnection-wide, steady-state and dynamic models of the registered entities within their regions that have been developed by the applicable planning coordinators consistent with the program design and structure.

(4) Regional Entities perform the data gathering function for certain performance analysis data efforts, assuring integrity, quality, and timeliness of the underlying data, and using data-gathering quality control procedures, forms and reporting mechanisms provided by NERC.

(5) Regional Entities provide technical resources and expertise in support of strategic plan initiatives, aligning budget and resource process proposals that maximize the efficiency and effectiveness of the overall ERO enterprise on technical, analyses, information technology and program approaches.

(6) Regional Entities manage their technical participation in applicable ERO committees and sub-groups in alignment with overall strategic objectives and the RAPA program structure and design while minimizing duplication and the overlap with SMEs and technical groups.

(7) Regional Entities coordinate with registered entities and provide technical resource support to wide-area analysis of technical issues (oscillations, frequency, modeling, system protection, BES, etc.) that involve joint efforts.

(8) Regional Entities support the development and implementation of major projects and initiatives (e.g., application of the BES definition), process exceptions requests, implement compliance, registration and standards applicability activities, and arrange Regional Entity processes for consistent use within North America.

(9) Regional Entities manage the relationship with registered entities with respect to RAPA program deliverables and objectives, including data and analytic assembly quality, integrity, and timeliness.

(10) Regional Entities collect misoperation data in fulfillment of obligations in PRC-004-2.1a, Requirement R3. The Regional Entities, in conjunction with their respective protection system subcommittees, analyze the data to determine trends and recommendation actions.

Based on its review of the Regional Entities' performance in Reliability Assessment during the assessment period, NERC makes the following observations:

(1) All Regional Entities conduct Reliability Assessments in general accordance with the NERC Guidebook.

(2) NERC supports and collaborates with Regional Entity staff through stakeholder committees to ensure consistent execution of delegated functions. In addition, the Regional Entities directly collaborate and communicate with registered entity personnel when conducting reliability assessments. Together, NERC and the Regional Entities have maintained a common framework for assessing the reliability of the BPS.

(3) Further improvements in data checking and validation processes are needed. Regional Entities are leading and participating in the development of the NERC Reliability Assessment Data System (RADS). While this automated data system is still under development, significant improvements to data collection and validation have already been made at the Regional Entity level to support RADS in 2015.

(4) Each Regional Entity reviews the data submitted by registered entities for completeness and accuracy in TADS, DADS, and GADS. Once the review is complete, the Regional Entity informs NERC that the data is ready for analysis. The Regional Entities have typically met these expectations.

(5) In the future, some Regional Entities may need more resources to support evolving assessment approaches. More granular reliability assessments, which are expected through the course of increased evaluations of high-priority emerging reliability issues, may require additional data and information. This is true particularly in response to a changing resource mix and an evolving electricity grid; different approaches for measuring and evaluating future reliability may be needed. Most reliability assessment data supports the measurement of resource adequacy. To support a comprehensive understanding of essential reliability services, NERC will be considering how other long-term reliability evaluations should occur and what data and information will be needed over the next several years. These efforts, along with further evaluation of environmental regulations, DSM, gas and electric interdependencies, increasing variable generation, and other emerging reliability issues, require strong support from the ERO.

(6) Some Regional Entities rely upon their member entities to perform various technical reviews. In order for Regional Entities to provide an independent review of both BPS performance and future states of reliability, Regional Entities may need increased staff participation. The need for independent review by regional staff will be greater over time given the challenges of the evolving BPS.

Based on its review, NERC makes the following recommendations for improvements:

(1) NERC and the Regional Entities should work collaboratively to develop an ERO enterprise-wide database solution to reinforce the existing structures and processes (including Regional Entity involvement) used to develop NERC assessments. An ERO-wide database solution would allow for consistent data error checking which would ultimately improve the overall efficiency across the ERO and contribute to better reliability assessments.

(2) NERC RAPA department management needs to further work on the best design for managing functional area relationships with the Regional Entities and developing better metrics to evaluate Regional Entity performance.

Going forward, NERC, in collaboration with the Regional Entities, will: (i) develop a comprehensive overarching design and set of controls, reporting requirements, metrics, and feedback mechanisms for reliability assessment activities, including the essential oversight elements listed above; (ii) identify functional qualifications for performance of reliability assessment activities; and (iii) adopt risk-based approaches to monitoring performance of delegated functions and providing effective feedback and coaching to continuously improve overall ERO Enterprise performance.

In conjunction with these improvement efforts, the Regional Entities should (1) continue to support NERC in the development of comprehensive functional program designs and controls (e.g., performance metrics and Regional Entity assessments based on common criteria); and (2) adapt existing Regional Entity programs for reliability assessment activities to conform with emerging program designs provided by NERC (e.g., ERO-enterprise wide data collection and database systems).

Many of the improvement activities described above have been initiated during the latter stages of the assessment period. In October 2013, the ERO Executive Management Group, comprised of senior management from NERC and each Regional Entity, approved a revised ERO-RAPA group charter. The purpose of the revised ERO-RAPA group charter is to provide a forum for Regional Entities and NERC RAPA department staff to collaborate on ongoing activities that are part of the RAPA department's approved roles and responsibility. This group will facilitate the flow of information, jointly coordinate work product expectations (scope, timing, resource expenditures, schedule, etc.) and promote consistency in the final products. The ERO-RAPA group includes a staff person from each of the eight Regional Entities (selected by the Regional Entity) to provide overall coordination of assessment activities with the NERC RAPA staff. Also, the ERO-RAPA group will implement, promote, and provide strategic and tactical guidance for Reliability Assessment activities per the ERO oversight model.

IV. RELIABILITY RISK MANAGEMENT (SITUATION AWARENESS AND EVENT ANALYSIS)

This §IV evaluates the Regional Entities' activities during the assessment period with respect to Reliability Risk Management (RRM). RRM encompasses the program areas of Situation Awareness and Event Analysis.

A. Regional Entity Progress in Identifying and Analyzing System Events and Improving Situation Awareness

Pursuant to the RDAs and the NERC ROPs, NERC and the Regional Entities collaborate to monitor present conditions on the BPS by gathering and assessing situation awareness information from registered entities.[152] The Regional Entities also assist NERC in analyzing major events, off-normal occurrences, BPS performance and BPS vulnerabilities.[153] NERC notes that as a general matter, the Regional Entities have not devoted, and have not been asked to devote, a level of resources to these activities comparable to the resources devoted to compliance monitoring and enforcement and reliability assessment. However, during the assessment period, the Regional Entities as a group made significant progress in executing these duties. The primary, collaborative achievement during this period was the formalization of a voluntary ERO Event Analysis process which facilitates coordinated responses to and review and analysis of system events. As part of the formalization of the Event Analysis process, an event classification system based on event severity was developed and put into effect. During the assessment period, NERC and the Regional Entities began using the event analysis process to analyze events and disseminate lessons learned to all industry members and to Regional Entities.

Prior to formalization of the Event Analysis process, which brought the ERO Event Analysis program to a mature state, the Regional Entities interacted individually with registered entities without a coordinated ERO-wide program for information sharing. In 2010, the Regional Entities initiated a dialogue with registered entities to discuss the requirements for preparing

[152] ROP §1001 (Situation Awareness). The Regional Entities' responsibilities with respect to event analysis and situation awareness are described in §7 of the RDAs.

[153] ROP §§807 (Analysis of Major Events) and 808 (Analysis of Off-Normal Occurences, Bulk Power System Performance, and Bulk Power System Vulnerabilities).

consistently formatted event reports. ReliabilityFirst, for example, developed a series of questions and a list of Reliability Standards that registered entities could use as a guideline as they developed event analysis reports and performed internal compliance reviews.

In June 2010, NERC and the Regional Entities created the NERC Event Analysis Working Group (EAWG), which included members from every Regional Entity. The EAWG expended significant efforts to develop an ERO Event Analysis process document in coordination with industry stakeholders for use across North America. On October 25, 2010, personnel from NERC, the Regional Entities, and the EAWG commenced a field trial of the ERO Event Analysis process, and conducted a comprehensive evaluation of the field trial data. Industry engagement in the field trials was noteworthy. Using the extensive feedback received from registered entities during the field trials, the EAWG developed version 1 of the *ERO Event Analysis Process*, which went into effect on February 21, 2012.[154] In June 2012, the NERC OC approved version 2 of the *ERO Event Analysis Process*, and the EAWG was transitioned to the NERC Event Analysis Subcommittee (EAS). By integrating industry engagement and the collaborative review of disturbances into the ERO Event Analysis process, the EAWG improved the effectiveness, predictability, consistency, and timeliness of the ERO Event Analysis program. The EAWG has since been elevated from a working group to a subcommittee under the NERC OC. Regional Entity staff continue to actively participate in the implementation and improvement of the ERO Event Analysis program. Since October 2010, registered entities have submitted more than 325 event reports through the ERO Event Analysis program. Several lessons learned have already been shared with the industry as a result of the ERO Event Analysis program.

The ERO Event Analysis program facilitates the sharing of lessons learned from applicable system events and trends. This sharing of lessons learned provides benefits to industry in terms of enhanced reliability. The new process provides a mechanism for registered entities to complete a preliminary event report for events occurring on their system. The higher the category of the system event (based on the event classification system), the more detailed analysis the registered entity is expected to perform and to share with the Regional Entity and NERC.

During the assessment period, a major test of the Regional Entities' progress in situation awareness and event analysis occurred in connection with the February 2011 Southwest Cold Weather Event, which affected areas of New Mexico, Arizona, and Texas and was the first major Category 4 Event to occur after the current ERO Event Analysis process was put in place. Approximately 1.3 million electric customers were out of service at the peak of this event. NERC, the Commission, and the Regional Entities whose areas were affected jointly analyzed the Southwest Cold Weather Event, conducted an assessment of previous severe winter events, published lessons learned, distributed training materials, and hosted an informational webinar to help industry members prepare for future severe cold weather events. As a result of the experience with this event, the ERO Event Analysis program was enhanced.

In addition to executing the Event Analysis process upon the occurrence of significant system events, the Regional Entities support NERC's situation awareness efforts by providing

[154] *See* the Event Analysis Program web page, available at: http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx.

more detailed information on occurrences of interest,[155] making initial notifications of certain Regional Entity-specific occurrences, and participating in daily situation awareness conference calls and weekly event analysis meetings. The Regional Entities also code all events and present them in monthly discussions with NERC.

NERC and the Regional Entities are continuously refining the ERO Event Analysis process based on experience and as system conditions change. For example, in 2013, NERC began focusing on energy management system (EMS) outages and their impact on BPS reliability. This focus on EMS outages has resulted in the publication and dissemination of two NERC Advisories pursuant to NERC ROP §810 as well as multiple lessons learned. NERC and the Regional Entities also conducted a monitoring and situation awareness workshop in September 2013 to share the lessons learned and the good industry practices learned from this work.

An added benefit of the ERO Event Analysis process is that it has driven a significant decrease in the initiation of formal compliance investigations by NERC and the Regional Entities. The responsiveness of registered entities in providing more extensive information about BPS disturbances has enabled NERC and the Regional Entities to perform more complete compliance assessments of these occurrences, without the use of a formal compliance monitoring method.

B. Hurricane Sandy Provided a Meaningful Case Study and Test of the ERO's Situation Awareness Capabilities

During the assessment period, in late October 2012, Hurricane Sandy provided a major test of the abilities of NERC, the Regional Entities, and the registered entities to engage in large-scale situation awareness and information sharing activities during a major system event. The hurricane made landfall on the Eastern Seaboard on October 29, 2012, and caused massive disruptions to the electric power system in New York, New England, and the Mid-Atlantic states. Over the course of the event, 20,007 MW of generation capacity was rendered unavailable and the distribution system was severely damaged. Approximately 8.35 million electric customer outages were reported across the impacted area.

In preparation for Hurricane Sandy, the Regional Entities and registered entities assisted NERC in monitoring conditions on the BPS and in responding to events as necessary. For example, ReliabilityFirst, NPCC, SERC, the New York Independent System Operator, ISO New England (ISO-NE), and PJM Interconnection, in conjunction with NERC's situation awareness team, coordinated storm preparation plans with the transmission owners, generation owners, balancing authorities, and other registered entities within the area forecasted to be impacted. Entities worked to ensure that sufficient numbers of additional field operation crews were scheduled and available to respond to the expected storm-related disruptions. Where possible, previously scheduled outages were postponed to ensure that facilities would be available over the next several days. Generators were advised of expectations during the storm, which included the potential for abnormal dispatch instructions. Blackstart units were also contacted to confirm that the units had sufficient fuel available to run for an extended duration.

[155] Many of these occurrences do not rise to the level of a reportable event within the ERO Event Analysis program.

A day before the hurricane made landfall, NPCC initiated a series of daily coordination conference calls. During these calls, the reliability coordinators in NPCC shared reported current and projected system status and operational challenges. These regional conference calls were an important means of monitoring and communicating events with adjacent reliability coordinators, and they continued daily throughout the storm and during the ensuing recovery efforts. In addition, gas pipelines were contacted and requested to advise ISO-NE of any special procedures or anticipated abnormal conditions in light of the impending storm. All gas pipelines implemented their hurricane preparedness plans for the Northeast region, which included checking on-site generators for compressor stations and reviewing staffing plans and facility flood plans.

Registered entities convened or participated in numerous conference calls and broadcasts. They also communicated with the mutual assistance groups to which they belonged. These calls began on October 27, 2012, and continued through the restoration effort, with some lasting though November 9, 2012. Following the storm, NPCC, ReliabilityFirst and SERC, whose footprints include the areas directly impacted by the storm, participated in a joint effort with NERC to provide an overview of the impact of Hurricane Sandy on the interconnected BPS and gather lessons learned for storm preparation and restoration. The results of this effort are included in the *Hurricane Sandy Event Analysis Report* published by NERC in April 2014.[156]

Other Regional Entities have had the opportunity to exercise their situation awareness and information sharing processes and to demonstrate their proficiency, but not at the level that was required during Hurricane Sandy. FRCC, SERC, and SPP RE demonstrated their situation awareness processes and proficiency during Hurricane Isaac in September, 2012. ReliabilityFirst demonstrated its situation awareness processes and proficiency during the Derecho storm response in June through July 2012. Finally, WECC demonstrated its situation awareness processes and proficiency during multiple wildfires that caused transmission system disturbances in the Spring of 2013. While all of these events were smaller in scale and impact than Hurricane Sandy, the general processes used by the Regional Entities were the same and in each instance they were successfully executed.

C. Areas for Future Improvement and Enhancements

The EAS of the NERC OC conducts an annual review of the ERO Event Analysis process. The OC receives comments from industry members on the ERO Event Analysis process and gives these comments full consideration during the annual review. Some commenters have suggested that communication and coordination between the parties involved in event analysis should be further enhanced. Examples of suggested improvements include increasing the timeliness, transparency and comprehensiveness of dissemination of information relating to event analysis and lessons learned, and streamlining the cause coding mechanism. In response, NERC is exploring the possibility of implementing enterprise information technology systems to provide efficiencies in event analysis and related reporting processes.

[156] Available at: http://www.nerc.com/pa/rrm/ea/Oct2012HurricanSandyEvntAnlyssRprtDL/Hurricane_Sandy_EAR_20140312_Final.pdf.

V. BUSINESS PLANNING AND BUDGETING, FINANCE AND ACCOUNTING

A. Provisions of Commission Orders, the RDAs and the ROP Concerning the Regional Entities' Business Plans and Budgets and Financial Accounting and Reporting

The Commission's regulations at 18 C.F.R. §39.4(b) require that the ERO's annual business plan and budget submission include "the entire annual budget for statutory and non-statutory activities for each Regional Entity, with supporting materials, including . . . each Regional Entity's complete business plan and organization chart, explaining . . . the proposed expenditure of funds collected in sufficient detail to justify the requested funding collection and budget expenditures . . . ." The regulation further specifies that the ERO's annual budget submission "shall include the line item budgets for the activities of each Regional Entity that are delegated or assigned to each Regional Entity pursuant to §39.8." Further, in Order No. 672, the Commission stated that "The ERO must determine, at a minimum, whether each Regional Entity's proposed budget is adequate to carry out the functions delegated to it." [157]

The RDAs specify that the Regional Entity and NERC shall develop, through a collaborative process, an annual business plan and budget, in accordance with the Commission's regulations and orders and NERC business planning and budgeting policies and instructions.[158] The Regional Entity's business plan and budget is to describe the activities necessary for, and provide a budget with adequate resources for, the Regional Entity to carry out its delegated activities under the RDA. The business plan and budget is also required to show the funding sources and amounts to fund the proposed budget, including, as applicable, assessments to end users, penalty monies and other sources of funds. The RDAs further provide that NERC is to provide the Regional Entity with the form or forms, and accompanying instructions, for submittal of the Regional Entity's business plan and budget. NERC and the Regional Entities are to develop an annual schedule for preparation of the business plan and budget, and each Regional Entity is to submit its proposed annual business plan and budget for carrying out its delegated authority functions and related activities in accordance with the schedule. These RDA provisions are also reflected in §§1103 and 1104 of the NERC ROP.

Additionally, the RDAs specify that NERC shall develop, in consultation with the Regional Entities, a reasonable and consistent system of accounts, with a level of detail and record keeping comparable to the Commission's Uniform System of Accounts and sufficient to allow the Commission to compare the Regional Entity's approved budget with actual results for the year.[159] The Regional Entity must follow NERC's prescribed system of accounts except where a departure is specifically allowed by NERC. Further, the RDAs require the Regional Entities to submit to NERC (i) unaudited quarterly interim financial statements, in a form provided by NERC, no later than 20 days after the end of each fiscal quarter, and (ii) audited annual financial statements,

---

[157] *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), at P 229.

[158] The RDA provisions described in this paragraph are generally found in §9 of each RDA.

[159] This provision is also specified in NERC ROP §1103.4 (NERC Budget Development).

including supporting materials, in a form provided by NERC, no later than May 1 of the following year.

The Commission has also required NERC and the Regional Entities to file annual comparisons of each entity's budget to actual results for the year. These reports (sometimes referred to as "true-up reports") are to be filed on or before May 30 of the following year. The Commission originally imposed this requirement in its order accepting the NERC and Regional Entity business plans and budgets for the year 2008,[160] and clarified the requirements for this filing in several subsequent orders. The filings are to provide a comparison of the NERC and Regional Entity budgets to actual costs incurred in the preceding year, "in sufficient detail and with sufficient explanations for the Commission to determine, by program area, the reasons for deviations from the budget and the impacts of those deviations."[161] In an order issued in June 2008, the Commission provided additional direction concerning the required contents of the Regional Entities' annual true-up reports:

> 37. To promote consistency and transparency, the Commission directs the use of certain practices and formats in future true-up filings. In particular, Regional Entities must provide a cover letter discussing major areas of actual cost-to-budget variances for all of the Regional Entity's statutory programs in the aggregate. Regional Entities should also follow NERC's template for the presentation of actual costs and budgeted costs on a program-by-program and line-item basis. Significant variances must be explained on a line-item basis with enough particularized information to clearly support each such variance. Regional Entities should refrain from using generic, program area summaries to support significant variances. The cause for each such variance should therefore be clear on its face. Further, each Regional Entity must provide an explanation of the allocation methods it used to allocate indirect costs to the direct statutory program or functional areas, as well as any allocation between any statutory and non-statutory activities.[162]

In addition, the Commission directed that in the annual true-up reports, NERC and the Regional Entities should justify any use of cash reserves as variances.[163]

B. Regional Entity Performance in Business Planning and Budgeting, Accounting, and True-Up Reporting

Throughout the assessment period, consistent with the provisions of the Commission's regulations and orders, the RDAs, and the ROP summarized above, NERC and the Regional Entities have collaboratively developed annual business plans and budgets for each year 2010 through 2014 which describe the activities and resources necessary to execute the Regional

[160] *North American Electric Reliability Corporation, Order Conditionally Accepting 2008 Business Plan and Budget of the North American Electric Reliability Corporation and Ordering Compliance Filings*, 121 FERC ¶ 61,057 (2007).

[161] *Id*. at P 23. In addition, any use of statutory funds for non-statutory activities is to be identified and an explanation provided as to how the statutory funds will be reimbursed. *Id*. at P 66.

[162] *North American Electric Reliability Corporation, Order Conditionally Accepting Compliance Filing*, 123 FERC ¶61,282 (2008), at P 37.

[163] *Id.* at P 38.

Entities' delegated authority functions and related activities. Overall, the Regional Entities have performed their responsibilities in the business planning and budgeting process in accordance with the requirements of the Commission's regulations and orders, the RDAs and the NERC ROPs. In a sense, the five-year evaluation of the Regional Entities' performance in business planning and budgeting, accounting and true-up reporting can be considered redundant because NERC and the Regional Entities engage in these activities on an annual basis (or more frequent basis for some aspects of financial reporting), which provides NERC with continuous opportunities to review each Regional Entity's performance of these functions and its compliance with procedures and requirements, and to identify and correct any deviations or deficiencies. Further, the Commission's annual review and acceptance of each Regional Entity's business plan and budget and true-up report provides an ultimate check on the Regional Entity's performance.

To provide ongoing, collaborative oversight of the business planning and budgeting and accounting and financial reporting processes, NERC and the Regional Entities have formed an ERO Finance Group comprised of representatives of NERC and each Regional Entity. The purpose of the group is to: (i) facilitate the coordination, preparation, review and approval by NERC and the Commission of the NERC and Regional Entity business plans and budgets consistent with the requirements of the NERC ROP, the RDAs, any specific requirements established by the NERC Finance and Audit Committee or Board, and applicable statutory, governmental and regulatory requirements; (ii) facilitate the coordination, preparation, review and filing of the NERC and Regional Entity business plans and budgets with Canadian and, to the extent applicable, other governmental and regulatory authorities consistent with applicable governmental and regulatory requirements; (iii) collaborate and support initiatives to improve the cost effectiveness and efficiency of NERC and Regional Entity operations; and (iv) provide general support to the NERC and Regional Entity executive leadership regarding such other finance and accounting matters as may from time to be deemed necessary.

Since NERC became the ERO, NERC and the Regional Entities have continuously striven for consistency and improved transparency and detail in the annual NERC and Regional Entity business plans and budgets. The ERO Enterprise business planning and budgeting processes matured significantly during the assessment period. During this period, the ERO Enterprise implemented numerous process improvements in the areas of business and resource planning, allocation and budgeting. In the development of the 2010 business plans and budgets, in particular, a number of significant improvements were adopted. NERC believes that in the preparation of the 2012 business plans and budgets, a mature, steady state was reached with respect to process, format and content. This steady state has been maintained in the development of the 2013 and 2014 business plans and budgets and the currently ongoing development of the 2015 business plans and budgets (which will be completed outside of the assessment period). A partial list of steps that have been taken to achieve consistency, transparency and appropriate levels of detail includes the following:

(1) Development, adoption and use of a common, consistent chart of accounts by all entities and the presentation of budget and financial information in accordance with the accounting system;

(2) Development and use of a consistent organization and format for the business plans and budgets and the annual true-up reports, including a common table of contents,

common and consistent information, and common and consistent format for tables and charts providing the Regional Entity's funding, budget, actual costs, and staffing information;

(3) Development and use of a common definition of administrative (indirect) costs and consistent methodologies for identifying budgeted and actual expenses as "direct" or "indirect" expenses;

(4) Development and use of a consistent methodology for allocating indirect expenses to the direct program budgets;

(5) Development and use of a consistent policy for capitalizing vs. expensing expenditures;

(6) Collaborative development, on an annual basis, of a set of detailed shared (common) business planning and budgeting assumptions to be used by NERC and each Regional Entity in preparing their individual business plans and budgets. In recent budget preparation cycles, these assumptions have been expanded from a one-year set of assumptions to a three-year set of assumptions;

(7) Development of a common set of budget metrics for each Regional Entity to present in the annual business plan and budget filings; and

(8) Introduction of a three-year budget forecast into NERC's and each Regional Entity's annual business plan and budget.

In addition, NERC and the Regional Entities jointly develop a three-year rolling *ERO Enterprise Strategic Plan* which includes goals, objectives and deliverables over the planning period and is used in the development of each entity's business plan and budget. The development and implementation of these common formats and methodologies has helped to continuously improve the efficiency of the business plan and budget preparation process and enabled NERC and Regional Entity financial and accounting staffs and senior management to devote greater attention to more substantive budget issues.

In accordance with the RDA provisions described earlier, NERC and the Regional Entities establish and publish, for each annual budget preparation cycle, a detailed schedule for preparation, review, and approval of the business plans and budgets. The annual business planning and budgeting process for a year typically begins late in the second preceding year or early in the preceding year. The schedule provides for posting of initial and revised drafts, and periods for receipt of stakeholder comments, leading up to the ultimate approval of the business plans and budgets by the NERC Board at its August meeting and filing of the business plans and budgets with the Commission by on or about August 23 as required by the Commission's regulation. In addition, each Regional Entity goes through a posting and stakeholder review and comment process for its membership and other interested parties prior to approval of its business plan and budget by its governing body for submission to NERC. In its business plan and budget filing with the Commission, NERC provides descriptions of each Regional Entity's internal process. Over the assessment period, NERC and the Regional Entities have significantly increased the

transparency of the business plan and budgeting process, by providing numerous opportunities for stakeholder input and feedback prior to Regional Entity board and NERC Board approval and submittal to the Commission.

NERC's oversight of the Regional Entities' business plan and budget preparation, leading up to approval of the Regional Entities' business plans and budgets, is generally focused on the following areas:

(1) An assessment of the adequacy of the Regional Entities' resources and activities being budgeted by the Regional Entity to perform delegated functions.

(2) A review of the alignment of the Regional Entity's goals, objectives and major activities to the *ERO Enterprise Strategic Plan*.

(3) A review of the quality and completeness of the financial information presented by the Regional Entities, including:

  (a) Conformance with the Commission's budget reporting requirements;

  (b) Separation of statutory and non-statutory activities;

  (c) Supporting detail for projections; and

  (d) Working capital and operating reserve budgets, projections, policies and controls.

(4) A review of the Regional Entities' efforts to improve efficiency and control costs.

Throughout the budget review process, where appropriate, NERC requests additional information and recommends changes. As needed, NERC and Regional Entity management and finance staffs convene meetings and conference calls to provide feedback and to refine their respective business plans and budgets. In addition to reviewing and providing feedback to the Regional Entities, NERC management considers other relevant information when reviewing the Regional Entity budgets, such as the findings and recommendations contained in the audits the Commission has conducted of NERC and the Regional Entities.

During the assessment period, the Regional Entities also performed in accordance with requirements with respect to financial reporting, including the preparation of the annual true-up reports. During the assessment period, NERC and the Regional Entities have significantly increased the transparency and content of quarterly and year-end actual-to-budget variance reporting to the Finance and Audit Committee of the NERC Board. In general, the Regional Entities have consistently submitted their unaudited quarterly financial reports on a timely basis as required by the RDAs. With respect to the annual true-up reports, NERC and the Regional Entities developed a common, consistent format for these reports complying with the Commission's directives. The format consists of: (i) a cover letter identifying major areas of actual cost to budget variance for each program and providing the other information specified by Commission orders (e.g., whether any statutory funds were used for non-statutory activities, the Regional Entity's use of cash reserves and change in its working capital position); (ii) tables comparing on a line-item basis actual to budgeted expenditures on a total statutory basis and (if the Regional Entity also has non-statutory activities) total company basis; and (iii) tables

comparing on a line-item basis actual to budgeted expenditures for each of the Regional Entity's direct statutory programs and its administrative (indirect) programs, with narrative explanations provided for line-item variances that exceed $10,000 and 10% of budget. In general, the Regional Entities have submitted their audited annual financial reports and their draft true-up reports to NERC on a timely basis to allow for NERC to review and provide any feedback and the reports to be filed with the Commission by the May 30 deadline. In addition, NERC and the Regional Entities have developed a set of administrative cost metrics to be presented to the Commission as part of the annual true-up report filing.

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 4

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

NERC CONSIDERATION OF INDUSTRY FEEDBACK

JULY 21, 2014

Attachment 4

This Attachment presents information from the stakeholder survey that the North American Electric Reliability Corporation (NERC) conducted in October 2013 for purposes of the *Five-Year Electric Reliability Organization (ERO) Performance Assessment Report*, and from stakeholder comments received on postings of drafts of the *Five-Year ERO Performance Assessment Report*. This Attachment includes tables summarizing key comments received from stakeholders and NERC's responses to those comments, including identifying where in the *Five-Year ERO Performance Assessment Report* the comment is addressed.

This Attachment also includes summary information on the responses to the questions posed in the stakeholder survey and the type and distribution of the respondents. The stakeholder survey requested comments on the following broad categories of the ERO Enterprise's activities:

(1) Reliability Standards

(2) Compliance Operations

(3) Enforcement

(4) Registration and Certification

(5) Reliability Assessment & Performance Analysis Metrics

(6) Training, Education, and Personnel Certification

(7) Event Analysis

(8) Critical Infrastructure Protection

(9) Stakeholder Communications, Public Relations, and IT

(10) Business Plan and Budget

(11) Independence and Stakeholder Input

Table 1: Stakeholder Comments Concerning NERC

In the following table, (i) the first column contains summaries of key stakeholder comments; and (ii) the second column lists a brief response to an individual comment and, where applicable, the specific location(s) where the comment is addressed within the *Five-Year ERO Performance Assessment Report*. The table is divided into sections that correspond to the broad categories of questions asked in the stakeholder survey.

Summary of Key Stakeholder Comments	Where Comment is Addressed[1]
Reliability Standards	
Improve articulation of the need for a new Reliability Standard before development.	II(A)(6)(a); II(A)(6)(b); II(A)(6)(d) In 2013, NERC spearheaded an "informal development" effort, which uses informal groups composed of industry subject matter experts to conduct early outreach to industry stakeholders prior to initiating formal development of new or revised Reliability Standards. This early outreach encourages stakeholder conversations to obtain inputs on the proposed Reliability Standards development project. This approach is positively affecting how standard drafting teams are conducting their work. The Reliability Issues Steering Committee (RISC) provides a framework for steering, developing, formalizing, and organizing recommendations to help NERC and the industry effectively focus their resources on the critical means to improve the reliability of the bulk power system (BPS). In some cases, this includes recommending reliability solutions other than the development of new or revised Reliability Standards and offering high-level stakeholder leadership engagement and input on issues that enter the Reliability Standards process. In other cases, the development of a new Reliability Standard or modification of an existing Reliability Standard may be the best way to address a particular issue.
Speed up the process for developing Reliability Standards.	II(A)(6) Projects that were initiated and completed after FERC's approval of the *Standard Processes Manual* (SPM) changes, effective June 26, 2013, have shown significant increases in efficiency while simultaneously improving quality. Implementing the revisions within other projects that were already in process has also resulted in improvements.

[1] Unless otherwise indicated, all references in this table are to the *Overview of NERC Activities and Accomplishments in the Five-Year Period*.

	The most significant improvement is the composite result of all the revisions – the amount of time required to develop a quality Reliability Standard. As reported in the *Analysis of NERC Standards Process Results, Fourth Quarter 2013* filing, the baseline for the time to revise an existing Reliability Standard was approximately 27 months and 40 months to develop a new Reliability Standard. The times to produce each of the eight standards development projects that began formal development after implementing the revised SPM were dramatically reduced. Six and one-half of the projects (GMD Phase 1, INT, Physical Security, MOD A, MOD B, PER, and one of the two standards in the VAR project (VAR-001)) completed formal development from posting the SAR to being adopted by the NERC Board of Trustees in less than seven months. The remaining Reliability Standard in the VAR project (VAR-002) and the MOD C project completed formal development in ten months.
Better articulate how prioritization is determined in the Reliability Standards development process.	II(A)(1)-(4); II(A)(6)(a)-(b) The *Reliability Standards Development Plan 2014-2016* (RSDP) prioritizes future Reliability Standards projects as high, medium, low, or pending technical committee input based on a series of inputs. Prioritization considerations were influenced by: (i) RISC areas of risk and category rankings; (ii) outstanding regulatory directives; (iii) regulatory deadlines; (iv) Paragraph 81 retirement candidates; (v) content and quality assessments by the Standards Independent Experts Review Panel (IERP); and (vi) additional considerations such as fill-in-the-blank status and five-year standards review assessment commitments. The RISC provides input into prioritizing Reliability Standards development activities by providing input to the RSDP in two ways: first, by considering whether the projects identified in the RSDP address areas of risk for the BPS; and second, by developing a priority rank for each of the projects. In reviewing the priority of each project, the RISC provides a mechanism for addressing any scheduling conflicts between projects through the development process. NERC will continue working with the RISC to develop risk profiles for the ERO, which will include high impact low frequency (HILF) issues. These profiles of the BPS will inform how the ERO prioritizes and ranks reliability risks. For high priority risks, NERC will develop project plans and business case assessments outlining initiatives to address those risks.

Provide greater clarity regarding the "Applicability" section of each Reliability Standard.	Where practical, the applicability of Reliability Standards is being targeted to entities meeting specific requirements. This effort narrows applicability to specifically identified entities within registered functions, thus focusing requirements to entities where the actions impact the reliability of the BPS. For example, in PER-005-2, rather than the Reliability Standard being applicable to all Transmission Owners, it is applicable to those Transmission Owners that have: *Personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System [(BES)] transmission Facilities in Real-time.* Additionally, the Reliability Standard narrows applicably from all Generator Owners to those Generator Owners that have: *Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.*
Clarify avenues to obtain information regarding the development history of Reliability Standards. Streamline and enhance communications regarding the development of Reliability Standards to be more useful to industry.	II(A)(7); II(A)(6)(a) The revision of the NERC public website that was implemented during the assessment period significantly increased the information available on this topic and improved the ease of accessing it. On the current website, all Reliability Standards are available to stakeholders on the "Standards" webpage (*see* "Program Areas & Departments"). The "US Enforcement Dates" link on the page offers listings for: (i) Reliability Standards that are currently enforceable in specific jurisdictions (i.e. in the U.S. and Canadian provinces); (ii) Reliability Standards pending regulatory approval; (iii) Reliability Standards approved by the NERC Board of Trustees and pending regulatory filing; and (iv) Reliability Standards no longer subject to enforcement. This page also includes information regarding the enforcement dates for Reliability Standards and, for standards pending enforcement, the NERC Board of Trustees adoption date and the date the standard was filed with FERC. Stakeholders can also locate

	historical information on the "US Enforcement Status/Functional Applicability" link, which offers information regarding when the NERC Board of Trustees adopted, filed or retired requirements. It also provides the date standards were filed with FERC, the effective date of the FERC order and the enforcement date of each requirement. Stakeholders may see all prior versions of standards on the "Reliability Standards" section of the webpage. A click on the "related information" for link for each standard will provide access to historical project development pages. In 2012, NERC launched an improved interface, the VRF matrix, to allow stakeholders to filter the complete set of Reliability Standards so that they could identify which Reliability Standards were applicable to their respective registered functions. Work is ongoing to improve the completeness and timeliness of the above information for non-U.S. jurisdictions (i.e., Canadian provinces or Mexico). Additionally, beginning in 2013, interested entities can track current Reliability Standards development projects in a publicly posted spreadsheet, the *Project Tracking Spreadsheet*, available on the left navigation tab of the NERC Standards home page. NERC updates this spreadsheet monthly. The spreadsheet also provides a link to the projects page, the deliverables, the number of Paragraph 81 requirements, the number of regulatory directives or guidance, the Project Management and Oversight Subcommittee (PMOS) liaison assigned to the project, the NERC Reliability Standards developer, and a month-by-month timeline. Also in 2013, NERC began posting the *Projected Standards Posting Schedule*, which provides the industry with an outlook of near term postings.
Provide greater transparency regarding the process for selecting standard drafting teams and the rationale for standard drafting team decision-making.	II(A)(6)(a) NERC has improved the composition of standard drafting teams by enhancing the selection process to identify, for each project, the necessary technical, writing, and project management expertise to form a balanced team that will foster improved effectiveness and enhanced efficiency. These changes were instituted as a result of the recommendations made by the Standards Process Improvement Group (SPIG) to modify the way NERC develops Reliability Standards, which resulted in revisions to the SPM. In these revisions, NERC memorialized the intent to revise the composition of standard drafting teams to ensure they are appropriately equipped to meet reliability objectives (e.g., by adding legal and compliance experts).

	Additionally, the NERC Standards Committee created a new subcommittee, the PMOS that acts as an industry and standard drafting team partner. The PMOS assigns a representative to each standard drafting team for the purpose of oversight. This oversight includes such actions as: (i) assisting the standard drafting team in understanding any stakeholder concerns; (ii) reaching out to stakeholders if they do not understand the actions being taken by the standard drafting team; (iii) being partners in reviewing the standards for quality; and (iv) assisting with advice on a range of topics from direction to posting schedules. This group has assisted standard drafting teams in avoiding or overcoming hurdles during the process. The revisions made to the SPM and other changes made to the standards development process, including strengthened partnerships, while still in their infancy, are showing great promise as improvements to the process, both in creating efficiency and improving quality. These improvements have allowed the ERO Enterprise to make significant progress towards achieving a body of steady-state Reliability Standards.
Provide a detailed explanation as to how the Standards improve reliability for the industry.	II(D)(1)-(2) This *Five-Year ERO Performance Assessment Report* shows that NERC is improving the performance of, and mitigating risks to, the BPS as measured by avoidable outages. Further, as detailed in NERC's *State of Reliability 2014* report, the number of BPS transmission-related events resulting in loss of firm load, other than events caused by factors external to the transmission system's actual performance (i.e., weather-initiated events), decreased from an average of ten per year over a ten-year period (2002 through 2011) to seven in 2013. The daily severity risk index value, a new metric created by NERC that measures risk impact or "stress" from events resulting in the loss of transmission, generation, and load, has been stable from 2008 to 2013. Including weather-initiated events, 2013 had no high-stress days, which is within the range of zero to seven days experienced during 2008 through 2013. The availability of the bulk transmission system continues to remain high with no statistically significant change from 2008 to 2013. This improved performance is due to a combination of activities led by the ERO Enterprise. NERC Reliability Standards are one component of these activities; they are designed to prevent events that are detrimental to the reliability of the BPS. As detailed in this *Five-Year ERO Performance Assessment Report*, during the

	assessment period, NERC's compliance monitoring and enforcement efforts have matured into a robust program that provides industry with more certainty on actions, outcomes, and reliability consequences. The actions taken to identify, correct, and prevent violations of Reliability Standards have promoted the reliability of the BPS. For example, the adoption and rigorous enforcement of NERC's transmission vegetation management Reliability Standard, which became mandatory and enforceable in 2007, has dramatically reduced the number of outages caused by vegetation growing into high voltage lines. From 2004 through 2008, there were 58 reported outages. By contrast, from 2009 through 2013, only six instances were reported. The RISC identifies new or emerging issues that could impact the reliability of the BPS, and various solutions for mitigating those issues are investigated. Those solutions may include the development of a Reliability Standard, a guideline, necessitate an alert, initiate training, or other potential solutions tailored to the issue. It is the combination and sequencing of these actions – identify risk, determine solutions (of which a standard may be one), monitor compliance or adherence to the solution, and monitor until issue is resolved – that improves the reliability of the BPS. NERC will continue working with the RISC to develop risk profiles for the BPS, which will include HILF issues. These risk profiles of the BPS will inform how the ERO prioritizes and ranks reliability risks. For high priority risks, NERC will develop project plans and business case assessments outlining initiatives to address those risks.
Consider equally or more effective tools than a Reliability Standard for emerging issues such as Geomagnetic Disturbances (GMD), new Critical Infrastructure Protection (CIP) threats such as coordinated physical attack, cold weather preparedness, etc.	NERC will continue working with the RISC to develop risk profiles for the BPS, which will include HILF issues. These profiles of the BPS will inform how the ERO Enterprise prioritizes and ranks reliability risks. For high priority risks, NERC will develop project plans and business case assessments outlining initiatives to address those risks. This will include evaluating whether the risk is most effectively and efficiently addressed through a new or revised Reliability Standard or through some other initiative. In response to direction from the NERC Board of Trustees in February 2013, NERC developed a Reliability Risk Management (RRM) process to create and execute plans for managing reliability risk and to integrate these plans with the business

	planning and budgeting process. The RRM process leverages several resources including the business acumen of the RISC.
Continue to integrate recommendations of the RISC into NERC's decision-making.	II(A)6)(b); II(D)(1) NERC will continue working with the RISC to develop risk profiles for the BPS. These profiles of the BPS will inform how the ERO Enterprise prioritizes and ranks reliability risks. For high priority risks, NERC will develop project plans and business case assessments outlining initiatives to address those risks. In response to direction from the NERC Board of Trustees in February 2013, NERC developed a RRM process to create and execute plans for managing reliability risk and to integrate these plans with the business planning and budgeting process. The RRM process leverages several resources including the business acumen of the RISC.
Consider alternatives such as the forum process, which engages asset owners, to address reliability issues.	II(A)(8)(e); III(D)(3) NERC has used and will continue to use the North American Transmission Forum (NATF) and North American Generator Forum (NAGF), where efficient and appropriate, to address reliability issues. For example, the response to FERC's directive to develop and submit a physical security Reliability Standard within 90 days offered an opportunity for NERC to use the forum process to solicit industry input. On April 1, 2014, NERC staff convened a technical conference to focus stakeholder discussion on developing a draft of CIP-014-1 – Physical Security, with the intent of assisting the standard drafting team to quickly develop and post a Reliability Standard for comment and ballot. The conference provided a forum for industry input on the concepts in the draft Reliability Standard, to include criteria for determining applicable entities, identification of critical facilities, evaluation of potential threats and vulnerabilities, development and implementation of physical security plans, and the proposed standard's implementation plan. NERC Compliance staff also provided an overview of the Reliability Standard Audit Worksheet (RSAW) approach. Additionally, NERC is collaborating with the NATF and the NAGF to further enhance the Event Analysis process and lessons learned dissemination in identifying risks to the BPS.
Compliance Operations	

Provide better oversight to ensure consistency in auditing practices.	II(C)(2)(a); Attachment 3 – (II)(B)[2] During the assessment period, the Regional Entities made meaningful progress in improving their compliance monitoring programs and their audit practices and procedures consistent with the requirements of the NERC Rules of Procedure (specifically, the *Compliance Monitoring and Enforcement Program* (CMEP), Appendix 4C) and the Regional Delegation Agreements. Overall, the Regional Entities worked diligently to plan and complete their scheduled compliance audits during the assessment period. NERC's oversight of the Regional Entity compliance programs shows that the Regional Entities are meeting the baseline requirements of the NERC Rules of Procedure and the Regional Delegation Agreements. However, NERC's oversight has also shown (as this comment suggests) that there continue to be varying compliance monitoring practices across the ERO Enterprise. NERC has three main objectives for the continued evolution of the compliance monitoring program. First, the Regional Entities are revising their existing practices to better align with risk using generally accepted audit practices. Second, NERC and the Regional Entities have developed a standardized *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, to ensure consistent conduct of audits across the ERO Enterprise. Third, NERC, in conjunction with the Regional Entities, have developed competency (qualifications) guidelines for compliance monitoring staff and are developing training to accompany the competency guidelines.
Provide greater clarity on the Reliability Assurance Initiative (RAI) to inform industry about what is expected.	II(C)(2) To foster dialogue and seek industry feedback on the various aspects of RAI, NERC hosted a series of workshops in 2013 that addressed important components of RAI including defining internal controls, conducting risk assessment, launching pilot programs, enhancing the Find, Fix, Track and Report (FFT) process, and improving self-reporting. NERC also included the Compliance and Certification Committee (CCC) in the development and review of RAI activities including the development of white papers on internal controls and other guidance.

[2] Attachment 3 to the *Five-Year ERO Performance Assessment Report* is titled *NERC Assessment of Regional Entity Delegated Functions*.

	Compliance-related activities under the RAI program will help achieve a risk-based approach for compliance monitoring by evaluating current compliance monitoring practices, identifying improvements, and addressing the consistent application of audit techniques and the use of uniform tools to carry out compliance monitoring activities. Similar to the RAI compliance monitoring effort, the enforcement element of RAI seeks to align the ERO Enterprise's enforcement processing activities with levels of risk to the reliability of the BPS. Achieving this alignment will promote efficiencies for both the ERO Enterprise and registered entities by eliminating undue regulatory burdens, streamlining documentation and filing requirements, and substantially improving the processing of noncompliance and related mitigating activities.
Improve communications regarding how registered entities are to demonstrate compliance by making them more substantive, timely, and useful to the industry.	II(C)(2); Attachment 3 – II(B)(1)-(2) In 2013, NERC and the Regional Entities began to develop and implement tools that will define techniques and methods to perform compliance monitoring in a consistent manner across the ERO Enterprise. The Regional Entities began using the first of these tools, the *Compliance Auditor Checklist*, in August 2013. In December 2013, NERC and the Regional Entities completed the first draft of a companion document for the *Compliance Auditor Checklist*, the *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*. NERC disseminated the manual and provided initial training to Regional Entity auditors during the first quarter of 2014. In the second quarter of 2014, the Regional Entities began to use the *ERO Enterprise Compliance Auditor Manual* and its related processes and procedures on a select number of audits. Throughout 2014, NERC and the Regional Entities will revise and expand the manual to address additional audit topics, reflect additional processes developed through RAI activities, and include lessons learned. NERC has made the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, available to industry. A second key RAI compliance activity, the Prototypes and Pilot program, focuses on the development and implementation of a formalized approach to risk assessments and testing of management controls. NERC and the Regional Entities initiated the first phase of the pilot program during 2013. This phase explored different approaches to applying risk-based auditing

	concepts (e.g., audit scoping, reliability risk assessments, and management controls review and testing). For 2014 and beyond, a team consisting of NERC, Regional Entity, and industry representatives as well as an independent audit consultant will evaluate the findings and determine the best audit approach to implement throughout the ERO Enterprise. In addition, NERC and the Regional Entities have consolidated the annual CMEP Implementation Plans into a single document with the goal of implementing certain risk-based compliance enhancements. The CMEP Implementation Plan is provided to stakeholders annually. Finally, NERC has aligned the RSAW development process with the development and publishing of balloted Reliability Standards. This initiative enables stakeholders to follow the development of this compliance monitoring tool contemporaneous with the development of the Reliability Standard to which it relates, and to provide comments on the draft RSAW.
Reassess the role of Compliance Application Notices (CANs) in an audit.	(II)(A)(4) CANs were notices drafted to respond to questions that arose in the compliance monitoring process regarding how to assess compliance. Although developed for the use of audit teams and other compliance monitoring personnel, CANs were posted on the NERC website to provide transparency to industry. However, since CANS were drafted well after the related Reliability Standard was developed, the compliance assessment positions articulated in the CANs often varied from industry's perspective of the intent of the Reliability Standard or requirement at the time of its development and adoption. The CAN process demonstrated that there is a need for concurrent development and dialogue between standard drafting teams and Compliance Operations staff. As a result, in 2013, NERC began incorporating the concurrent development of compliance assessment information into the Reliability Standards development process. After June 2013, informal development project teams began posting documents during standards development titled "Compliance Input." These documents provided questions from industry and answers developed by Compliance Operations staff regarding how to assess compliance for specific requirements, or phrases in the requirements, of the proposed Reliability Standard. This basic

	tool opened the door for discussions between the standard drafting teams and Compliance Operations staff. It also allowed for discussions regarding the wording of requirements and the effect of that wording on how compliance would be assessed. The move to develop RSAWs concurrently with Reliability Standard development eliminates the need for CANs, as separate documents, effective February 2013.
Make RSAWs available before, during, and after the balloting process and ensure that they do not exceed the scope of the Requirement.	(II)(A)(4) As a result of the new processes adopted during the assessment period as described in the preceding response, RSAWs are now written concurrently with new Reliability Standard development projects. A draft RSAW is now posted during the formal comment period and prior to the ballot period for a Reliability Standard, thereby allowing stakeholders to provide comments or to raise concerns about the RSAW at that time.
Ensure that compliance guidance tools like Case Notes, Compliance Analysis Reports (CARs), CANs and Bulletins are used for guidance only, and not as vehicles for interpretations of or revisions to Reliability Standards.	Compliance training going forward will reinforce the fact that documents cannot interpret Reliability Standards. NERC has eliminated CANs (as noted in a previous response), and RSAWs are meant only as guidance to obtaining and reviewing evidence in order to obtain reasonable assurance of compliance with reliability standards. Any existing documents that are used as audit guidance will be addressed to remove language that interprets the Reliability Standard and all training going forward will be developed to demonstrate testing and audit methodology only.
Provide small entities with additional guidance regarding scoping their internal self-assessments and programs.	The purpose of RAI is to assure that entities and auditors focus on relevance. In this connection, as processes are developed for the assessment of risk and more specifically linking risks to functions and Reliability Standards, this will allow a registered entity (including smaller entities) to receive better guidance on where they should focus. Over the course of the next few months, this guidance will be published and supported with training to help smaller entities target their specific risks.
Require self-certifications only for quarters in which a misoperation occurred, rather than for every quarter.	The Regional Entities review self-certifications for all registered entities at least once annually. Regional Entities have the discretion to require monthly self-certifications for certain Reliability Standards and requirements.

Clarify how registered entities will be impacted by improvements to RAI.	II(C)(2) Building upon the success of FFT through RAI, NERC and the Regional Entities are creating additional incentives to discourage poor performance and encourage positive behaviors that contribute to higher accountability and improved reliability performance. In 2013, NERC began implementing RAI processes that promote more effective reliability risk mitigation by encouraging development and enhancement of internal management controls and corrective action programs at registered entities. Achieving the desired alignment of enforcement processing and compliance monitoring with levels of risk will benefit registered entities by eliminating undue regulatory burdens, streamlining documentation and filing requirements and improving the processing of noncompliance and related mitigating activities. The development of tools like the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, also help to set clear expectations for registered entities regarding audit practices and procedures; thereby allowing them to increase the efficiency and effectiveness of their pre-audit preparation. The ability to appropriately evaluate the risks of a registered entity will result in a more appropriately scoped audit and test plan in contrast to a one-size-fits-all approach to compliance. The more the ERO Enterprise understands the control environment and function of controls, the frequency and extent of oversight will change accordingly. In addition to compliance, sound controls also drive organizational efficiencies for the registered entities. Overall, a positive impact of RAI for registered entities is expected to be a more efficient compliance monitoring process that enables registered entities to reduce the extent of time and resources expended on external compliance monitoring activities by implementing or improving effective internal controls to minimize reliability risk.
While some regions are already employing RAI-like approaches in audits and other compliance enforcement activities, all	II(C)(2); Attachment 3 – II(B)(1); II(D)(1)(b)(iv); II(D)(1)(c)-(d) NERC is developing standardized training for Regional Entity compliance auditors to ensure that Regional Entities are consistently (both within each Regional Entity and across all

regions should be implementing an ERO-wide program as soon as possible.	Regional Entities) applying the procedures and methodologies of the new compliance monitoring documents such as the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, and RSAWs.
Enforcement	
Treat similar findings with greater consistency.	II(C)(4)(b); Attachment 3 – II(D)(1)(d) NERC and the Regional Entities engage in a number of activities to enhance consistency in enforcement processing across the ERO Enterprise. NERC and the Regional Entities participate in a multi-region working group on enforcement activities. Through this group, NERC communicates guidance and provides training on many different aspects of the enforcement program. This group is actively involved in the development or enhancement of any enforcement activities. In addition, NERC conducts oversight to ensure the consistent application of enforcement processing mechanisms and other enforcement-related processes under the CMEP. Examples of NERC's oversight includes the annual review of FFTs which results in a public report filed with FERC. Additionally, NERC reviews and approves all Notices of Penalty (NOPs) prepared and submitted by Regional Entities. One aspect of NERC's review of NOPs is to ensure that similar actions and inactions are treated consistently within and across Regional Entities in terms of whether a violation is determined to have occurred; and, to ensure that consistent penalty determinations are made for similar violations, both within the Regional Entity and across the Regional Entities.
Streamline and refine the scope of investigations.	Attachment 3 – II(C); IV(A) The NERC Rules of Procedure permit all eight Regional Entities and NERC to conduct compliance investigations (CIs), and it is extremely important for the ERO Enterprise to have a consistent approach for this activity. NERC developed a CI leaders training class to provide a methodology for the conduct of the CI process. The class introduces the approach of conducting CIs in phases, with accompanying activities and deliverables for each phase. It also explains the roles of the Regional Entity, NERC, and the applicable governmental authority in CIs. One of the key messages in the class is to reinforce that CIs are one of several formal compliance monitoring tools, and there are

	specific circumstances where a CI may be the best tool, and other circumstances where a CI is not the best tool. In addition, the class introduces the Events Analysis process. NERC found that Compliance staffs benefit from additional exposure to and familiarity with this process. The Event Analysis process has greatly reduced the number of CIs, as the Event Analysis process provides the relevant facts and circumstances of events that were previously only available through the tools employed in a CI.
While efforts are outlined in the report regarding a transition to a risk-based approach for compliance and enforcement, including discretion, targeted measurable improvements are still needed.	II(C)(4)(a); Attachment 3 – II(B)(1); II(D)(1)(b) NERC and the Regional Entities have continued to work collaboratively to develop and implement a set of metrics to measure the efficiency with which enforcement items are processed. The four metrics which have been developed during the assessment period to monitor the performance of NERC and the Regional Entities in processing enforcement items are: (1) Caseload Index – computes the number of months it would take to clear the violations in a Compliance Enforcement Authority's (CEA, i.e., NERC or a Regional Entity) inventory based on the CEA's average monthly processing rate for the preceding twelve-month period; (2) Violations in Inventory – reports the number of violations in the CEA's caseload; (3) Violation Aging – reports, by Regional Entity, the number of violations discovered in each year beginning with 2007 which have not been filed with the Commission or otherwise resolved; and (4) Mitigation Activity Aging – identifies the status of mitigation activity based upon age of violations. These metrics now provide quantitative measures by which efficiency gains (or losses) in enforcement processing can be seen and resources can be focused on areas as needed to improve performance.
Increase the timeliness of enforcement processing.	II(C)(4)(a); Attachment 3 – II(D)(1)(b)(i)-(ii) The ERO Enterprise has achieved significant success in processing older cases and reducing processing times. NERC

	tracks enforcement processing rates through its Caseload Index metric. The ERO Enterprise has demonstrated substantial improvement in this metric from July 2011 through the end of 2013. By working to reduce the number of aging violations while improving the processing speed for newer violations, NERC and the Regional Entities reduced the average age of violations in the ERO caseload by six percent in 2013, from 11.86 months in 2012 to 11.2 months. Other data on improvements in the timeliness of enforcement processing is provided in III(D) of Attachment 3. As noted in that section, as of December 31, 2013, several Regional Entities had completed processing of all or virtually all of their enforcement items that were discovered before 2012, thereby achieving or moving toward achievement of the ERO Enterprise goal of completing processing of all enforcement items within 24 months after discovery.
Provide greater transparency and detail regarding penalty calculation and enforcement in general.	II(C)(4)(b); Attachment 3 – II(D)(1)(d) NERC and the Regional Entities have taken steps to increase the transparency regarding penalty calculations and enforcement in general. With respect to penalty calculations, each of the Regional Entities considers the factors set forth in the NERC *Sanction Guidelines* when assessing penalties. During the assessment period, the *Sanction Guidelines* were significantly revised to simplify them and state more clearly how mitigating and aggravating factors are to be taken into account in penalty determinations. NERC conducts ongoing oversight of the penalty determination process, reviewing each penalty determined by a Regional Entity to ensure consistency with other penalties assessed across the ERO Enterprise for similar violations occurring under similar facts and circumstances. NERC also reviews Regional Entity processes associated with all aspects of the enforcement program. NERC also provides information on enforcement actions, trends, and metrics on a regular basis, usually by posting the information on its website. In 2013, NERC conducted a training session to better enable stakeholders to locate all publicly available enforcement-related information.
Treat repeat violations that could not have been prevented by any of the mitigating activities approved by the Regional	II(C)(2)(b); Attachment 3 – II(D)(1)(c)(ii) The ERO Enterprise works closely with registered entities to develop mitigating activities that will both address the noncompliance as well as work to prevent future reoccurrence. These are by definition fact-specific determinations.

Entity and NERC similarly as non-repeat violations.	Violations are considered repeat when the conduct underlying the two violations is repetitive. As a general matter, whether a repeat instance of noncompliance will be treated as a repeat violation for the purposes of compliance history, and whether that compliance history will warrant aggravation of the monetary penalty under the *Sanction Guidelines* in a given case, necessarily depends on the facts and circumstances of the specific case.
Provide sufficient details regarding the different tracks for disposition of compliance issues, and explain how the CEA will make the determination as to which is the proper track for disposition. Also, explain how the oversight roles will be administered between the CEA Compliance staff, the CEA Enforcement staff, NERC, and FERC.	II(C)(2)(b); II(C)(4)(b); Attachment 3 – II(D)(1)(d) The different tracks for disposition of compliance issues are as follows: (1) The FFT program, which was recently enhanced to include additional possible violations; (2) The Spreadsheet Notice of Penalty (SNOP) format; and (3) The full NOP format. The criteria for use of each disposition are discussed in Attachment 3. In addition, the ERO Enterprise, through the RAI, is developing mechanisms for addressing noncompliance outside of the enforcement process through the use of greater enforcement discretion. Under this initiative, minimal risk issues will be eligible to be recorded as compliance exceptions and mitigated without triggering an enforcement action. Among other things, NERC reviews and approves all violations filed through the SNOP or full NOP mechanisms. NERC also conducts a monthly sampling and yearly spot check of issues posted by each Regional Entity through the FFT program to ensure that the issues processed through FFT are appropriate for the FFT program, and to identify areas for further improvement. NERC and FERC maintain visibility and exercise oversight over all noncompliances, regardless of the disposition track (FFT, SNOP, full NOP, or compliance exception). FERC reviews each filing or posting and also conducts a yearly review of a sample of issues posted as FFTs.
Associate timeframes with CEA actions to be taken during the disposition process. This will provide a tracking measure to help expedite processing of low reliability risk violations.	II(C)(4)(a); Attachment 3 – II(D)(1)(b)(i), (ii), (iii) NERC works closely with each of the Regional Entities to ensure that noncompliance is processed in a timely and efficient manner and measures performance through a number of metrics. These metrics include the Caseload Index, Violations in Inventory, Violation Aging, and Mitigation Activity Aging. These metrics

	are described in further detail in II(C)(4)(a) of the *Overview of NERC Activities and Accomplishments in the Five-Year Period* and in II(D)(1)(b) and the individual evaluations of the Regional Entities in Enforcement in Attachment 3. The time needed to process a particular case may vary considerably based on the facts and circumstances of that case. However, NERC has developed and is using the above-referenced metrics to monitor overall increases and decreases in the timeliness and efficiency of enforcement processing activities by each Regional Entity.
Better communicate and emphasize the benefits of self-reporting.	II(C)(1); II(C)(2)(b); Attachment 3 – II(D)(1)(c)(i) To encourage registered entities to take proactive steps to self-identify their noncompliance and thereby promote a more reliable BPS, the ERO Enterprise provides certain incentives. For example, self-reporting is considered a mitigating factor in the penalty determination pursuant to the *Sanction Guidelines*. In addition, whether or not noncompliance was self-reported is a factor considered when selecting a streamlined disposition track such as FFT. Further, as the RAI is implemented, the extent of a registered entity's self-reporting of noncompliances (versus discovery by the CEA) will be a factor considered in evaluating the quality of the registered entity's internal controls and therefore the frequency, nature and extent of compliance monitoring of the registered entity. Early self-identification, self-reporting, and mitigation of noncompliance are important steps in improving electric reliability. NERC has established a corporate goal that reflects the importance of self-reporting and closely tracks progress with respect to this goal.
Do not issue penalties for administrative violations.	NERC does not believe that it is appropriate to determine whether or not to assess a penalty based solely on whether the violation is characterized as "administrative." The disposition of any instance of noncompliance, including whether a penalty is appropriate, is based on the risk posed by the noncompliance to the reliability of the BPS as well as other factors. Penalties were assessed for 52% of the violations processed in 2012 and 2013.
While NERC has made progress toward reducing its caseload through FFT and the bulk processing of	II(C)(1); II(C)(2)(b); Attachment 3 – II(D)(b) NERC and the Regional Entities are continually exploring ways to adopt streamlined processes to resolve noncompliances or to

violations, effort should be made to reduce time spent by the registered entities.	improve the efficiency of existing processes. During the assessment period, NERC adopted and enhanced several streamlined enforcement processing tracks. Through the metrics that have been developed, as described in earlier responses, NERC is able to monitor increases and decreases in enforcement processing timeliness and efficiency at each Regional Entity. The metrics are showing that progress is being made, e.g., as evidenced by reduction of processing times and reduced caseloads In addition, the ERO Enterprise has enhanced outreach efforts so that time spent by registered entities in providing information regarding noncompliance, risk, and mitigation is more efficiently and effectively used. For example, NERC and the Regional Entities recently distributed the *ERO Self-Report User Guide* and *ERO Enterprise Mitigation Plan Guide*. These documents were developed by NERC and the Regional Entities to provide guidance to registered entities on submitting self-reports and mitigation plans that have all of the details necessary to facilitate timely processing and avoid protracted follow-up periods and requests.
Clarify how registered entities will be impacted by improvements to the FFT program.	II(C)(1); II(C)(2)(b); Attachment 3 – II(D)(b)(iv) Through the use of FFT, the ERO more efficiently resolves instances of noncompliance that pose a lesser risk to BPS reliability, recognizing that efficient disposition of such issues allows the ERO Enterprise and industry to devote its emphasis and resources to more important reliability matters. The FFT process provides incentives for self-reporting and encourages registered entities to continue to aggressively self-identify, self-report, and mitigate reliability issues. Recent expansion of the scope of the program to possible violations posing a moderate risk to reliability, as well as issues that will be mitigated after the FFT posting, make this efficient enforcement processing mechanism available for a larger number of possible violations. Issues resolved through the FFT process are typically resolved more expeditiously than issues resolved through other disposition tracks. Further, resolution through the FFT track means that those issues will not result in the assessment of a monetary penalty.
Describe the efficiency and effectiveness of the compliance and	II(C)(2), (4); Attachment 3 – II(D)(1)

enforcement programs and their impact on reliability in light of the high percentage of lower risk violations.	The actions taken by the ERO Enterprise to identify, correct, and prevent violations of NERC's Reliability Standards have promoted the reliability of the BPS. For example, the adoption, modification, and rigorous enforcement of NERC's transmission vegetation management Reliability Standard (FAC-003), which became mandatory and enforceable in 2007, has dramatically reduced the number of outages caused by vegetation growing into high voltage lines. Beyond individual standards, the ERO Enterprise compliance and enforcement programs promote reliability by encouraging registered entities to create and maintain cultures of compliance. The ERO Enterprise creates incentives for registered entities to proactively self-identify and mitigate noncompliance. For example, the FFT program allows for a streamlined disposition of noncompliances without a monetary penalty being assessed. Through the RAI, NERC and the Regional Entities are working together to implement further enhancements that will allow minimal risk noncompliance to be processed outside the enforcement track. NERC and the Regional Entities are also developing and implementing procedures and processes to enhance auditing approaches across the ERO Enterprise. These efforts will allow registered entities and the ERO Enterprise to shift toward a risk-based model of compliance and enforcement, thereby allowing registered entities to dedicate more of their resources toward addressing issues posing greater risks to reliability.
Clarify how NERC's compliance monitoring and enforcement efforts have matured into a "robust program that provides industry with more certainty on actions, outcomes, and reliability consequences."	II(C); Attachment 3 -II(D)(1)(a) During the assessment period, NERC and the Regional Entities worked on increasing consistency in compliance monitoring processes across the ERO Enterprise. These efforts have included the development of common auditor qualifications and competency requirements, development of the common *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, and development of a common training program for auditors. During the assessment period, NERC and the Regional Entities also worked to develop more mature enforcement processes for the ERO Enterprise. The resulting efficiency gains in enforcement processing ensure that final outcomes relating to noncompliances are known earlier.

	The implementation of streamlined enforcement processing mechanisms, such as SNOP and FFT, has facilitated the faster resolution of noncompliance items. NERC provides significant transparency regarding the processing tracks that are available and the associated criteria for a noncompliance item to be placed onto each track. In addition, NERC and the Regional Entities worked together to design and build a system for the collection, management, and exchange of compliance-related information between NERC and the Regional Entities. NERC's centralized system and the complementary systems in place at the Regional Entities enable enforcement processing efficiencies and facilitate consistent tracking of violation status across the ERO Enterprise. Further, for several years, NERC has closely tracked various measures regarding the overall performance of the ERO Enterprise as it relates to enforcement activities. Beginning in 2013, NERC and the Regional Entities developed and implemented a series of metrics (described in earlier responses) to track and evaluate the performance of the ERO Enterprise and of each Regional Entity in enforcement processing. These metrics allow NERC to analyze trends and identify areas where further improvements may be achieved.
Registration and Certification	
Enhance the System Operator Certification program by making training for exam preparation more available.	The System Operator Certification program has multiple vendors and individual utilities that have developed NERC system operator certification exam preparation courses. NERC does not believe that further assistance from NERC is appropriate. As an independent certifying entity, if NERC were to develop and/or sponsor training, NERC would compete with established vendors.
Provide greater clarity, guidance, and consistency regarding Coordinated Functional Registration (CFR) and Joint Registration Organizations (JROs), and examine how the process can be streamlined.	II(B); Attachment 3 – II(A) During the assessment period, revisions to NERC Rules of Procedure Section 507 and the addition of Section 508, approved by the Commission on June 10, 2010, clarified the operations of CFR and JRO registrations. Specifically, revised Section 507 allows an entity to 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. The registering entity thereby accepts on behalf of such members or related entities all compliance

	responsibility for that function or those functions including all reporting requirements. Section 508 allows multiple entities to register using a CFR for one or more Reliability Standard(s) or for one or more requirements or sub-requirements with particular Reliability Standard(s) applicable to a specific function. The CFR is the complete registration for each entity, with each entity taking full compliance responsibility for those Reliability Standards or requirements or sub-requirements applicable to the CFR.
Registration should be more carefully tailored and based on sounder reasoning. Update the functional model to provide greater clarity and guidance to registered entities. The risk-based registration concept must be carefully developed and implemented to ensure that entities that remain registered are not adversely impacted.	II(B)(1)-(2); Attachment 3 – II(A) In January 2014, NERC launched the Risk-based Registration Assessment initiative to enhance the compliance registration and certification program to be more efficient and better aligned with reliability benefit. Through this initiative, NERC will register entities and assign appropriate Reliability Standard requirements commensurate with the need to mitigate the risk that they pose to the BES, by scaling registration criteria based on their contributions to reliability. NERC will also develop tools that will enhance a registered entity's understanding of the relevant Reliability Standards and requirements that apply to them. Scoping compliance responsibilities according to BPS reliability risks will equate to better use of resources at both the registered entity level in the implementation of compliance programs, and at the Regional Entity level in their overall compliance monitoring efforts. During the assessment period, NERC revised the definition of the BES in the *Glossary of Terms Used in NERC Reliability Standards*, in response to Commission directives in Order Nos. 743 and 743-A. The objective of the revisions is to ensure consistent inclusion or exclusion of entities and elements that are subject to Reliability Standard requirements. The Commission-approved revised BES definition enables NERC and the Regional Entities to identify assets that are material to the reliability of the interconnected transmission network. By using a set of continent-wide, "bright line" criteria that eliminates regional discretion, the revised definition effectively ensures that the users, owners and operators of BES assets are identified and registered on a consistent basis in order to comply with applicable Reliability Standards. The revised BES definition provides improved clarity for industry by identifying specific categories of facilities and configurations as inclusions and exclusions to the BES. Additionally, the case-by-case exception process to add elements to, and to remove elements from, the BES provides

	transparency and uniformity to the determinations of what constitutes the BES. In summary, the revised, much more detailed and granular BES definition along with the BES exception process should result in greater consistency, transparency and predictability in registration determinations.
Provide additional clarification, guidance, and training regarding the definition of the term BES to ensure consistent application in both Reliability Standards and the compliance registration process.	II(B)(2) In March 2014, FERC approved the revised definition of BES. As described in the preceding response, the revised BES definition provides improved clarity for industry by identifying specific categories of facilities and configurations as inclusions and exclusions to the BES. During the first half of 2014, NERC held communications and training sessions for Regional Entities, registered entities, and NERC staff to address, among other things: (i) evidentiary requirements for BES determinations; (ii) review and appeal mechanisms; and (iii) Reliability Standards applicability. These sessions included workshops and webinars. NERC has a dedicated webpage for information related to the BES definition and the notification and exception processes. This page hosts links to materials that support the application of the BES definition and provide entities with the information needed to make uniform determinations of BES elements. These materials include, among other things, webinars, training videos, process documents, and guidelines. The page is updated as new materials become available. The webpage is available at: http://www.nerc.com/pa/RAPA/Pages/BES.aspx.
Provide an explanation regarding the use of the term BES in certain instances and BPS in other instances.	The full definitions of BES and BPS are contained in the *Glossary of Terms Used in NERC Reliability Standards*. "BPS" is the statutory term in Section 215 of the FPA and sets the outer limit of NERC (and FERC) authority. FERC has accepted NERC's use of the term "BES" and its definition and has indicated that the "BES" does not exceed the scope of the "BPS." Entities that use, own, or operate elements of the BES as established by the FERC-approved definition of BES are: (i) owners, operators, and users of the BPS; and (ii) candidates for registration. Since 2006, NERC has registered entities for one or more functional categories depending on whether it is a user, owner or operator of the BPS.

	NERC has used "BES" principally for registration purposes. In March 2014, FERC approved the revised definition of "BES." As described in a previous response, the revised BES definition includes bright line core criteria with various enumerated inclusions and exclusions. Now that "BES" is clearly defined, the term can be used to determine on a consistent basis the entities that warrant registration and address material impacts on reliability.
Reliability Assessment & Performance Analysis Metrics	
Develop performance measures to determine if a Reliability Standard is actually reducing risk to reliability.	Performance measures from the CMEP assist NERC in assessing whether a Reliability Standard is actually providing more certainty on actions, outcomes, and reliability consequences NERC compliance staff supply standard drafting teams with compliance and enforcement information, statistics, and perspectives to help develop Reliability Standards that provide an increased reliability benefit and clarify compliance risks.
Explain more thoroughly how the information provided in reliability assessments affects the future adequacy and reliability of the BPS.	II(D)(1), II(D)(2), II(D)(3) In response to direction from the NERC Board of Trustees in February 2013, NERC has developed a RRM process to create and execute plans for managing reliability risk and to integrate these plans with the business planning and budgeting process. The RRM process includes the identification of the *ERO Top Priority Reliability Risks* for each upcoming business planning and budget cycle. The development of the list of top ten high priority reliability risks is intended to focus the efforts of the ERO Enterprise program areas, including training and education, Reliability Standards setting, and compliance. NERC developed a set of the top ten priority reliability risks to be focused on in the development of the *ERO Enterprise Strategic Plan 2014-2017*. NERC has also developed a voluntary Event Analysis process that delivers quality, timely and actionable lessons learned to registered entities. NERC assesses every event submitted through the voluntary Event Analysis process to identify and share possible risks to reliability with industry members.
Provide metrics that focus not only on enforcement but also measure performance risk and	VII NERC and the Regional Entities have collaboratively made significant progress in developing a shared, rolling three-year *ERO Enterprise Strategic Plan*, which includes performance

specify specifically what is working and what is not.	metrics. The NERC Board of Trustees approved the 2014 *ERO Enterprise Performance Metrics*. These performance metrics will be used to assess the overall effectiveness of the ERO Enterprise in addressing risk to the BPS, achieving reliability results, measuring and assuring the effectiveness of Reliability Standards and compliance programs, and improving risk mitigation and program execution. NERC's performance metrics include four overarching metrics focused on overall effectiveness in addressing BPS risks and improving reliability. NERC's performance metrics also include a number of supporting measures that assess the effectiveness of the key operational elements of the ERO Enterprise.
Describe the basis for including the 345-kV breaker failures as a potential trend in risk prioritization.	II(D)(2) Circuit breaker failures, in conjunction with another fault, may lead to more BES facilities removed from service than required to clear the original fault. NERC has identified a potential trend of 345 kV SF6 puffer type breakers failing as being one of the ten high priority reliability risks.
Provide a more complete explanation of how the daily severity risk index is used to help prioritize risks.	I(A) The daily severity risk index value, a metric created by NERC that measures risk impact or "stress" from events resulting in the loss of transmission, generation, and load, provides an industry reference for historical BPS reliability. This metric also offers analytical insights toward industry action and enables the identification and prioritization of specific steps that can be implemented in order to reduce and manage risks to reliability.
Training, Education, and Personnel Certification	
Increase the availability and accessibility of training regarding audit preparation, Reliability Standard compliance, Event Analysis, and major NERC initiatives such as BES definition, and CIP Version 5 Reliability Standards.	II(A)(4), II(B)(2), II(C)(2), II(D)(1), II(D)(2), II(D)(3), II(E)(1)(c); Attachment 2, pp. 44, 45;[3] Attachment 3 – II(B)(1)(d) (*NERC Training Activities for Regional Entity Compliance Staff)*; II(B)(2)(a) (*Regional Entity Training, Education and Outreach Programs for Registered Entity Personnel*); II(B)(2)(b)(ii)-(ix) (*Assessments of the Individual Regional Entities*) Between 2011-2013, the Regional Entities' workshops and equivalent training programs attracted more than 30,000 attendees. NERC and the Regional Entities develop new training

[3] Attachment 2 to the *Five-Year ERO Performance Assessment Report* is titled *Joint Regional Entity Self-Assessment*.

	offerings as new needs arise. Recent examples are provided below. Additionally, NERC developed a set of the top ten priority reliability risks to be focused on in the development of the *ERO Enterprise Strategic Plan 2014-2017*. The development of these top ten high priority reliability risks is intended to focus the efforts of the ERO Enterprise program areas, including training and education, Reliability Standards setting, and compliance. NERC is working to provide training to industry (as well as to compliance auditors) on how to assess compliance with new or revised Reliability Standard. This training is provided following FERC approval of a Reliability Standard, but well before the Reliability Standard effective date. To implement the revised BES definition, NERC developed a web-based, ERO Enterprise-wide application to provide a consistent platform for registered entities to submit self-determined notifications and to submit exception requests for inclusions in or exclusions from the BES. This application is called the BESnet Enterprise Application Tool. During the first two quarters of 2014, NERC held communications and training sessions for Regional Entities, registered entities, and NERC staff to address, among other things: (i) evidentiary requirements for BES determinations; (ii) review and appeal mechanisms; and (iii) Reliability Standards applicability. These sessions included workshops and webinars. NERC hosted a series of workshops in 2013 that addressed defining internal controls, conducting risk assessment, launching pilot programs, enhancing the FFT process, and improving self-reporting. In 2013, NERC and the Regional Entities began to develop and implement tools that will define techniques and methods to perform compliance monitoring in a consistent manner across the ERO Enterprise. The Regional Entities began using the first of these tools, the *Compliance Auditor Checklist*, in August 2013. In December 2013, NERC and the Regional Entities completed the first draft of a companion document for the *Compliance Auditor Checklist*, the *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*. NERC disseminated the manual and provided initial training to Regional Entity auditors during the first quarter of 2014. NERC has made the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor*

	Manual, available to industry to provide guidance on audit preparation. Specific documentation or other aids to assist in the implementation of the RRM process, document templates, and detailed instructions and training are being developed to support the execution of this process and will be made available to industry. NERC provides registered entities (as well as Regional Entity staff) with cause analysis training. As of December 2013, 164 personnel from all eight Regional Entities and over 600 people from 115 different registered entities have received more than 4,000 hours of cause analysis training, with 432 hours of continuing education hours awarded to 54 NERC-certified system operators. NERC is adding a training and education component to the Event Analysis process to increase the relevance and impact of lessons learned for the Regional Entities, industry, and other stakeholders. Beginning during the assessment period, NERC holds an annual Grid Security Conference (GridSecCon). Over 300 industry and government stakeholders attended the most recent GridSecCon in October 2013. Additionally, almost 200 stakeholders attended credentialed training sessions in cybersecurity and physical security. NERC is committed to working with industry to ensure smooth transition to the CIP Version 5 Reliability Standards. NERC has been collaborating with Regional Entities and responsible entities by establishing a transition program to support implementation of Version 5. NERC has implemented several program elements related to outreach, communication, and training, to include periodic guidance documents to keep industry informed during the transition period. NERC conducted a pilot Version 5 implementation study, which included six volunteer entities that implemented the Version 5 Reliability Standards on an accelerated basis. Future training will include auditor training, technical workshops, guidance, and other lessons learned from the Version 5 implementation study.
Incorporate registered entity independent subject matter experts into the audit process.	Attachment 3 – II(B)(2)(b)(ii)-(ix) (*Assessments of the Individual Regional Entities - Department Structure / Staffing / Conflict of Interest Avoidance*)

	As a key RAI compliance activity, the Prototypes and Pilot program focuses on the development and implementation of a formalized approach to risk assessments and testing of management controls. NERC and the Regional Entities initiated the first phase of the pilot program during 2013. This phase explored different approaches to applying risk-based auditing concepts (e.g., audit scoping, reliability risk assessments, and management controls review and testing). For 2014 and beyond, a team consisting of NERC, Regional Entity, and industry representatives as well as an independent audit consultant will evaluate the findings and determine the best audit approach to implement throughout the ERO Enterprise.
Event Analysis	
Separate Event Analysis from Compliance Operations.	II(D)(3) Event Analysis and Compliance Operations are separate processes. NERC has developed a voluntary Event Analysis process. Participation in this voluntary process does not relieve registered entities of their obligation to comply with NERC Reliability Standards. Registered entities are encouraged to continue performing critical self-assessments of compliance with Reliability Standards in connection with a qualifying event, occurrence or any other time when adherence to the NERC Reliability Standards is in question.
Increase the efficiency and clarity of the compliance assessment process associated with an event.	II(D)(3); Attachment 3 – IV(A) and (C) The annual NERC CMEP Implementation Plan and the *ERO Event Analysis Process* document describe the expected actions by affected registered entities following an event or disturbance. While voluntary on the part of registered entities, this process includes a systematic review of the event against approved Reliability Standards, improved self-reporting and expedited mitigation of any possible noncompliances, thus improving reliability. The Regional Entities use outreach forums and other mechanisms to describe the process and encourage these actions by registered entities.
Streamline the cause coding mechanism.	II(D)(3) NERC is continuously striving to improve how it defines, catalogs and trends the causes of system events. The cause code assignment allows for greater historical trending and predictive analysis. NERC plans to further facilitate event analysis by merging its event-driven databases across the ERO Enterprise

	and defining the relationships between various system cause codes.
Increase the timeliness, transparency and comprehensiveness of dissemination of information relating to Event Analysis and lessons learned.	II(D)(3) NERC is collaborating with the NATF and the NAGF to further enhance the Event Analysis process and lessons learned dissemination in identifying risks to the BPS. NERC plans to improve the timeliness of the availability of and access to final event reports by creating a secure portal that will be accessible by industry to obtain these reports.
Improve the consistency of the NERC alert system by ensuring that alert levels are commensurate with the risk of the issue presented and do not impose unnecessary burdens on registered entities.	II(D)(3) NERC generates alerts in limited circumstances. If an event merits an alert, NERC first discusses the potential alert with Regional Entities and registered entities before disseminating the alert. Under Section 810 of the NERC Rules of Procedure, NERC can issue "Level 1 Advisories," "Level 2 Recommendations," and "Level 3 Essential Actions," depending on the underlying circumstances. Each of these issuances requires different actions (if any) by registered entities. NERC strives to use the issuance that is appropriate to the circumstances so as not to impose undue burdens on registered entities.
Ensure that sabotage events are communicated by NERC Alert.	Not all sabotage events are appropriate for issuing an alert; however, additional information on security-related events is available to all users on the improved Electricity Sector Information Sharing and Analysis Center (ES-ISAC) portal and through other ES-ISAC channels.
Make improvements in full publication of events (under appropriate confidentiality controls) to users, owners and operators.	NERC now has a secure site that allows registered entities to gain NERC-authorized access to reports from other registered entities that have agreed to share such information.
Consider that not all issues identified by the Event Analysis program are issues that should become standards or even alerts.	Reliability issues presenting a risk to the BPS that have been identified by Event Analysis are subject to further NERC consideration and discussion with Regional Entities and registered entities before becoming the subject of a Reliability Standard development project. The decision to issue an alert or develop a Reliability Standard is based on this collaborative process. Additionally, the RISC considers risk-related issues and

	advises the NERC Board of Trustees on the appropriate action to take to address risks to the BPS. *See also* II(A)(6)(a) and II(A)(6)(b)
Critical Infrastructure Protection	
Increase the focus on physical security, in addition to cybersecurity.	II(A)(8)(e); II(E) NERC recognizes that identifying, assessing, and preventing threats and risks to both the physical security and the cybersecurity of the BPS, while always matters of concern, have attained increasing significance in the last three to four years. NERC, through its Critical Infrastructure department, ES-ISAC, and the Critical Infrastructure Protection Committee, is engaged in various activities to address physical security issues. In addition, NERC recently developed and submitted for Commission approval a new physical security Reliability Standard (CIP-014-1).
Increase the speed at which registered entities will be able to learn how CIP Reliability Standards will be interpreted by auditors, and ensure that these interpretations are consistent across the Regional Entities.	II(A)(4) RSAWs are now being written concurrently with new Reliability Standard development projects. Draft RSAWs are to be posted during the formal comment period and prior to the ballot period for the associated Reliability Standards. Stakeholders are encouraged to provide feedback on the draft RSAWs.
Provide additional guidance with alerts that will help avoid public disclosure request responses with CIP-related information.	NERC exercises the utmost caution and will not issue alerts that include sensitive CIP-related information. It is also the responsibility of the entity responding to a request for information to ensure that any sensitive information it provides is appropriately marked and that appropriate exemptions from disclosure are claimed.
Explore a full functional separation of NERC and the ES-ISAC as recommended in the February 2014 report from the co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative.	II(E)(2) NERC is committed to keeping the ES-ISAC separate from NERC's compliance monitoring and enforcement activities and enforcing the Board of Trustees-approved corporate policies that are in place. In addition, NERC is considering a physical separation of ES-ISAC personnel in the Washington, D.C. office.
Strengthen inter-sector coordination: the ES-ISAC should explore ways to	ES-ISAC has acted to strengthen inter sector coordination through increased information sharing and support to ESCC in the following ways:

provide information and support the activities of the Electricity Sub-Sector Coordinating Council (ESCC).	(1) Extensive subject matter expert contribution to "Energizer" and ESCC Playbook products; (2) Alignment of ES-ISAC capability under ESCC to provide operationally informed context and implementation; (3) Full ESCC Senior Executive Working Group participation; (4) National Cybersecurity and Communications Integration Center watch floor and Department of Homeland Security Unified Coordination Group (UCG) participation; and (5) Full participation at Department of Energy Sector Specific Agent (SSA) hosted Clear Path II restoration event and all pertinent OSD Defense Critical Infrastructure Program (DCIP) events. In addition, ES-ISAC contributed subject matter expert leadership to initiation of a pilot continuous monitoring and automated information exchange capability undertaken with selected major utilities, known as the Cybersecurity Risk Information Sharing Program (CRISP). This capability provides foundational support to top future ESCC inter-sector information sharing objectives. Further involvement in CRISP by the ES-ISAC on a permanent basis is under active consideration. Further, ES-ISAC accelerated its own capability maturation consistent with NERC CIPC Information Sharing Task Force and Government-Industry Information Sharing Survey findings with an advanced portal fitted to entity, ESCC Secretariat, and National Council of ISACs cross sector sharing requirements.
Stakeholder Communications, Public Relations, and IT	
Offer more unified, coordinated, and user-friendly IT tools and programs to registered entities.	ERO senior leadership intends to develop ERO Enterprise IT applications, where appropriate, to support common processes, to enhance the efficiency and effectiveness of Regional Entities' practices, to increase the consistency of the interface with registered entities, and to facilitate NERC's oversight function.
Provide greater consistency between NERC and Regional Entity websites.	VII; Attachment 6, pp. 14-16.[4] NERC and the Regional Entities are engaged in several activities to develop unified or consistent IT programs and tools and to

[4] Attachment 6 to the *Five-Year ERO Performance Assessment Report* is titled *NERC's Plan and Initiatives for Improving Coordinated Operations Across the ERO Enterprise*.

	coordinate key messages and direction and enhance consistency across the ERO Enterprise.
Improve technical support, accessibility, and organization of the NERC website.	In 2013, the NERC public website was converted from a legacy platform to a SharePoint site greatly improving search functions, security and scalability of the website. Converting the website to a contemporary off-the-shelf application will allow continued improvements to document organization, and enhanced search capability through the use of metadata. Technical support has been enhanced by usage of the contact form, with relevant questions and comments being directed to the correct program area or to the IT department for resolution.
Reduce travel expenses for registered entities by more frequently changing locations where meetings are held (beyond Atlanta), and increasing the availability of webinars and teleconferences.	Industry engagement is a critical component of NERC's activities and strategic initiatives. NERC uses webinars to engage and educate industry on a number of topics. For example, in 2013 alone, NERC hosted 43 Reliability Standard industry webinars attended by an average of 360 participants. However, NERC decided to move its headquarters from Princeton, N.J. to Atlanta, G.A., among other reasons, because Atlanta is a major airline hub that is directly accessible from many parts of the country. In addition, in selecting meeting locations, NERC must balance the cost to and convenience for potential participants of using Atlanta versus locations other than Atlanta, with the cost savings associated with holding the meeting in NERC's own facilities (rather than in rented space in another location and the travel expenses for NERC staff to other locations.
Improve retention of NERC staff to ensure better, less disruptive functioning of the ERO.	NERC management and the Board of Trustees recognize the importance of retaining experienced employees. Several initiatives are in place or underway to enhance employee engagement, including improving hiring practices, conducting regular check-ins with new staff periodically after hiring, periodic evaluation of culture through formal employee surveys, and the development of appropriate initiatives including a set of corporate core values, as well as ongoing review of market compensation for personnel with the necessary skills and experience.
Increase the consistency and clarity of the communications of NERC leadership regarding the end-state vision and	VII; Attachment 6, pp. 16. To facilitate effective communications across the ERO Enterprise, in May 2013 the NERC Board of Trustees initiated a practice of meeting twice yearly as a group with all the chairs and

progress of major ERO initiatives.	vice-chairs of the Regional Entities, with a portion of these meetings conducted with the NERC and Regional Entity CEOs also present. Additionally, a NERC-Regional Entity communications working group has been active for several years, coordinating consistent messaging across the ERO Enterprise. Further, NERC and the Regional Entities have coordinated outreach to FERC Commissioners and staff and to Canadian governments. NERC is working to address the areas where improvement is needed.
Make processes for developing documents related to compliance more transparent and open to stakeholder feedback.	II(A)(4); II(C)(2)(a) NERC has taken several steps to address this concern. RSAWs are now developed concurrently with Reliability Standards development projects, allowing for increased coordination among compliance staff and the standard drafting teams and the opportunity for industry comment on the draft RSAWs. Draft RSAWs are to be posted during the formal comment period and prior to the ballot period for the associated Reliability Standards, allowing stakeholders to provide comments or raise concerns at that time. Further, NERC is also engaged in several activities under RAI to enhance transparency and consistency in auditor practices across the ERO Enterprise, including making the *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, available to industry.
Increase the specificity of the ERO strategic plan.	VII NERC and the Regional Entities have collaboratively made significant progress in developing a shared, rolling three-year *ERO Enterprise Strategic Plan.* In May 2014, the NERC Board of Trustees approved a series of performance metrics which will be used to assess the overall effectiveness of the ERO Enterprise in addressing risk to the BPS, achieving reliability results, assuring Reliability Standards and compliance effectiveness, and improving risk mitigation and program execution. They include four overarching metrics focused on overall effectiveness in addressing BPS risks and improving reliability. They also include a number of supporting measures that assess the effectiveness of the key operational elements of the ERO Enterprise.
Improve and streamline external communications to	NERC has created a once-a-week bulletin for Reliability Standards announcements, and is working to include compliance

make them more useful and accessible to stakeholders.	activities in this bulletin as well. Additionally RSS feeds have been added to the "NERC Newsroom" webpage enabling stakeholders to subscribe or unsubscribe to the NERC newsletters or NERC headlines. Future releases will include more RSS feeds that will provide stakeholders the opportunity to subscribe or unsubscribe to information on the NERC website, coupled with ongoing enhancements to content and search features.
Continue to work with Canadian entities regarding NERC's efforts to seek recognition in Canada, including preparing and verifying the information in Attachment 1.[5]	III; Attachment 1 – I(6) NERC is actively working with Canadian entities in a variety of ways. NERC participates in the meetings of a trilateral group consisting of regulators from Mexico, FERC, and the Federal-Provincial-Territorial Electricity Working Group (Canada). In addition, each month NERC staff participates in calls to discuss standards drafting efforts and associated governance and committee-related activities. Workshops and organized forums over the course of each year provide dedicated time for outreach and exchange of perspectives. NERC is also working with relevant stakeholders in Canada, including registered entities and applicable government authorities, on increasing visibility of compliance monitoring and enforcement activities that assure reliability in Canada. NERC appreciates the assistance provided by Canadian entities in the preparation and verification of information in the detailed discussion in Attachment 1 regarding NERC's efforts to seek recognition in Canada.
Business Plan and Budget	
Give stakeholders earlier opportunities to provide input for the business plan development process and the business plan. Extend the time by which stakeholders have an opportunity to provide input into the business plan and	Attachment 3 – V(B) NERC and the Regional Entities typically start the BP&B process in the fourth quarter of the second preceding year. The process includes multiple opportunities for stakeholder input, and NERC attempts to provide opportunities for stakeholder input on the *ERO Enterprise Strategic Plan* and the BP&B as early as reasonably possible in the process.

[5] Attachment 1 to the *Five-Year ERO Performance Assessment Report* is titled *Discussion of How NERC Meets the ERO Certification Criteria of 18 C.F.R. §39.3(b)*.

budget (BP&B), and increase the clarity of projected costs.	In the preparation schedule for the 2015 BP&B, policy input for the *ERO Enterprise Strategic Plan* was requested by the NERC Board of Trustees on January 8, 2014 with a response date of January 29, 2014. Meetings with trade associations were held in January 2014 on the *ERO Enterprise Strategic Plan* and in April 2014 on the 2015 BP&B. The Member Representatives Committee (MRC) meetings on February 5, 2014 and May 6, 2014 included further opportunities for policy input. A draft NERC 2015 BP&B was posted on May 16, 2014 for a 45-day stakeholder comment period. A final draft of the 2015 BP&B was posted on July 15, 2014 for a 2-week stakeholder comment period. Additional opportunities for stakeholder comment are provided through multiple scheduled meetings of the MRC BP&B Input Group (described below) and meetings of several NERC standing committees (Operating, Planning, Standards, Critical Infrastructure Protection, Compliance and Certification, and Reliability Issues Steering Committees) to receive input, as well as through opportunities for stakeholder comments in open sessions of the quarterly MRC and NERC Board of Trustees meetings. NERC provided more opportunities for stakeholder input in the 2015 BP&B preparation schedule than was provided for the 2014 BP&B.
Explain how stakeholder input on the BP&B is actually utilized	NERC carefully and thoroughly considers all stakeholder input on the BP&B, whether it is submitted in writing during formal posting and comment periods or in open meetings. Typically, stakeholder comments are not directed to individual detailed line items in the draft BP&B, but rather are primarily directed to the overall amount of increase in the proposed budget for the ERO Enterprise or for certain departments, or the overall assessment increase. In a number of years, NERC has responded to stakeholder concerns about the overall level of budget and assessment increases shown in earlier drafts of the BP&B, by reducing planned expenditures (e.g., through eliminating or deferring specific projects and other initiatives or by reducing planned levels of compensation increases for some or all employee categories) to produce a lower level of expenditures and assessments in the final BP&B. Additionally, in each annual BP&B filing with FERC beginning with the filing for 2009, NERC has included an attachment summarizing stakeholder comments received during development of the BP&B and how NERC addressed or considered the comments. Finally, a number

	of enhancements to NERC's BP&Bs have been the result, in whole or in part, of stakeholder comments, including the provision of greater granularity and more detailed explanations for consultant and contractor expenses and for proposed Information Technology and other information systems and infrastructure projects in the BP&B; and the development and inclusion of long-term (three-year) future budget projections in the BP&B.
Permit greater incorporation of policy input from the MRC into the business plan.	Under the NERC Bylaws, one of the purposes of the MRC is "to provide advice and recommendations to the board with respect to the development of annual budgets, business plans and funding mechanisms, and other matters pertinent to the purposes and operations of the Corporation" (Article VIII, §1). Under Article XIII, §4 of the Bylaws, consultation with the MRC and posting of draft BP&Bs for review and comment by the MRC are mandatory components of the development of the annual BP&B. Obtaining MRC comments and input has always been a part of the BP&B development process; however, over the last three BP&B cycles, steps have been taken to increase MRC input. Specifically, a MRC BP&B Input Group was formed in August 2012 and began to function as part of the development of the 2013 BP&B; the participation of this group has been formalized as a specific mechanism for the provision of MRC input. The BP&B development process now includes a specific schedule of meetings with the MRC BP&B Input Group – for example, the preparation schedule for the 2015 BP&B includes 5 scheduled meetings or conference calls with the MRC BP&B Input Group, as well as 2 scheduled MRC informational session webinars and the regular quarterly MRC meetings. Additionally, as indicated earlier, the NERC Board of Trustees has now made it a regular practice to solicit policy input from the MRC as well as other stakeholder groups, early in the process, on various issues relevant to the *ERO Enterprise Strategic Plan* and the BP&B; the policy input received is then discussed at subsequent meetings of the Board of Trustees. NERC does not believe that prior policy input from the MRC regarding goals has not been taken into account in developing business plans, as suggested by the comment. However, the development of both the rolling three-year *ERO Enterprise Strategic Plan* and the annual BP&B reflects consideration and accommodation of input and comments from numerous stakeholder sources, some of which may be inconsistent or even conflicting, as well as the need to meet NERC's legal, regulatory, and corporate responsibilities. Therefore, it will not necessarily

	be possible to trace specific input from a specific source into specific provisions of the BP&B.
Clarify that certain non-statutory requirements were transitioned out of the NERC BP&B.	Without agreeing or disagreeing that these were non-statutory activities, this comment is correct that the Interchange Distribution Calculator, previously funded by NERC, has been transitioned to the IDC Association, and the E-Tag registry has been transferred to the North American Energy Standards Board; both are no longer funded by NERC. Other reliability-related tools have been transitioned to industry sponsorship and funding. NERC Rule of Procedure Section 1002, as amended during the assessment period, states that NERC will review all tools and services it provides to determine if they can be transitioned to an appropriate industry group or organization. Additionally, NERC will be ending its funding and management of the North American Synchro-Phasor initiative by the end of 2014 as it is transitioned to private sector sponsorship and funding. Finally, the formation of the NATF and NAGF has resulted in those organizations taking responsibility for some educational and collaborative activities that otherwise might have been conducted and funded by NERC.
Provide presentations to stakeholders on NERC's efforts to ensure maximum efficiency in the use of resources. The *Five-Year ERO Performance Assessment* should address reasons for budget increases and NERC's plans to control costs going forward.	NERC strives to explain in each annual BP&B how it is using resources efficiently within the proposed budget. Specific actions that have been taken to reduce budgeted costs and use resources efficiently are described in each BP&B; typically, these actions are at a very granular level (e.g., actions within specific program areas) rather than actions that will impact the efficiency of all aspects of NERC's operations. In addition to the textual discussion in the final BP&B, during the BP&B preparation process, NERC conducts a number of meetings, conference calls and webinars for stakeholders and stakeholder groups to explain the proposed BP&B. These include meetings with trade associations and NERC committees as well as webinars, meetings, and conference calls (such as meetings and conference calls with the Board of Trustees, the Finance and Audit Committee, and the MRC) that are open to all stakeholders. In these meetings, conference calls and webinars, the proposed BP&B is typically reviewed at a more aggregated level with focus on the more significant projects and initiatives impacting cost increases and decreases. There are several specific initiatives that NERC has implemented or is in the process of implementing that have increased or will increase the efficiency of the ERO Enterprise operations. These initiatives have been discussed and described through numerous

	means accessible to stakeholders including in the rolling three-year *ERO Enterprise Strategic Plan*, BP&Bs, CMEP Implementation Plans, and workshops, seminars and webinars, as applicable to each particular activity. NERC will continue to look for additional means to communicate with stakeholders on NERC's efforts to use its resources efficiently, both through giving added focus to this topic in existing presentations and through additional stakeholder communications addressing this topic. NERC respectfully disagrees that a detailed analysis of budget increases over the five-year period and possible future increases is necessary for the *Five-Year ERO Performance Assessment Report*. NERC's annual BP&Bs already provide an annual review of (and opportunity for stakeholder comment on) budget increases from the prior year to the budget year. Each annual BP&B provides an explanation of budget increases (if any) in each of several line items for each program area, with more extensive discussion of more significant cost increase items. The *Five-Year ERO Performance Assessment Report* describes a number of initiatives that NERC has implemented and is continuing to undertake to improve the efficiency of NERC and Regional Entity operations while enhancing BPS reliability, including: (i) the SNOP process and FFT process (which continues to be enhanced); (ii) the RAI and the entire RRM process, all of which are focused on making more efficient use of ERO Enterprise (and stakeholder) resources while focusing resources on the issues and areas that pose the greatest risk to BPS reliability; (iii) the development of common training programs, the *Compliance Auditor Checklist*, and the *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, for compliance auditors across all Regional Entities; (iv) the Paragraph 81 project and the Standards Independent Expert Review Panel review of Reliability Standards requirements, which have resulted in the elimination of numerous requirements, thereby reducing the number of requirements that NERC and the Regional Entities must expend resources to monitor; and (v) the risk-based and cost-effectiveness reviews of proposed standards development projects so that resources are not expended on development of standards that will have minimal impact on reliability. The development of new or enhanced, uniform information and data management systems (both internal and user-facing) to be used by the entire ERO Enterprise will also increase efficiencies and

	help to control costs in the future. Additionally, NERC has reorganized departments, such as Reliability Standards, to use personnel more efficiently. By far the most significant component of NERC's BP&B are personnel-related costs, both direct personnel expenses (salaries and benefits) and costs that vary primarily based on the number of personnel (such as travel expense, office space costs, and telecommunications and computing costs). Therefore, as NERC has increased staffing in response to input from FERC and stakeholders indicating the need for more extensive or expeditious activities in specific areas (e.g., faster Reliability Standards development, increased NERC staff support for standard drafting teams, increased oversight of Regional Entity compliance monitoring activities, more expeditious processing of noncompliance items, increased training, education and outreach activities, and additional, focused reliability assessment reports), and has responded to the increased significance of certain reliability risk areas (e.g., cybersecurity), NERC staffing has necessarily increased and therefore budgets have increased. A second, overall area of budget increases has been for new and enhanced IT and other information and infrastructure systems in response to: (i) stakeholder desires for more efficient systems with commonality across Regional Entities; (ii) the need for more efficient NERC and Regional Entity internal business processes; and (iii) the development of new user-facing systems to meet emerging needs such as the Technical Feasibility Exceptions process and the BES definition exceptions process.

Table 2: Stakeholder Comments Concerning Regional Entities

In the following table, (i) the first column contains summaries of key stakeholder comments concerning the Regional Entities; and (ii) the second column lists, where applicable, the specific location within the *Five-Year ERO Performance Assessment Report* where the comment is addressed. Additionally, for most of the stakeholder comments, the second column contains a brief response to the comment. The table is divided into sections that correspond to the broad categories of questions asked in the Stakeholder survey.

Summary of Key Stakeholder Comment About Regional Entities	Where Comment is Addressed
Reliability Standards	
Improve the dissemination of information by providing additional information regarding evolving Reliability Standards.	Attachment 3 – I.A; II.B.2.a[6] Many Regional Entities have committed more resources in order to engage in additional training, education, and outreach activities to assist registered entities with their compliance and enforcement responsibilities. These increased activities have included additional workshops, newsletters to industry, and other direct communications.
Compliance Operations	
Improve the speed and consistency of CIP compliance audits.	Attachment 3 – II.B.2.b An important goal of RAI is to develop standard audit policies and procedures for all Regional Entities to serve as a common baseline approach to compliance audits. NERC and the Regional Entities have developed a standardized *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, to ensure consistent application of audit procedures across the ERO Enterprise and is now beginning auditor training on these tools.
Enhance the quality, consistency, and accessibility of compliance training.	Attachment 3 – II.B.2.b; *see also* II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders*)

[6] Attachment 3 to the *Five-Year ERO Performance Assessment Report* is titled *NERC Assessment of Regional Entity Delegated Functions*.

	Feedback from registered entities regarding training workshops has generally been positive. To address requests from the industry for an increased level of compliance information, many Regional Entities have committed more resources to training. Training activities during the assessment period have included in-person workshops, webinars, training videos and recordings, compliance update letters, on-site visits, and individualized outreach to registered entities.
Ensure that compliance audits are carried out in an efficient, accurate, consistent, and professional manner, and that the procedures and methodology followed by auditors are clear and ultimately useful to the registered entity.	Attachment 3 – II.B.1.c and d; II.B.2.b During the assessment period, NERC and the Regional Entities have increased training opportunities for Regional Entity audit staffs. Through RAI, NERC and the Regional Entities are working together to enhance the clarity and consistency of audit practices across the ERO Enterprise.
Better communicate to the registered entity how to become compliant.	Attachment 3 – II.B.2.a; *see also* II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders*); II.D.2.c.ii-iii – II.D.9.ii-iii (*Ensuring the Timely Mitigation of Violations / Promoting Reliability through Enforcement Philosophy and Practices*) In addition to workshops and webinars intended for a broad stakeholder audience, the Regional Entities offer individualized outreach opportunities to the registered entities within their regions to help facilitate compliance with Reliability Standards. Enforcement and mitigation staff at each Regional Entity also work with registered entities to develop and implement effective, appropriate mitigating activities to both address noncompliance and prevent recurrence.

Increase the quality and consistency of compliance-related IT applications.	Attachment 3 – II.B.2.b.ii-ix (*Compliance Monitoring Tools and Procedures / Maintaining Confidentiality*) The Regional Entities are currently exploring ways to enhance their compliance-related IT applications. Several Regional Entities have implemented enhancements, which are described in the individual assessments.
Streamline self-report and enforcement resolution processes.	Attachment 3 – II.D.1.a and b; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(C) The Regional Entities have worked with NERC to streamline enforcement processes during the assessment period. NERC and the Regional Entities developed and implemented streamlined enforcement processing mechanisms, such as the SNOP and FFT program, which allowed for a marked improvement in enforcement processing rates. Through regular communication and the oversight activities of NERC, NERC and the Regional Entities work to develop and share efficiency-enhancing process improvements. These improvements include the *ERO Self-Report User Guide* and the aggregation program, which were developed under RAI.
Better articulate the CIP Reliability Standards compliance and performance expectations.	Attachment 3 – II.B.2.a; *see also* II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders*); *Overview of NERC Activities and Accomplishments in the Five-Year Period* II.A.4. In addition to their regular training and outreach to registered entities, the Regional Entities are working with NERC to identify challenges and best practices for transitioning to Version 5 of the CIP Reliability Standards. The results of a transition implementation study will inform a report that will be broadly shared among industry and stakeholders.

Ensure that guidance tools like Case Notes, CARs, CANs, etc., are consistent and useful to registered entities, but do not become vehicles to reinterpret or revise Reliability Standards outside of the stakeholder process.	*Overview of NERC Activities and Accomplishments in the Five-Year Period* II.A.4 (*Development of Compliance Assessment Tools Concurrently with Reliability Standards Development*) NERC and Regional Entity staff are coordinating on the development of RSAWs as new Reliability Standards are developed. By creating a uniform understanding of compliance expectations for each Reliability Standard early in the standard development process, the need for interpretations or other forms of compliance guidance should be reduced. NERC has terminated the issuance of CANs as of February 2013.
Consider ways to improve the clarity and utility of RSAWs.	*Overview of NERC Activities and Accomplishments in the Five-Year Period* II.A.4 See response to immediately preceding comment.
Enforcement	
Increase transparency regarding the process by which penalties and sanctions are calculated and assigned, and the reasoning behind the calculation and assignment of those penalties and sanctions.	Attachment 3 – II.D.1.d, II.D.2.d-II.D.9.d (individual Regional Entity *Implementation of Various Aspects of the CMEP*) Each of the Regional Entities has taken steps to increase the transparency regarding its penalty determination processes through the assessment period. Each of the Regional Entities follows the NERC *Sanction Guidelines*, and each penalty is reviewed to ensure consistency with other penalties assessed across the ERO Enterprise for similar violations occurring under similar facts and circumstances.
Streamline and hasten the enforcement process so as to make it more efficient and reduce the cost burden on registered entities.	Attachment 3 – II.D.1.a-b; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(C)

	The Regional Entities have worked to streamline their enforcement processes during the assessment period. NERC and the Regional Entities developed and implemented streamlined enforcement processing mechanisms, such as SNOP and FFT, which allowed for a marked improvement in enforcement processing rates and reductions in caseloads. Through regular communication and the oversight activities of NERC, NERC and the Regional Entities work to develop and share efficiency-enhancing process improvements. These improvements include the *ERO Self-Report User Guide* and the aggregation program, which were developed under RAI.
Address the backlog in violation processing.	Attachment 3 – II.D.1.b.i-iii; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(C)(4) By the end of the assessment period, NERC and the Regional Entities processed over 99% of violations discovered from 2007 through 2011 (excluding on hold violations). NERC and the Regional Entities are working to achieve an objective that all violations are processed before reaching 24 months in age. Some Regional Entities achieved this objective as of the end of 2013.
Better communicate why violations occurred so registered entities can learn from them.	Attachment 3 – II.D.2.c.ii-iii–II.D.9.ii-iii (*Ensuring the Timely Mitigation of Violations / Promoting Reliability through Enforcement Philosophy and Practices*); II.B.2.a; *see also* II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders*) In the event a registered entity is found to be noncompliant with one or more Reliability Standards, Enforcement and Mitigation staff at the Regional Entity will work with the registered entity to develop and implement effective, appropriate mitigating activities to both address the noncompliance and prevent recurrence.

	Compliance and Enforcement staff at the Regional Entities also conduct workshops, webinars, and individualized outreach opportunities to help facilitate compliance with Reliability Standards.
Expand the use of FFTs.	Attachment 3 – II.D.1.b.iv; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(C)(1) In 2013, NERC and the Regional Entities worked together to expand the FFT program and implement certain enhancements approved by the Commission. As a result of these enhancements, FFT treatment is now available for a limited pool of possible violations posing a moderate risk to the reliability of the BPS (in addition to possible violations posing a minimal risk). In addition, certain unmitigated possible violations may be processed through the FFT program, so long as mitigation is completed within 90 days from the date the FFT is posted. Additional FFT enhancements may be implemented in the future under RAI.

Enhance consistency regarding enforcement processing across the regions.	Attachment 3 – II.D.1.b.vi; II.D.1.d; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(C)(4)(a)-(c) NERC and the Regional Entities engage in a number of activities to enhance consistency. For example, each of the Regional Entities have participated in RAI development activities and the multi-region working group on enforcement activities. In addition, NERC conducts oversight activities to facilitate the consistent application of streamlined enforcement processing mechanisms and other enforcement-related processes under the CMEP. Further, NERC and the Regional Entities take steps to promote reasonable consistency in the application of monetary penalties. Each penalty is reviewed to ensure consistency with other penalties assessed across the ERO Enterprise for similar violations occurring under similar facts and circumstances.
Registration and Certification	
Increase the clarity, regional consistency, quality, and overall efficiency of the CFR and JRO process.	Attachment 3 – II.A ; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II.B.1 The JRO and CFR mechanisms are important components of the NERC Organization Registration and Certification program. Amendments to the NERC Rules of Procedure during the assessment period have clarified the operations of both types of registration. In addition, the Regional Entities began using consistent registration forms during the assessment period. As of May 1, 2014, there are 34 JROs and 44 CFRs, which illustrates that numerous entities have been able to utilize these registration options.
Reduce redundancies in the registration and certification processes.	Attachment 3 – II.A ; *Overview of NERC Activities and Accomplishments In the Five-Year Period* II.B

Better communicate the requirements for certification and re-certification. Increase clarity and guidance surrounding how entities are registered by NERC, and respond timely to deregistration inquiries.	During the assessment period, the Regional Entities began using consistent registration forms. In addition, a Regional Entity working group developed a prototype "Common Registration Form" which will provide greater assurance that all entities that should be registered are in fact registered. Two initiatives are underway to improve registration and certification processes. The first pertains to multi-regional registered entities. The second is the risk-based registration effort, which will improve the efficiency with which a Regional Entity is able to process registration activation and deactivation requests.
Reliability Assessment & Performance Analysis Metrics	
Ensure that the Regional Entity self-assessments are consistent by using consistent criteria and trigger points.	Attachment 3 – III.B Each Regional Entity's self-assessment is distributed to Regional Entity members of the NERC Reliability Assessment Subcommittee (RAS) for an in-depth and comprehensive review of the data and information. Peer reviewer comments are discussed with Regional Entity and assessment area representatives, and refinements and adjustments are made, as needed. The Regional Entity self-assessments are then subjected to scrutiny and review by the entire RAS. This peer review process provides an essential check and balance to ensure the validity of the information provided for each assessment. It also provides a mechanism for the members of the RAS to become fully convinced that each Regional Entity self-assessment is accurate, thorough, and complete.
Training, Education, and Personnel Certification	
Increase the availability, quality, and accessibility of training regarding audit preparation and Reliability Standard compliance.	Attachment 3 – II.B.2.a; *see also* II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders*); *Overview of NERC Activities and Accomplishments in the Five-Year Period* II.C.2.a. To address requests from the industry for an increased level of compliance information, many

	Regional Entities have committed more resources to training and expanded their training offerings. Training activities during the assessment period have included in-person workshops, webinars, training videos and recordings, compliance update letters, on-site visits, and individualized outreach to registered entities. In addition, under RAI, the Regional Entities are working with NERC to develop and implement improvements to audit processes, including changes in the timing of preparation of RSAWs and development of a common *Compliance Auditor Checklist* and *Compliance Auditor Handbook*, as found in the *ERO Enterprise Compliance Auditor Manual*, which was made available to industry. These improvements provide additional insight for registered entities into how they will be audited and what they can do to prepare.
Event Analysis	
Increase the speed by which Event Analysis information (including lessons learned) is disseminated.	Attachment 3 – IV.A; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(D)(3) In June 2010, NERC and the Regional Entities created the NERC Event Analysis Working Group (EAWG). The EAWG expended significant efforts to develop an ERO Event Analysis process for use across North America. By integrating industry engagement and the collaborative review of disturbances into the ERO Event Analysis process, the effectiveness, predictability, consistency, and timeliness of the program was increased. Several lessons learned have already been shared with industry. The Event Analysis process is resulting in faster dissemination of information and lessons learned from outage events and other system disturbances than had been occurring through compliance investigations.
Improve the quality of disseminated Event Analysis information by showing relative	Attachment 3 – IV.C

and key emerging risks based on data analyzed through Event Analysis processes and by releasing more meaningful lessons learned.	NERC is considering improvements to increase the timeliness, transparency, and comprehensiveness of dissemination of information relating to Event Analysis and lessons learned.
Better coordinate information requests when NERC and a Regional Entity are involved in an event investigation.	Attachment 3 – IV.C In response to suggestions received during the ERO Event Analysis annual review, NERC is exploring potential solutions (including the possibility of implementing enterprise IT systems) to provide efficiencies in Event Analysis and related reporting processes.
Increase the effectiveness and efficiency of ERO-wide Event Analysis communications, particularly as to when an event is closed out.	Attachment 3 – IV.A; *Overview of NERC Activities and Accomplishments in the Five-Year Period* II(D)(3) NERC and the Regional Entities are continuously refining the ERO Event Analysis process based on experience and as system conditions change.
Stakeholder Communications, Public Relations, and IT	
Make Regional Entity websites more accessible, user-friendly, secure, and useful to registered entities.	Attachment 3 – II.B.2.b.ii-ix (*Guidance and Training for Industry Stakeholders / Maintaining Confidentiality*) The Regional Entities post a number of compliance and technical materials to assist registered entities in their compliance program implementation. In addition, the Regional Entities use encryption and other methods to ensure that information submitted through Regional Entity websites is secure.
Business Plan and Budget	
Increase transparency regarding the funding mechanisms for Regional Entities when they undergo reorganization.	Attachment 3 – V.B. NERC and the Regional Entities have continuously striven for improved transparency and detail in the business plans and budgets. Numerous improvements have been implemented in this regard. To provide ongoing, collaborative oversight of the business planning,

	budgeting, accounting, and financial reporting processes, NERC and the Regional Entities have formed an ERO Finance Group comprised of representatives of NERC and each Regional Entity.

Table 3: Overview of Five-Year and Three-Year Survey

The following table provides comparative statistics concerning the stakeholder survey that was taken in connection with the preparation of the *Three-Year ERO Performance Assessment Report*, in 2009, and the stakeholder survey that was taken in late 2013 in connection with the preparation of this *Five-Year ERO Performance Assessment Report*.

Five-Year Survey	Three-Year Survey
326 registered entity responses	128 registered entity responses
0 trade association or organized group responses	5 trade association or organized group responses
0 regulator, state, provincial, federal or other responses	3 regulator, state, provincial, federal or other responses
0 reliability stakeholder or public responses	6 reliability stakeholder or public responses

Table 4: Stakeholder Average Scores

The remainder of this Attachment summarizes information from the stakeholder survey conducted in October 2013.

Regional Entity	Response Rate (%)	Total Number of Responses	Total Unique NCR IDs
FRCC	33	23	69
MRO	28	38	135
NPCC	21	62	301
RF	22	75	343
SERC	32	74	233
SPP RE	27	39	145
TRE	20	46	225
WECC	20	97	477

Reliability Standards Questions					
	1. Develops Reliability Standards that indicate which BPS owners, operators and users must comply with individual requirements	2. Develops Reliability Standards that have a sound basis in engineering and operations	3. Develops and modifies Reliability Standards in a timely manner giving consideration to the prioritization of reliability objectives	4. Develops an annual *Reliability Standards Development Plan* that is an effective tool to communicate and gather stakeholder input to the proposed scope of work, schedules, and priorities for developing and	5. Communicates information about Reliability Standards, their development, and opportunities for stakeholder participation in an efficient and

				revising Reliability Standards	effective manner
Average Score					
NERC	4.0	3.3	3.2	4	3.8

Compliance Operations Questions					
	1. Provides accessible information about the level of performance necessary to comply with requirements of applicable Reliability Standards	2. Provides accessible information about what documentation and other evidence is needed to demonstrate compliance	3. Conducts audits, investigations, spot-checks and other compliance monitoring methods in a professional, thorough, and efficient manner	4. Utilizes electronic tools and forms that provide for clear, effective, and efficient submittal and handling of compliance information	5. Encourages registered entities to conduct internal self-assessments of compliance and self-report possible violations
Average Score					
NERC	2.1	1.8	1.6	1.4	3.3
FRCC	3.2	3.1	3.7	3.5	4.2
MRO	3.3	3.3	3.8	3.7	4.1
NPCC	3.8	3.6	4.0	4.0	4.2
RF	3.6	3.6	3.6	3.9	4.0
SERC	3.7	3.5	4.1	3.9	4.2
SPP RE	3.4	3.3	3.4	3.6	3.8
TRE	3.7	3.6	4.0	4.0	4.1
WECC	3.6	3.6	3.9	3.8	4.1

Enforcement Questions			
	1. Ensures that possible violations are investigated, assessed and closed in a timely manner	2. Levies penalties and sanctions for the violation of a Reliability Standard that bear a reasonable relation to the risk to reliability the violation presents	3. Levies penalties and sanctions that reflect consideration of the other factors specified in the *Sanction Guidelines*
Average Score			
NERC	1.7	2.1	2.3
FRCC	3.5	3.6	3.4
MRO	2.9	2.8	2.9
NPCC	2.8	2.7	2.8
RF	3.2	3.1	3.2
SERC	2.9	3.2	3.2

SPP RE	2.9	2.4	2.4
TRE	3.2	3.1	3.2
WECC	3.1	2.8	2.8

Registration and Certification Questions			
	1. Establishes adequate criteria to determine which owners, operators, and users of the BPS perform certain reliability functions and should therefore be registered as responsible for complying with Reliability Standards applicable to those reliability functions	2. Has a registration process that is effective in addressing situations in which compliance responsibilities are shared or delegated among entities, such as through the use of CFR or JRO	3. Conducts inquiries in a professional, thorough, and efficient manner for entities applying or submitting changes for certification as Reliability Coordinators, Balancing Authorities, and/or Transmission Operators
Average Score			
NERC	2.5	2.6	1.2
FRCC		3.5	3.2
MRO		3.4	2.8
NPCC		3.3	3.0
RF		3.3	2.8
SERC		3.4	2.5
SPP RE		3.2	2.5
TRE		3.3	2.5
WECC		2.6	2.6

Reliability Assessment Questions		
	1. Effectively communicates reliability assessments to stakeholders, policy makers, and the public, to explain why certain actions are necessary or appropriate to ensure future adequacy and reliability of the BPS	2. Effectively reports on regional self-assessments of electric supply and bulk power transmission reliability, including emerging and long-term reliability issues of specific regional and North American concern
Average Score		
NERC	2.4	2.2

Performance Analysis and Metrics Questions		
	1. Compiles and publishes useful information on performance metrics and benchmarks to observe and understand trends in the reliability and performance of the BPS and in the reliability performance of users, owners and operators, and to highlight areas for potential improvements	2. Identifies reliability performance issues for consideration in the development or modification of Reliability Standards
Average Score		
NERC	2.7	2.7

Training, Education, and Personnel Certification Questions			
	1. Provides effective training to registered entities on complying with Reliability Standards	2. Provides effective training on how to demonstrate compliance to auditors	3. Has an effective program for issuing certification credentials to skilled, trained, and qualified BPS operators, and for the maintenance of those certification credentials
Average Score			
NERC	2	1.8	2.9
FRCC	3.7	3.6	
MRO	3.2	2.9	
NPCC	3.5	3.4	
RF	3.4	3.1	
SERC	3.6	3.4	
SPP RE	3.5	3.4	
TRE	3.8	3.5	
WECC	3.8	3.4	

Event Analysis Questions				
	1. Develops and disseminates timely and useful information about system events and specific reliability risks affecting reliable operation of BPS through the lessons learned processes	2. Effectively uses the Alert Level 2 (Recommendations) and Level 3 (Essential Actions) under Rules of Procedure Section 810 to effectively track specific reliability risks affecting the reliable operation of the BPS	3. Has an Event Analysis program that provides and supports analysis on reliability risks that is useful to the industry and focused on BPS reliability	4. Investigates and analyzes events in an efficient manner, appropriate to the severity of the event
Average Score				
NERC	2.3	1.4	2.7	2.7

FRCC	3.6		3.4	3.3
MRO	3.0		2.9	2.8
NPCC	3.3		3.3	3.4
RF	3.3		3.0	3.1
SERC	3.5		3.3	3.2
SPP RE	3.2		3.1	2.8
TRE	3.6		3.5	3.5
WECC	3.2		3.0	2.9

Critical Infrastructure Protection Questions		
	1. Serves as an effective leader and facilitator of the industry's efforts to identify and protect BPS critical infrastructure, including by identifying and publicizing threats to critical infrastructure	2. Provides cybersecurity alerts that are effective for notifying BPS owners, operators, and users of vulnerabilities and actions to address those vulnerabilities
Average Score		
NERC	2.3	1.7

Stakeholder Communications, Public Relations, and IT Questions			
	1. Provides a public website that is useful in meeting stakeholder needs and provides easy access to information	2. Provides newsletters, conferences, and other stakeholder communications that are effective in providing stakeholders with useful and timely information regarding reliability and ERO/Regional Entity activities	3. Provides effective outreach to all jurisdictional stakeholders, including smaller entities with limited ability to travel to meetings and conferences
Average Score			
NERC	3.3	4.1	3.9
FRCC	3.4	3.6	3.3
MRO	3.4	3.9	3.6
NPCC	3.6	3.8	3.4
RF	3.6	3.9	3.4
SERC	3.6	3.9	3.9
SPP RE	3.4	3.6	3.4
TRE	3.9	3.9	3.8
WECC	3.6	3.9	3.7

Business Plan and Budget Questions		
	1. Provides reasonable opportunity for members and other stakeholders to provide	2. Provides sufficient financial information in support of its business plan and budget and its

	input in the annual business plan and budgeting process	quarterly and annual financial reporting
Average Score		
NERC	2.4	2
FRCC	2.9	2.9
MRO	3.2	3.1
NPCC	2.8	2.7
RF	3.2	3.0
SERC	3.5	3.3
SPP RE	2.8	2.7
TRE	3.4	3.3
WECC	3.0	2.9

Independence and Stakeholder Input Questions				
	1. Retains staff that are independent of BPS owners, operators and users and responsive to the needs of reliability stakeholders	2. Effectively communicates a vision and expectations and provides effective leadership to achieve that vision consistent with the *ERO Enterprise Strategic Plan*	3. Performs statutory functions in a transparent manner with adequate opportunity for stakeholder input	4. Provides fair stakeholder representation in the selection of directors and other decision-making in committees or other subordinate organizational structures
Average Score				
NERC	3.8	2.3	3.7	3

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 5

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

STATUS OF AREAS FOR IMPROVEMENT IDENTIFIED IN THE ORDER ON THE THREE-YEAR ERO PERFORMANCE ASSESSMENT

JULY 21, 2014

Attachment 5: Status of Areas for Improvement Identified in the Order on the Three-Year ERO Performance Assessment

Citation to Order on the Three-Year ERO Performance Assessment (¶)	Areas for Improvement	Status Update[1]
100-102	Believes that NERC (along with its stakeholders) should prioritize those Reliability Standards projects that, in its expert judgment, are the most critical to the reliability of the Bulk-Power System (BPS).	The NERC Board of Trustees has established the Reliability Issues Steering Committee (RISC) to set priorities on issues of importance to the BPS, including the development of Reliability Standards. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, page 28.
104	Reach out to registered entities to provide expert volunteers on Reliability Standards drafting teams and continue streamlining NERC's procedure to aid in reducing the strain on industry resources overall.	NERC has increased focus on outreach to stakeholders for participation in the Reliability Standards development process. At the end of May 2014, 858 stakeholder representatives had registered their eligibility to vote on proposed Reliability Standards as members of the Registered Ballot Body, and in 2013 alone NERC hosted 43 Reliability Standard industry webinars attended by an average of 360 participants. During the last six months of 2013, standard drafting teams (SDTs) and five-year review teams made up of 195 industry volunteers participated in 60 team meetings to advance Reliability Standards development activities. NERC has also made revisions to the *Standard Processes Manual*, which were approved by the Commission on June 26, 2013. These revisions have, among other things, led to a substantial decrease in the time required to revise an existing Reliability Standard or to develop a new one. This reduction in time provides registered entities with increased flexibility in staffing SDTs due to the reduced time commitment.

		See Overview of NERC Activities and Accomplishments in the Five-Year Period, pages 5, 25.
108	NERC must clearly demonstrate that any proposed elimination of a requirement does not diminish the reliability and enforceability of the existing Reliability Standard.	In the first quarter of 2013, NERC assembled the Reliability Standards Independent Experts Review Panel (IERP) consisting of five independent industry experts and a sixth participant from the Commission. At the end of its review in August 2013, the IERP recommended (among other things) the retirement of 147 existing Requirements of Reliability Standards. In making this determination, the IERP assessed whether a requirement: (i) did not support a reliability principle; (ii) met the Paragraph 81 criteria for retirement; or (iii) was better suited as a guideline rather than as a part of a Reliability Standard. The IERP's recommendations set the course for delivering high quality, results-based Reliability Standards with sustainable requirements. For the remaining requirements that the IERP did not recommend for retirement, the IERP applied content and quality criteria to examine whether they were steady-state or needed additional work. The IERP evaluated whether these remaining requirements addressed a risk to reliability by examining: (i) the ranking developed by the NERC RISC; (ii) the violation risk factor (VRF) for each requirement; and (iii) the IERP members' own professional judgment The P 81 initiative identified three layers of criteria to determine whether a requirement should be recommended for retirement. These criteria were identified in a technical

[1] Status update references made to previous sections of this *Five-Year ERO Performance Report* include: (i) *Overview of NERC Activities and Accomplishments in the Five-Year Period*; (ii) Attachment 1: *Discussion of How NERC Meets the ERO Certification Criteria of 18 C.F.R. §39.3(b);* and (iii) Attachment 3: *NERC Assessment of Regional Entity Delegated Functions.*

		whitepaper dated December 20, 2012. The Commission issued an order on November 21, 2013 approving the retirement of 34 Requirements and sub-Requirements within 19 Reliability Standards. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 14-17, 17-19.
103	NERC and the Regional Entities should also plan to complete the fill-in-the-blank Reliability Standards, which remain pending from Order No. 693. We agree with NERC that setting priorities regarding fill-in-the-blank standards is an issue that should be resolved jointly by NERC and the Regional Entities.	NERC and the Regional Entities have determined that replacing the fill-in-the-blank Reliability Standards with continent-wide Reliability Standards is the optimal approach to addressing outstanding fill-in-the-blank Reliability Standards. NERC has been steadily working to complete revisions to replace fill-in-the-blank Reliability Standards with continent-wide versions. These revisions have been completed for Reliability Standards in four areas: (1) Emergency planning for system restoration and blackstart; (2) Data for steady state and dynamic system modeling; (3) Transfer capability requirements; and (4) Underfrequency load-shedding programs. Revisions are in progress at the time of this writing for Reliability Standards in five additional areas: (1) Analysis and mitigation of protection system misoperations (two projects, one scheduled for completion in 2014 and one in 2015); (2) Undervoltage load-shedding (scheduled for completion in early 2015); (3) Facility connection requirements (scheduled for completion in 2014);

		(4) Disturbance monitoring (scheduled for completion in 2014); and (5) Data for modeling demand (scheduled for completion in 2014). Once these in-progress projects are completed, all of the fill-in-the-blank Reliability Standards will have been revised through a Commission-approved standards development process.
85	Renews the directive that NERC submit quarterly reports on Reliability Standards development for an additional three years, with additional detail of required analysis. The quarterly reports should include: (i) the time required to complete projects; (ii) the time required to complete projects initiated in response to NERC's urgent action progress; and (iii) the time required to complete projects in response to Commission directives. The analysis should include data on the time required for each stage of the process.	NERC has been filing quarterly analyses of Reliability Standards voting results in Docket No. RR06-1 since May 2007. NERC continued to file these quarterly reports, including the additional information directed in the Order on the Three-Year ERO Performance Assessment, through and including the fourth quarter of 2013.
107-112	The Commission provided guidance regarding NERC's initiative to transition to results-based Reliability Standards. 107-108: the revised Reliability Standards should incorporate the Commission's	During the assessment period, NERC launched several initiatives designed to evolve the Reliability Standards into "steady-state," which means a stable set of clear, concise, high-quality, and technically sound Reliability Standards. Several important components of this evolution are: (i) the results-based Reliability Standards initiative; (ii) the P 81

	directives from prior orders that address the substantive performance goals of the BPS. 109: expanded background sections, purpose sections, or explanations of intent, should not contradict or seek to supersede or interpret the requirements within a Reliability Standard. 110: a requirement cannot be retired without its associated reliability benefit being addressed fully in another requirement or Standard. 111: revised Reliability Standards should include objective language rather than subjective modifiers, and should not include language requiring NERC or a Regional Entity to assess whether a registered entity intended to violate a Standard, nor whether a registered entity failed to perform due to, for example, negligence or human error. 112: revised Reliability Standards should not reduce BPS reliability from that which would be required by the existing approved Standards.	project; (iii) changes to the *Standard Processes Manual*; (iv) reorganization of the NERC Standards department; and (v) the work of the IERP. 107-108: Addressing Commission directives relating to Reliability Standards is a major priority to facilitate the transformation to steady-state Reliability Standards. As of December 2012, there were 191 outstanding Commission directives that were related to Reliability Standards development. More than half of the total number of Commission-issued directives were addressed during 2013. At the February 2014 meeting of the NERC Standards Oversight and Technology Committee (SOTC), it was reported that 128 directives had been addressed by the end of 2013, with 107 remaining. NERC anticipates that 90% of Commission directives issued to date will be resolved between the end of 2014 and the first half of 2015. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, page 12. 109: The NERC *Standard Processes Manual* explicitly states that "[t]he only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

		See Section 2.5 of the NERC *Standard Processes Manual*, Appendix 3A to the NERC Rules of Procedure. 110: The IERP works in conjunction with the RISC to ensure requirements are not recommended for retirement so as to leave gaps in reliability. Additionally, NERC systematically manages the development of new Reliability Standards and revisions to standards, in areas of highest need and importance, through its rolling three-year *Reliability Standards Development Plan* (RSDP). The RSDP is revised annually and identifies and prioritizes Reliability Standards development projects in the immediate three-year time horizon, taking into account, among other information, perceived gaps in the Reliability Standards, proposals for closing those gaps, and timing priorities for standards development projects. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 14-17, 85. 111: The IERP applies content and quality criteria when assessing whether standards are steady-state or need revisions. Additionally, Section 4.6 of the NERC *Standard Processes Manual* requires that NERC Standards staff conduct a quality review of the Reliability Standard, implementation plan, and VRFs and violation severity level (VSLs) in parallel with the development of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated standard authorization request (SAR), whether

		the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval of Reliability Standards. Item #4 of NERC's *Ten Benchmarks of an Excellent Reliability Standard* requires that "[e]ach performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area. 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." *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 15-16; Section 4.6 of the NERC *Standard Processes Manual*, Appendix 3A to the NERC Rules of Procedure; and *Ten Benchmarks of an Excellent Reliability Standard*, available at: http://www.nerc.com/pa/Stand/Resources/Documents/10BenchmarksofExcellentReliabilityStandards.pdf. 112: Section 4.6 of the NERC *Standard Processes Manual* requires that NERC Standards staff conduct a quality review of the Reliability Standard, implementation plan, and VRFs and VSLs in parallel with the development or modification of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated SAR, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for

		Excellent Standards and criteria for governmental approval of Reliability Standards. *See* Section 4.6 of the *NERC Standard Processes Manual*, Appendix 3A to the NERC Rules of Procedure.
102	NERC should determine whether there are new or modified Reliability Standards that would address identified gaps that may belong in the high priority group.	Two of the recommendations made by the IERP when it presented its report to the NERC Board of Trustees in August 2013 were that NERC address seven areas (high-level gaps) not currently addressed by the Reliability Standards, and complete standards development projects to address gaps within individual requirements. The IERP also made recommendations regarding compliance monitoring, prioritization for addressing the identified gaps, using risk to determine whether a future standard is needed, and use of the IERP's identified criteria to determine the quality and content as future standards are developed. The potential reliability gaps identified by the IERP were evaluated by the RISC and assigned in some cases to active drafting projects. The IERP recommendations that apply to Reliability Standards that were not part of active drafting projects were assigned to teams that conduct periodic reviews of Reliability Standards in the future for consideration. Additionally, NERC systematically manages the development of new Reliability Standards and revisions to Reliability Standards, in areas of highest need and importance, through its rolling three-year RSDP. The RSDP is revised annually and identifies and prioritizes Reliability Standards development projects in the immediate three-year time horizon, taking into account, among other information, perceived gaps in the Reliability Standards, proposals for

		closing those gaps, and timing priorities for standards development projects. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 15-17, 85.
74	Urge NERC to take measures, including hiring staff with the technical capability to independently advise the NERC Board of Trustees regarding the substantive content of a proposed Reliability Standard.	Although much of the work in the Reliability Standards development process is performed by committees and task groups comprised of volunteer technical experts, significant NERC professional staff resources are needed to facilitate and coordinate the work of industry volunteers, to administer the process and help ensure that it functions efficiently, and to provide input to support development of technically sound standards. NERC has budgeted 25.92 full-time equivalents (FTEs) for the Reliability Standards Program for 2014, which is a slight decrease of 0.58 FTEs from the 2013 budget and reflects the application of the 4% personnel attrition. In accordance with its 2013 business plan and budget, NERC has added 3 positions in the Reliability Standards Program in 2013. NERC has improved the composition of SDTs by enhancing the selection process to identify, for each project, the necessary technical, writing, and project management expertise to form a balanced team that will foster improved effectiveness and enhanced efficiency. In addition, SDTs now receive increased NERC staff support, including dedicated legal support for each project. Each standard development project is staffed by a lead standard developer, and many projects have a second supporting standard developer. Standard developers provide project management and facilitation experience as well as additional skills,

		including technical writing, legal skills, and outreach/ consensus-building skills, to the SDT, which contributes to the development of high-quality Reliability Standards. Additionally, Section 4.6 of the NERC *Standard Processes Manual* requires that NERC Standards staff conduct a quality review of the Reliability Standard, implementation plan, and VRFs and VSLs in parallel with the development of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated SAR, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval of Reliability Standards. Item #5 of NERC's *Ten Benchmarks of an Excellent Reliability Standard* requires that "[e]ach reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in the particular field." *See NERC 2014 Request for Acceptance of Business Plan and Budget*, page 42, Docket No. RR13-9-000; *Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 31-32; Section 4.6 of the NERC *Standard Processes Manual*, Appendix 3A to the NERC Rules of Procedure; and *Ten Benchmarks of an Excellent Reliability Standard*, available at: http://www.nerc.com/pa/Stand/Resources/Documents/10BenchmarksofExcellentReliabilityStandards.pdf.
152	Encourages NERC to intensify its efforts to provide additional oversight and guidelines to	

	assist registered entities in accurately determining that an asset is critical to the BPS (critical cyber asset identification).	The CIP Version 4 and 5 Reliability Standards move away from the use of the registered entities' risk-based assessment methodology in the identification of critical cyber assets. In Order No. 791, the Commission approved NERC's proposed implementation plan for CIP Version 5 to bypass CIP Version 4 and move directly to CIP Version 5. Recognizing that registered entities are in various stages of implementation of CIP Versions 3 and 4, NERC addressed the need for flexibility as well as the need to identify and address the associated transition challenges for the industry through guidance. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 34-36; and *Cybersecurity Standards Transition Guidance*, available at: http://www.nerc.com/pa/comp/Resources/ResourcesDL/Cyber%20Security%20Standards%20Transition%20Guidance%20(Revised).pdf.
154	NERC's proposed action item for "fast-track" interpretations of CIP Reliability Standards lacks specificity. NERC states that this process would not require implementation of the full existing Reliability Standards development process, and could improve efficiency without sacrificing quality, but otherwise NERC does not provide any details how it would implement this proposal. While we support efforts to provide greater guidance on CIP	A CIP-specific fast-track process for interpretations of CIP Reliability Standards has not been developed during the assessment period. However, the revisions to the *Standard Processes Manual* approved by the Commission on June 26, 2013, included a waiver provision that allows for modifications to the Reliability Standards development process for good cause, with five days' notice and reporting of the exercise of a waiver to the NERC SOTC. This waiver provision could be used to fast-track the development of an interpretation of a Reliability Standard, including a CIP Reliability Standard.

	implementation, we are concerned whether "fast track" interpretations will provide the consistency, clarity and transparency for meaningful assistance to entities that must comply with the CIP Reliability Standards. If NERC develops this proposal, NERC should submit it to the Commission for review, possibly in the form of a petition for approval of modifications to NERC's Rules of Procedure.	*See Overview of NERC Activities and Accomplishments in the Five-Year Period*, page 24.
169	Regarding Event Analysis, directs NERC to establish criteria it will use to select a subset of events, which should focus on those with the highest impact to reliability, to provide important "lessons learned" and submit the criteria in the informational report.	NERC has developed a voluntary Event Analysis process, including criteria to categorize events, that delivers quality, timely and actionable lessons learned to registered entities. Development of the Event Analysis process was led by the Event Analysis Subcommittee (EAS), a cross-functional group of industry experts. The Event Analysis process begins with a registered entity making an initial assessment of an occurrence and determining if the occurrence falls within one of five qualifying event categories. The event category is determined by weighing the level of significance of a qualifying event and its impact on the interconnected BPS. After a qualifying event occurs, the applicable Regional Entity holds a planning meeting with all involved parties, including other registered entities. If a qualifying event is categorized as Category 3 or higher, the registered entity will prepare an Event Analysis Report (EAR), in which the registered entity describes the sequence of events and identifies causal factors and appropriate corrective actions. The registered entity then submits the EAR to the applicable Regional Entity or Entities for review, and then to NERC.

		The registered entity, in collaboration with the ERO, drafts the proposed lessons learned from the event and submits them to the applicable Regional Entity. Once the event analysis is complete, NERC shares any lessons learned with industry by publishing them as soon as practical. NERC staff analyzes EARs to identify reliability risks, trends, and potential gaps in Reliability Standards, compliance, and other programs. NERC also reviews the EARs to assign descriptive cause codes, which assist in identifying trends and corrective actions that will prevent recurrence of similar events. Since initial implementation of the Event Analysis process in 2010, there have been more than 388 qualified events reported to the ERO and more than 77 lessons learned, including 14 published in 2013. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 68-71.

170-171, 173-178	170: Directs NERC to work with the Regional Entities to ensure that they provide to Commission staff sufficient and timely information on each event. NERC must report on steps it will take to implement this directive in the informational report. 171: Directs NERC to develop communication protocols between NERC, the Commission and the Regional Entities for use during events and report on its progress in the informational filing. 174: If a Compliance Violation Investigation (CVI) is initiated, it should be conducted concurrently with an Event Analysis and both processes should begin as soon as possible to the extent necessary. 175: maintain the respective focuses of the CVI and Event Analysis to ensure independence of the roles each mechanism is designed to fulfill. 176: In order to create more efficiency in the event analysis and CVI processes, all event analysis materials obtained by the event analysis team, including requests for information and responses, should be sent, at the same time as issued or collected, to the	170 - 171: NERC staff compiles and provides a daily summary of newly reported qualifying events to FERC staff, NERC's Event Investigation group under Compliance Operations, and Regional Entity situational awareness and event analysis points of contact. Event status is reviewed in a biweekly conference with NERC and FERC staff, and in a separate weekly conference call with NERC and Regional Entity staff. 174 - 178: Compliance Investigations (formerly CVIs) are governed by Section 3.4 of the *Compliance Monitoring and Enforcement Program* (CMEP), Appendix 4C to the NERC Rules of Procedure. Event Analysis is governed by Sections 807 and 808 of the NERC Rules of Procedure, along with Appendix 8. These are two separate processes within NERC. Additionally, widespread use of mechanisms like the voluntary Event Analysis process has in practice greatly reduced the need to initiate formal Compliance Investigations following events. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 68-71.

	compliance staff in each applicable Regional Entity and to NERC compliance staff. These materials, insofar as they relate to a U.S. registered entity, also should be available to Commission staff upon request. 177: Any communication between an event analysis team and a corresponding CVI team generally should be one-way only: from the event analysis team to the CVI team. An exception to this practice would be appropriate only for factual information collected by a CVI team that bears on an important industry advisory that the event analysis team would make (or recommend that NERC make) as part of an initial event analysis determination. 178: NERC shall report on the steps it has taken to clarify the interface between event analyses and compliance activities, including Compliance Investigations, in response to the Commission's guidance in the informational filing.	
126	Directs NERC to continue its oversight of Regional Entity audits with NERC staff that are technically proficient.	As outlined in the NERC Rules of Procedure and the Regional Entity Delegation Agreements, NERC is responsible for oversight of the Regional Entities compliance monitoring program. NERC restructured its oversight process to include a participatory role during Regional Entity compliance. In addition to oversight engagements, NERC has developed the Key Reliability Standard Spot Check (KRSSC), performs

		capability assessments of the Regional Entities, reviews reports submitted by the Regional Entities and conducts two workshops per year in addition to other auditor and lead auditor training. The KRSSC is a study of a single Reliability Standard and a sampling multiple audits across all eight Regional Entities to determine consistency of approach. The results of the study are then provided to the regions to identify improvement opportunities. Starting in 2012, NERC began the process of reviewing the background, education and credentials of the regional compliance auditors and providing feedback to Regional Entities. NERC reads each audit report submitted by the Regional Entities prior to posting to FERC. NERC conducts auditor workshops, performs lead auditor training and provides resources to enhance the consistency of auditor practices across the Regional Entities as well as to improve the technical proficiency of those NERC staff that provide oversight of the Regional Entities' compliance monitoring activities. Finally, NERC participates in the ERO and Compliance and Enforcement Management Group (ECEMG) on a monthly basis where audit activities and projects that improve audit processes and identify opportunities to drive consistency are discussed. *See also* Sections 402 and 403 of the NERC Rules of Procedure; and Attachment 3, pages 16-21.
127	Directs NERC and Regional Entities to have their staff, and Commission staff where applicable, discuss the appropriate role of	Section 3.1.5.3 of the CMEP defines who may participate as an observer in a Regional Entity compliance audit of a Registered Entity. This section also stipulates that

	observers during their pre-audit meetings or conferences.	"Compliance Audit observers and attendees are not Compliance Audit team members and do not participate in conducting the Compliance Audit or in making Compliance Audit findings and determinations." *See* Section 3.1.5.3 of the CMEP, Appendix 4C to the NERC Rules of Procedure.
220	Direct NERC to explain how it would implement risk-based approaches to compliance activities and at the same time complete its currently-required audit cycles.	A key, strategic transformation that NERC, in collaboration with the Regional Entities and stakeholders, embarked upon during the assessment period is the construction of a risk-based model for compliance monitoring and enforcement. This risk-based approach enables NERC to focus ERO and industry resource investment on the most important issues to BPS reliability. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 50-62.
153	NERC should ensure that there is quality, uniformity and consistency amongst the Regional Entities when conducting compliance audits and spot checks relating to CIP Reliability Standards. NERC should consider the worthiness of an ongoing "accreditation" of qualified auditor candidates through continued education. A program that establishes the requisite level of knowledge and skills needed to maintain necessary levels of technical expertise on a continuous basis should be the goal of the CIP	The NERC CIP audit staff works closely with the Regional Entity CIP staff and provides guidance to the ERO CIP Auditors. NERC provided direct feedback in the past on audit reports and has participated in post-audit phone calls to review best practices, lessons learned and staff qualifications. In order to share best practices and promote consistency, NERC has utilized Regional Entity working groups such as the CIP Compliance Working Group (CCWG) and the ECEMG to discuss technical and policy CIP issues. *See also Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 53-54, 61-62, for a discussion of the *ERO Enterprise Compliance Auditor Manual*, which

	audit program. These qualifications should be designed to verify the knowledge and skills of the auditor in the area of CIP, control systems and information technology.	includes the *Compliance Auditor Handbook* and *Compliance Auditor Checklist*, as well as auditor qualifications.
118	We suggest that NERC and Regional Entities consider providing ongoing training for their compliance auditors on effective auditing techniques. We expect that NERC's establishment of a Regional Operations Group that focuses on auditors will rapidly improve audit consistency and performance.	As part of its Compliance Operations function, NERC is responsible for supporting the development of qualified and trained compliance operations and auditing staffs at both NERC and the Regional Entities. In addition to the development of a common set of auditor qualifications, NERC ensures the proper qualifications of personnel for auditing and other essential compliance roles through training. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, page 62.
121	Encourages NERC to continually review its RSAWs to improve their quality and usefulness.	Prior to 2013, NERC developed RSAWs after regulatory approval of a Reliability Standard and at least six months before the Reliability Standard's enforcement date. Today, RSAWs are written concurrently with new Reliability Standard development projects. Each Reliability Standards project is assigned dedicated staff support and led by compliance. NERC compliance staff are coordinating with Regional Entity staff. This increased and ongoing coordination will help ensure that standard drafting teams, compliance staff and RSAWs are aligned with the intent of Reliability Standards, thereby increasing the quality and usefulness of these documents *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 19-21.

180	Directs NERC to continue developing scenario analysis in the long-term reliability assessments. The Commission requires NERC to update its reliability assessment protocols to establish a requirement for an annual scenario analysis and to file this update in the informational filing.	The latest version of the NERC *Reliability Assessment Guidebook* is version 3.1 (dated August 2012). This version was approved by the NERC Planning Committee in June 2012. *See* http://www.nerc.com/comm/PC/Pages/Reliability%20Assessment%20Subcommittee%20(RAS)/Reliability-Assessment-Guidebook.aspx. This version makes more explicit the requirement for an annual scenario analysis to be included in all future long-term reliability assessment (LTRA) reports. Since 2009, the following LTRAs include scenario analyses: • *2009 Long-Term Reliability Assessment* • *2010 Long-Term Reliability Assessmen*t • *2011 Long-Term Reliability Assessment* • *2012 Long-Term Reliability Assessment* Additional scenarios completed as part of the Reliability Assessment program in support of the LTRA: • *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf. • *2011 Potential Impacts of Future Environmental Regulations:* http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/EPA%20Section.pdf.

		• *2010 Special Reliability Scenario Assessment: Resource Adequacy Impacts of Potential U.S. Environmental Regulations:* http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/EPA_Scenario_Final_v2.pdf. • *2010 Special Reliability Scenario Assessment: Potential Reliability Impacts of Swift Demand Growth After a Long-Term Recession:* http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Swift_Scenario_Aug_2010.pdf. • *2010 Reliability Impacts of Climate Change Initiatives: Technology Assessment and Scenario Development:* http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/RICCI_2010.pdf. *See also Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 71-73.
183	Directs NERC to develop a plan to address capacity and energy in its reliability assessment methodology and a timeline for executing the plan, and submit the plan and timeline as part of the 2011 LTRA and file its preliminary plan and timeline in the informational filing.	NERC implemented probabilistic assessments in the LTRA in 2012 with a trial phase based on voluntary participation occurring in 2011. A detailed plan was included in the 2011 LTRA. In summary, the plan includes the following milestone dates: (1) Request for participation in voluntary trial period (March 2011); (2) Draft methods due to NERC (May 2011); (3) Results of 2011 study (October 2011); (4) Trial view complete (March 2012);

		(5) 2011 trial results to be included in 2012 LTRA (October 2012); (6) Request for full participation (March 2012); and (7) 2012 results to be included in 2013 LTRA (October 2013). Additionally, appropriate modifications were made to NERC's *Reliability Assessment Guidebook* to reflect these changes in the reliability assessment process. NERC completed the "Pilot" assessment in July 2011. *See* NERC's *Pilot Probabilistic Assessment* (dated June 2012), available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2012_ProbA.pdf. NERC completed the first NERC-wide probabilistic study using the 2012 LTRA reference case in June 2013. *See NERC Probabilistic Assessment*, available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_2012_Probabilistic_Assessment_Final.pdf. These probabilistic assessments will be completed on a biannual basis. *See* NERC's *2013 Long-Term Reliability Assessment* published in December 2013, available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2013_LTRA_FINAL.pdf.
185	Directs NERC to consider establishing permanent databases that could be automatically populated with: (i) new	NERC and the Regional Entities are working on the development of the Reliability Assessment Data System (RADS). While this automated data system is still under

	transmission projects data from the Regional Entities; (ii) generation interconnection queue data; and (iii) other data relevant for reliability assessment. The Commission requires NERC to discuss the feasibility of this improvement, and to the extent databases covering this information already exist, discuss how to better utilize or integrate that information into the reliability assessments in the informational filing.	development, significant improvements to data collection and validation have already been made at the Regional Entity level to support RADS in 2014. The NERC Board of Trustees has also approved mandatory data reporting concerning conventional generating units, transmission outages, and demand response availability. NERC collects this data using its Generating Availability Data System (GADS), Transmission Availability Data System (TADS), and Demand Response Availability Data System (DADS) databases. This unique series of databases is used to collect, record, and retrieve operating information tracking, reporting, analyzing, and improving the reliability performance of the BPS. Regional Entity staff work with NERC staff to ensure the data submitted by entities is timely, complete, and accurate. *See* Attachment 3, pages 143, 145.
57	NERC should continue to seek recognition in Canada and Mexico, as appropriate and keep the Commission informed about the status of those efforts.	NERC continues to engage in substantial efforts to gain and maintain recognition as the ERO in Canada and Mexico. In Canada, where by its constitution the regulation of electricity is primarily within the jurisdiction of each province rather than the national government, NERC's activities to obtain and maintain recognition are conducted on a province-by-province basis. Depending on the particular circumstances of each province, NERC has gained recognition through statutes or other provisions of provincial law, or through a memorandum of understanding with appropriate entities in the province.

		With respect to Mexico, the Comisión Federal de Electricidad (CFE), through the Centro Nacional de Control de Energia (CENACE), and the Area de Control Baja California (ACBC), have entered into a membership and operating agreement (MOA) with WECC. The MOA provides for WECC to assist CENACE and ACBC in monitoring compliance by "Designated Entities" (the Mexican equivalent of U.S. registered entities) with Mexico Reliability Standards for Baja California, Mexico. CENACE has approved a total of ten Mexico Reliability Standards. Pursuant to the MOA, WECC monitors compliance with Mexico Reliability Standards, but does not have enforcement or registration (designation) authority for CFE. WECC provides compliance monitoring, reviews proposed and completed mitigation plans, and provides assessment recommendations with respect to alleged violations. *See Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 90-91. *See* Attachment 1, pages 34-52.
195	Directs NERC to include a report in the informational filing detailing the feasibility of establishing a NERC-led Strategic Planning initiative utilizing multiple year budgets.	NERC and the Regional Entities jointly develop a three-year rolling *ERO Enterprise Strategic Plan* which includes goals, objectives and deliverables over the planning period and is used in the development of each entity's business plan and budget. The development and implementation of these common formats and methodologies has helped to continuously improve the efficiency of the business plan and budget preparation process and enabled NERC and Regional Entity financial and accounting staffs and senior management to devote greater attention to more substantive budget issues.

		See Attachment 3, pages 155-156.
138, 217	138: Agrees that NERC should develop performance metrics that help to ensure consistent implementation of the compliance enforcement process across the Regional Entities. 217: Agree that the development of reasonable metrics for assessment of the Regional Entities' performance of their compliance functions will increase efficiency of the enforcement process, provide incentives for effectively, timely handling of Regional Entity caseloads, and furnish important data for the next Performance Assessment.	NERC and the Regional Entities continue to focus efforts on the development of a comprehensive and interrelated suite of metrics. Through the Enforcement Functional Group (EFG, formerly ESMWG) forum, NERC and the Regional Entities have worked together to develop a set of enforcement metrics for tracking of the ERO key compliance enforcement activities. A list of final metrics was agreed upon and a set of common parameters (i.e. business rules) was developed to ensure that metric measurements by NERC and the Regional Entities remained consistent. Parameters agreed upon included violation start date, dismissal date, violations active and in inventory among the Regional Entities and NERC. NERC and the Regional Entities developed four metrics that measure the performance of NERC and each of the Regional Entities with respect to enforcement processing. These metrics are as follows: (i) Caseload Index; (ii) Violations in Inventory; (iii) Violation Aging; and (iv) Mitigation Activity Aging. Future initiatives can take up discussion of additional metrics to add to this initial set, particularly in the areas of measuring enforcement quality and effectiveness. (1) The Caseload Index is a metric that computes the number of months that it would take to clear the violations that are either in the Regional Entity's inventory, NERC's

		inventory based upon the respective average monthly processing rate over the preceding twelve-month period. This metric is useful in evaluating the efficiency of processing violations over time. (2) The Violations in Inventory metric is related to the Caseload Index but is also reported separately. It shows how many violations are in the ERO caseload. Month to month comparisons of violations in inventory can show how the workload of each Regional Entity, NERC, and ERO is changing. (3) The Aging metric identifies where older violations, which have not been filed with FERC or otherwise resolved, are located. The Violation Aging chart, which represents this metric graphically, takes all violations in the ERO inventory and shows by region how many violations were discovered in each year from 2007 to 2013. (4) The fourth metric, Mitigation Activity Aging, identifies the status of mitigation activity based upon the age of violations. NERC's BOTCC receives quarterly updates on these enforcement metrics. The latest update was presented to the BOTCC in May 2014. The *ERO Enterprise Strategic Plan 2014-2017* includes ERO Enterprise performance metrics that will be initially used in 2014. These metrics are intended as indicators of the overall effectiveness of the ERO Enterprise in achieving its mission and the goals and objectives outlined in the *ERO Enterprise*

		Strategic Plan 2014-2017. There are four overarching metrics focused on overall effectiveness in addressing BPS risks and improving reliability. In addition, there are a number of supporting measures that assess the effectiveness of the key operational elements of the ERO Enterprise. The Caseload Index and the Mitigation Activity Aging are included in these supporting measures. NERC reports the results of these metrics on an ERO Enterprise-wide basis, and also, as applicable, distinguishes results for NERC and individual Regional Entities.
215	NERC must provide training to Regional Entities and disseminate to each Regional Entity information and direction resulting from its review of proposed violations and penalties from all eight Regional Entities.	NERC conducts separate workshops for Regional Entity staff and industry members. The workshops are offered in February and September of each year. The workshop includes instructions and practical examples and exercises on compliance and enforcement issues including risk assessments under various Find, Fix, Track and Report (FFT), Spreadsheet Notice of Penalty, and Notice of Penalty scenarios. On August 29, 2013, NERC provided training to industry and Regional Entities on finding and analyzing available public NERC enforcement data in order to identify pertinent reliability issues and trends. The training described the raw and analyzed data available on the NERC website. It also showed where NERC's compliance and enforcement trends documents, annual reports and directives could be found. NERC provides feedback and training to the Regional Entities on a monthly basis during its review of the proposed violations and penalties. This ongoing process allows NERC

		and the Regional Entities to target specific issues applicable to each specific Regional Entity. NERC disseminates to each Regional Entity information and directions on pressing compliance and enforcement matters. For example, in 2013, NERC provided guidance on the FFT process twice. The first guidance document was disseminated in March and explained how to address risk in FFT situations. The document included an updated template and requirements for FFT filings. The second guidance was issued in July, following the Commission's order approving NERC's proposed enhancements to the FFT process. The guidance included a detailed description of the updated FFT process and associated FFT templates. Furthermore, NERC conducts periodic spot checks on various aspects of the Regional Entities' processes and outcomes. For example, NERC conducted a spot check of letters of dismissals from the eight Regional Entities and disseminated issues identified during the spot check, and the potential areas of improvement. NERC developed standardized templates for letters of dismissals and distributed them to the Regional Entities along with its findings. NERC has also scheduled spot checks of mitigation plans and settlements agreements issued by the Regional Entities and will distribute appropriate guidelines based on its findings.
216	Support the suggestions of the Regional Entities for the NERC Board of Trustees Compliance Committee to increase communications with Regional Entities regarding its decisions.	NERC has increased communications with the Regional Entities by providing various forums and channels for communication.

		NERC disseminates compliance information and guidance to the eight Regional Entities mainly through the Enforcement Functional Group (EFG) and the Compliance Monitoring Process Working Group (CMPWG), both of which include representatives from each Regional Entity. The groups meet regularly to discuss compliance issues with NERC, and receive written guidance directives, as appropriate. Furthermore, NERC Enforcement staff is available to answer questions and respond to inquiries from the Regional Entities. For example, in addition to the written guidance on the enhanced FFT process, staff has provided the Regional Entities with additional guidance and assistance throughout the new FFT implementation process. *See also* Attachment 3, pages 66-69.
217	Directs NERC to report on the timeline and plan for development of a non-public central compliance data hub, including details regarding how it will operate, what information it will contain, and whether it will supplant existing processes for providing non-public data to the Commission.	The Regional Entities have implemented compliance data systems to collect and track violation data. These systems interface with NERC's centralized database. At the Regional Entity level, these systems have enabled substantial enforcement processing efficiencies. At the NERC level, these systems have enhanced NERC's ability to identify compliance and enforcement trends and compile accurate metrics. *See* Attachment 3, page 69.

Attachment 5: Status of Areas for Improvement Identified in the Order on the Three-Year ERO Performance Assessment

218-219	Provides that if NERC still wants to pursue a "warning ticket" mechanism, it must explain how the mechanism would work without running afoul of the concerns raised. NERC is free to provide that explanation in the informational filing or, if it chooses to take additional time to develop the mechanism, in a later filing.	NERC has not pursued a "warning ticket" mechanism. FFTs, for example, are remediated issues, are recorded, and can be used in a subsequent penalty matter. *See generally* Attachment 3, pages 66-69.
134	NERC should continue to encourage, and develop incentives for, registered entities to self-report potential violations to the Regional Entities.	Whether or not the registered entity self-reported is a factor considered under the NERC *Sanction Guidelines*. *See* Section 3.3.3 of the *Sanction Guidelines*, Appendix 4B to the NERC Rules of Procedure; and *Overview of NERC Activities and Accomplishments in the Five-Year Period*, pages 50-51, 55-56. *See* also Attachment 1, page 29.

FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. RR14-___

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ATTACHMENT 6

TO

FIVE-YEAR ELECTRIC RELIABILITY ORGANIZATION PERFORMANCE ASSESSMENT REPORT

NERC'S PLAN AND INITIATIVE FOR IMPROVING COORDINATED OPERATIONS ACROSS THE ERO ENTERPRISE

JULY 21, 2014

Improving Coordinated Operations Across The Electric Reliability Organization (ERO) Enterprise

February 2014

Purpose

The purpose of this paper is to describe a vision and path forward to achieving a highly effective and efficient Electric Reliability Organization (ERO) Enterprise. The North American Electric Reliability Corporation (NERC) and eight associated Regional Entities[1] comprise the ERO Enterprise[2]. Part I provides background on why the ERO Enterprise was created in its current form, the unique aspects of the regulatory and delegation models applied, the relationship with the regulated industry and governance, benefits and successes of the ERO Enterprise approach thus far, and remaining opportunities.

Part II lays out a vision for a successful end state, and identifies changes needed to get there, including:

- Refining roles and responsibilities
- Coordinating strategic planning
- Coordinating operational decision-making
- Achieving consistency
- Sharing tools and infrastructure for delegated functions
- Coordinating communications

PART I – BACKGROUND

Creation of the ERO Enterprise

The mission of the ERO Enterprise is to ensure the reliability of the bulk power system in North America, including the continental United States and Canada, and the northern portion of Baja California, Mexico. Entities under the jurisdiction of the ERO Enterprise are the approximately 1,900 registered users, owners, and operators of the North American bulk power system – a system that serves the needs of over 334 million people, includes installed electricity production capacity of approximately 1,200 gigawatts, and operates 211,000 miles of high voltage transmission.

In the face of increasing competition and industry restructuring, and in the context of the August 2003 Northeast Blackout, the U.S. Congress added §215 to the Federal Power Act as part of the Energy Policy Act of 2005 to create the regime of mandatory reliability standards, to be developed and enforced in the U.S. by an Electric Reliability Organization (ERO) certified by, and operating under the oversight of, the Federal Energy Regulatory Commission. NERC was certified as the ERO in July 2006 and thereafter delegation agreements were established with the eight Regional Entities.

[1] The Regional Entities are: Florida Reliability Coordinating Council (FRCC), Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), Reliability First Corporation (RFC), SERC Reliability Corporation (SERC), Southwest Power Pool Regional Entity (SPP RE), Texas Reliability Entity (TRE), and Western Electricity Coordinating Council (WECC).

[2] As used here, "ERO Enterprise" refers to the informal affiliation of NERC and the eight Regional Entities for the purpose of coordinating goals, objectives, metrics, methods and practices across statutory activities. The ERO Enterprise does not supplant obligations of each organization through statutes, regulations, and delegation agreements, but rather enhances coordination through collaborative decision-making and communications.

Equivalent relationships have been sought and for the most part realized in Canada and Mexico. Prior to adoption of §215 in the U.S., the provinces of Ontario (in 2002) and New Brunswick (in 2004) adopted all reliability standards that were approved by the NERC Board as mandatory and enforceable within their respective jurisdictions through market rules. NERC presently has legislation in place or memoranda of understanding with governmental authorities in Ontario, New Brunswick, Nova Scotia, Québec, Manitoba, Saskatchewan, and Alberta, and with the National Energy Board of Canada[3].

Regulatory Model

When enacting legal authority for mandatory and enforceable reliability standards, Congress chose the model of audited self-regulation[4], as reflected in the consensus legislative discussions. Audited self-regulation means congressional or agency (in this case FERC) delegation of power to a private organization to implement or enforce laws or agency regulations with respect to the regulated entities, with powers of independent action and review retained by the delegating agency. The advantage of the audited self-regulatory model is that the statute and agency rules are supplemented and enforced by those entities most directly involved in the regulated activity, which may provide more detailed knowledge of the operational or technical aspects of the regulated activities.

[3] NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. The provincial law now provides for mandatory compliance and enforcement with Reliability Standards. Manitoba has adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and the Northeast Power Coordinating Council (NPCC) have been recognized as standards setting bodies by the Régie de l'énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC standards are now mandatory in British Columbia and Nova Scotia.

[4] U.S. Code of Federal Regulations, Title 1, Chapter III, Part 305.94-1: "Audited self-regulation is defined as congressional or agency delegation of power to a private self-regulatory organization to implement and enforce laws or agency regulations with respect to the regulated entities, with powers of independent action and review retained by the agency. This self-regulatory organization is often an association of regulated entities formed for the explicit purpose of self-regulation. Audited self-regulation is an alternative for Congress to consider in legislating any regulatory program. Properly implemented and monitored, a program of audited self-regulation may effectively advance the statutory objectives consistent with the public interest and the interests of the regulated entities. In certain circumstances, this approach may result in better regulation because the agency's statute and rules are supplemented and enforced by those entities directly involved in the regulated activity, which may have more detailed knowledge of the operational or technical aspects of that activity. The regulatory program also may be more effective because it can be tailored to the individual industry or group. In addition, the agency's regulatory enforcement costs may be reduced by this approach, although such cost reductions should be considered only if they can be achieved without eroding the effectiveness of enforcement. On the other hand, audited self-regulation may present the significant risks of uneven enforcement, capture of the regulators by the regulated industry, and creating barriers to entry or competition. Where the potential for institutional self-interest is too great, self-regulation is undesirable. Other risks can be lessened by requiring the self-regulatory organization to establish and follow procedures similar to those that would be applicable if the self-regulatory organization were an agency. For these procedures to work, effective interest groups must exist, and must have access to the agency, to raise concerns about the conduct of the self-regulatory organization. And of course, the agency itself must vigilantly oversee the activities of the self-regulatory organization and of the regulated entities themselves."

Improving Coordinated Operations Across The Electric Reliability Organization (ERO) Enterprise

February 2014

As the international, multi-jurisdictional ERO, NERC is authorized to:

- Propose, monitor compliance with, and enforce mandatory reliability standards for the North American bulk power system, subject to regulatory oversight and approvals of FERC in the U.S. and applicable authorities in Canada;
- Conduct near-term and long-term assessments of the reliability and future adequacy of the North American bulk power system;
- Certify bulk power system operators as having and maintaining the necessary knowledge and skills to perform their reliability responsibilities;
- Maintain situational awareness of events and conditions that may threaten the reliability of the bulk power system;
- Coordinate efforts to improve physical and cyber security for the bulk power system of North America;
- Conduct detailed analyses and investigations of system disturbances and unusual events to determine root causes, uncover lessons learned, and issue relevant findings as advisories, recommendations, and essential actions to the industry; and
- Based on lessons learned identify the potential need for new or modified reliability standards, improved compliance, or other initiatives.

In executing its responsibilities, NERC delegates certain authorities to eight organizations, the Regional Entities. Under NERC's oversight, the Regional Entities perform certain aspects of the ERO functions through delegation agreements, which are approved by FERC in the U.S. The delegation agreements with each Regional Entity address, among other things: (i) development of regional reliability standards, (ii) monitoring compliance with and enforcing mandatory reliability standards (both North American wide and regional), certification of registered entities, registration of owners, operators and users of the BPS, (iii) reliability assessment and performance analysis, (iv) training and education, (v) event analysis and reliability improvement and (vi) situation awareness and infrastructure security.

The current regional delegation model was first adopted in 2006, with a January 1, 2007 effective date for the initial delegation agreements between NERC and the Regional Entities. It was at this time that NERC began approving regional business plans and budgets, and funding the statutory activities of the Regional Entities through revenues collected from Load-Serving Entities. NERC's oversight role and the obligations of the regions are addressed in NERC Rules of Procedure and the delegation agreements.

As shown in Figure 1, the international ERO footprint covers North America and is comprised of eight reliability regions.

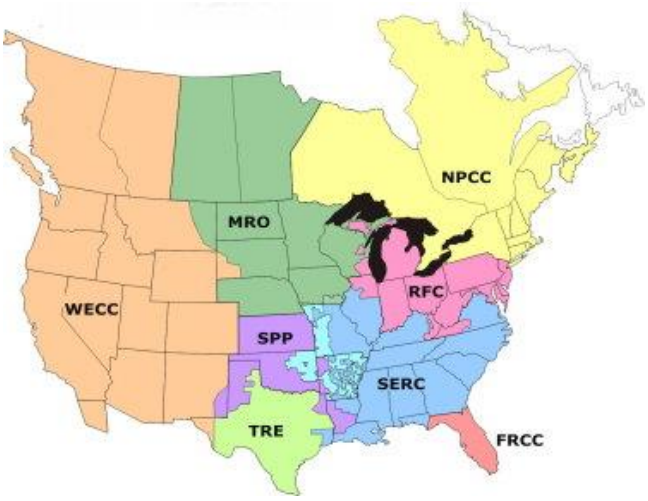


Figure 1 – Map of Regional Entities within NERC

The audited self-regulation model adopted by Congress and the further delegation of statutory functions to Regional Entities present some important benefits and opportunities, but also some challenges. Audited self-regulation results in better regulation because, "[t]he agency's statute and rules are supplemented and enforced by those entities directly involved in the regulated activity, which may have more detailed knowledge of the operational or technical aspects of that activity."[5] This has been the experience with NERC and the Regional Entities since the inception of the ERO in 2006.

The ERO Enterprise is able to directly engage and leverage local and regional technical expertise regarding reliability matters, drafting and commenting on reliability standards, reviewing system events and determining lessons learned, assessing reliability performance and future reliability impacts of emerging issues, just to name a few activities. There exist complex risks, with numerous interdependencies at both the regional and international level, and the regional structure allows us to leverage the expertise across this entire footprint. The regional structure brings greater input from industry experts than could be accommodated in a single ERO organization, and encourages senior utility executive involvement on Regional Entity boards. Experts participate in regional technical committees, providing local and regional system knowledge and experience essential in maintaining a strong technical understanding of the reliability of the interconnected bulk power system. Industry engagement in NERC and the Regional Entities builds commitment, or buy-in, from industry in successful reliability outcomes. The current model can foster reliability excellence whereas a traditional top down regulatory model would tend to enforce reliability adequacy.

Bulk power system risks are dispersed, interdependent and can be asymmetrical across North America. Combining centralized and regional activities is well-suited to identifying and addressing these risks. Given the highly technical and intricate complexities of planning and operating the bulk power system – and given that an interconnected system is a "system of systems" - the concept of local, regional and wide-area views

[5] U.S. Code of Federal Regulations, Title 1, Chapter III, Part 305.94-1

on risk is necessary and has been long accepted.[6] It follows that a "top-down" view of interconnected system risks and a "bottom-up" view of individual system risks is most effective at triangulating the priority risks to be addressed at both a local and interconnection-wide level.

With active engagement of industry experts in the ERO Enterprise technical committees and activities, it is important to maintain effective governance to ensure entities that are regulated do not unduly influence the determination and/or conclusions of the ERO Enterprise. Balance is achieved through governance controls including, but not limited to: an independent board at NERC and segregation of responsibilities and decision-making, especially on compliance and enforcement matters; governance measures at the regions, such as legal and operational separation from registered entities and in some regions the inclusion of independent directors; and, maintaining compliance and enforcement matters as confidential and separate from direct stakeholder participation. Independence and objectivity of NERC and the Regional Entities are further enhanced by government authority oversight, including periodic audits. This layered delegation approach – government to NERC, and NERC to Regional Entities – allows much more active participation by industry participants at the regional level, while maintaining independent oversight by NERC and applicable government agencies.

The distributed governance structure of the ERO Enterprise, with NERC and each Regional Entity having its own board, understandably presents challenges in coordinating ERO Enterprise activities and priorities. At the same time, this distributed governance provides an opportunity to create reliance and trust of the overall enterprise through greater transparency and accountability among all nine entities – the nine entities are mutually interdependent and must be transparently accountable to each other and their respective stakeholders to ensure overall success.

It is also significant that the North American bulk power system is an interconnected, international grid. A single integrated forum – the ERO Enterprise working at the North American and regional levels – ensures that the interests of multiple governmental jurisdictions and their stakeholders can be considered and addressed. Outcomes that are mutually satisfactory across all of North America can then be taken by NERC to the applicable regulatory authorities for approval, without concerns over intrusions by governmental agencies in one country over another country's sovereignty.

ERO Enterprise Progress and Accomplishments Through 2013

The ERO Enterprise has been effective in mitigating a number of important risks to the reliability of the bulk power system since 2006. Results do matter and the achievements since 2006 support the notion that the delegation model works. Using the ground-up approach, the ERO Enterprise has taken advantage of the ability of the Regional Entities to uncover trends and leading indicators of potential reliability problems, such as protection system misoperations and transmission facility right-of-way clearances. The ERO Enterprise was able to use this information to craft strategies to prevent these potential risks from causing actual harm to the bulk electric system. The ERO Enterprise has developed a system of bulk power system reliability metrics based on actual measured performance of the grid. This system of metrics is driven by analysis of event reports, transmission and generator outage data, and relay misoperations. The most recent annual *State of Reliability 2013* report indicates the bulk power system remains reliable and that certain risks have been reduced. Excluding weather-related events, the number of significant system events

[6] For example, over forty years ago, regional reliability organizations were formed; over fifteen years ago, regional reliability coordinators were formed.

resulting in loss of firm load decreased from nine per year on average from 2008 to 2011 down to two events in 2012, and a similar trend is continued through 2013.

Transmission outages caused by grow-in of vegetation, a major cause of the 2003 and several preceding large blackouts, have been virtually eliminated in recent years. NERC introduced a new mandatory standard in 2007 requiring transmission owners to implement vegetation management programs to maintain safe clearances. Strong enforcement actions by NERC and Regional Entities were effective in eliminating grow-ins and reducing the risk of cascading failures initiated from vegetation contacts as seen in the past. Industry experts helped to shape the standard, including a recent update to focus on reliability performance outcomes and risk management while maintaining practicality.

Working with industry system protection experts, NERC developed new relay-loadability requirements for transmission line relays. In the August 2003 Northeast Blackout, over 300 high voltage transmission lines tripped in a high speed cascade due to a previously little understood issue with the relay settings, even though no fault conditions existed on those lines. Industry experts were able to determine that the settings could be modified to prevent a similar future cascade and the requirements were included in new reliability standards. The risk of repeating this mode of uncontrolled high speed cascade of transmission lines has been substantively mitigated.

Industry experts have worked with NERC and the Regional Entities to develop new standards for frequency response to address decades of gradual decline in resources available to respond to frequency disturbances. Experts are currently developing technical methods and tools to mitigate the risks and potential consequences of solar magnetic disturbances. Guidelines have been developed and training implemented to prevent a repeat of a February 2011 loss of generation and firm load in Texas due to extreme cold weather. These are but a few examples of how direct engagement of industry experts through the ERO Enterprise can result in reliability improvements that benefit the public.

The compliance monitoring and enforcement program implemented by NERC and the Regional Entities has been effective in ensuring that compliance violations are identified and mitigated, thereby reducing reliability risk. The ERO Enterprise processed 5,115 confirmed violations of Reliability Standards through 2012 year end. Of these, 85% were deemed to present minimal risk to bulk power system reliability, 13% presented moderate risk, and 2% high risk. The *State of Reliability 2013* report indicates that risks due to noncompliance have trended significantly lower in recent years. NERC and Regional Entities have encouraged self-reporting of violations and timely mitigation – to date, more than 70% of all violations are self-identified by registered entities.

The ERO Enterprise has implemented uniform procedures for compliance monitoring and enforcement, including penalty guidelines, and continues to focus on improving consistency of implementation. FERC has approved the vast majority of notices of penalty without comment since 2008. In recent years, the ERO Enterprise developed greater efficiencies in processing enforcement issues through the find, fix and track (FFT) and spreadsheet notice of penalty (SNOP) initiatives. Work is now continuing to develop the Reliability Assurance Initiative (RAI) to ensure risks are effectively and efficiently addressed through the compliance monitoring and enforcement programs. RAI specifically seeks to improve the reliability of the BPS due to enhanced focus on high reliability risks and registered entities' internal controls relative to those risks, performance of self-assessments and corrective actions, and enhancement of the enforcement processes to process violations in accordance with risk.

The ERO Enterprise has implemented registration criteria to identify entities that can have an impact on bulk power system reliability. There are approximately 1,900 entities registered and an even greater number of entities engaged in reliability activities through the ERO Enterprise. Industry engagement is significantly greater than the number of entities that historically were engaged in NERC during the voluntary era.

The ERO Enterprise has developed a systematic approach to capturing and analyzing bulk power system events. Industry has been very responsive to a program established in 2011 for the voluntary reporting of system events, including sequence of events, root causes, and mitigating actions. Though voluntary, the ERO Enterprise is experiencing nearly 100% participation by industry. The information arising from this program is valuable in identifying reliability risks and trends and in developing lessons learned and mitigating actions for industry.

Since the initiation of the ERO model, major progress has been made in securing critical infrastructure in the bulk power system. Mandatory cyber security standards have been established, and the ERO Enterprise has actively monitored compliance with these standards, noting significant numbers of compliance gaps mitigated by registered entities.

Finally, NERC and the Regional Entities have developed electronic tools, forms, and templates to support information management across the ERO Enterprise, and NERC and Regional Entities are looking to standardize these tools to drive more efficiencies

The outcomes outlined above are a sampling of the positive results that have been developed within the current ERO Enterprise framework, demonstrating that the ERO Enterprise model based on the principles of audited self-regulation and delegation to Regional Entities can be and has been effective in improving reliability and serving the public interest.

PART II – VISION FOR A SUCCESSFUL END STATE

A Vision for the ERO Enterprise

Despite the successes outlined above, the current nine-entity model is not without challenges and risks. The formative years, identified as 2006 through 2013, were focused mainly on achieving the substantial work at hand, guided by the rules of procedure, delegation agreements, and extensive amounts of coordination of activities. With the experience gained and the maturation of the ERO Enterprise, however, it is clear that substantial benefits can be envisioned for an end state.

At its core, the ERO Enterprise must exercise effective and well-coordinated reliability oversight that mitigates reliability risks to the bulk power system. The ERO Enterprise programs must be effective at the mission of ensuring risks are addressed to maintain reliable operations of the bulk power system.

The end state should include more clarity around the roles and responsibilities between NERC and the Regional Entities which will lead to better coordination of goals, more uniform work processes/tools, and performance measures across the enterprise, along with an understanding that all parties comprising the ERO Enterprise must be vested in each other's success. These improvements will create a framework for higher levels of productivity, less duplication, and greater efficiency through more standardization.

The ERO Enterprise must adhere to certain principles. The ERO Enterprise must:

- Apply technical expertise that is focused on risks to the bulk power system and important reliability outcomes;
- Achieve results and methods across the enterprise that are predictable, consistent and timely;
- Share common goals, objectives and measures of success;
- Build relationships that are founded on candor and mutual trust, openness and cooperation;
- Apply collaborative decision-making;
- Ensure efficiencies, minimize duplication and any activities not affecting reliability outcomes;
- Avoid undue burden, discrimination, or capriciousness affecting regulated entities.

The remainder of this paper identifies a path forward to achieving excellence in the oversight and execution of statutory functions and mitigation of bulk power system reliability risks. This discussion is organized in the following areas:

- Clarifying and refining roles and responsibilities
- Coordinating strategic planning
- Coordinating operational decision-making
- Achieving consistency
- Sharing tools and infrastructure for delegated functions
- Coordinating communications

Each section describes the key goals that must be achieved to implement the ERO Enterprise vision for effective, coordinated operations across the enterprise.

Clarifying and Refining Roles and Responsibilities

Achieving the vision requires a clear understanding of the roles and responsibilities of both NERC and the Regional Entities and a clear set of expectations in the execution of the activities performed across the ERO Enterprise.

As the single ERO certified in the U.S. and sanctioned in Canada, NERC has unique responsibilities within the nine-entity ERO Enterprise. NERC is accountable to be the program designer and architect for statutory functions, setting necessary qualifications and expectations for the performance of delegated activities. NERC should respect and be responsive to the expertise and views of Regional Entities, whose staffs have a technical understanding of regional operations, are experienced in the direct interactions with registered entities, and promote the entire ERO Enterprise as one collective thought leader in setting direction and expectations. NERC should also set expectations, provide necessary training and coaching and assess performance of delegated statutory functions.

These roles suggest different qualifications and activities for NERC staff than in the past. Rather than observing regional activities and providing feedback or reviewing and approving final results submitted to

NERC, the emphasis needs to shift toward a different set of skills involving program design and setting management controls to ensure effectiveness. Essential capabilities at NERC include identifying personnel qualifications for program implementation, which itself suggests senior and experienced qualifications, and being able to determine when program adjustments are needed to address bulk power system risks or program risks.

All of this suggests NERC should design its oversight of program areas to encompass program design and development, operational oversight and leadership, coaching and support, and ongoing assessment with feedback to the corresponding regional programs. The goal is to add value and ensure the successful performance of the enterprise. The NERC program staffs must be experts in their field and competent program designers and managers, and teachers and coaches for the regional program staffs. The NERC staff needs to be able to recognize risks, to guide the program and introduce necessary adjustments along the way.

Furthermore, given the distributed and regional nature of the risks being managed and the external environment of a diverse industry across North America, this leadership role must be conducted in a consultative fashion. While NERC has overall responsibility for program design, the goal is to leverage the expertise across the ERO Enterprise in developing future program enhancements. Once designed, the program must be implemented by all Regional Entities consistently in accordance with the approved design. Any variations that do exist must be planned and coordinated for the overall betterment of the ERO Enterprise, within existing fiduciary responsibilities.

NERC is positioned to review data and information from all of the Regional Entities to identify trends and leading indicators of potential reliability risks, develop responsive strategies, and communicate this information to all of the Regional Entities to ensure a uniform, consistent manner of implementation. As the ERO Enterprise matures, process controls should be well established and routinely monitored, allowing greater emphasis on identifying and addressing threats and risks to reliability of the bulk power system.

Implementation of the oversight role must include well-defined and transparent procedures and controls so that all parties understand the qualifications and expectations surrounding execution of delegated functions and how results will be measured. Just as the delegated activities should apply consistent methods, practices, procedures, and tools, the oversight layer should also not be ad hoc, arbitrary, or opaque. It must be known and documented in advance, complete with reporting requirements and performance measures. NERC should be providing ongoing feedback to Regional Entities on patterns and trends, affecting both bulk power system risks and enterprise risks.

ERO Enterprise program oversight should include the following ***essential oversight elements*** to be provided by NERC in consultation with Regional Entities:

- An overall program design indicating the program purpose and goals, and design of controls to manage risks;
- Documentation of common methods, practices and procedures to be applied in the program and performance expectations for each;
- Statements of necessary qualifications of key positions within the regions for conducting certain statutory activities (*e.g.*, for auditors and investigators), and identification of any standards for critical positions;

- Training of NERC and Regional Entity staff for select positions in the conduct of delegated functions;
- A documented and transparent set of process controls and measures to assure delegated responsibilities are properly completed, and to assess the effectiveness of the delegated activities in assess effectiveness of delegated activities in managing bulk power system and enterprise risk; and
- Periodic reporting of results and feedback to Regional Entities on trends and providing opportunities to enhance consistency and effectiveness of results.

The objective is to integrate these elements into the ERO Enterprise operating model on a consistent basis across all the program areas. This is also an area where NERC executive management needs further work on a best design for managing functional area relationships with the regions.

The success of the ERO Enterprise requires NERC and the Regional Entities to recognize that each delegated activity is part of a single overall ERO Enterprise program, such as compliance assurance, enforcement, reliability assessment, or event analysis.

While NERC is responsible for the program design, the Regional Entities are responsible for providing insight and input into the overall design and development of each program area. In support of this, NERC should ensure there are mechanisms for the Regional Entities to provide meaningful insight and direction for incorporation into program design. Regional Entities should adopt conforming methods, practices, and procedures identified in the program design, with exceptions limited to those areas identified in coordinated plans for the purpose of promoting innovation or addressing material regional variations. Regional Entities need to report results using the tools provided, and consistent with reporting requirements identified in the program. Regional Entities should be receptive to feedback from NERC and making responsive adjustments. Regional Entities should ensure staffs are provided the training and development necessary to meet the qualifications required to implement the ERO Enterprise programs.

Regional Entity and NERC staff have an obligation to meet the highest ethical and professional standards in conducting ERO Enterprise work, including independence, objectivity, and providing the best available expertise for addressing bulk power system risks. Regional Entity staff should operate as part of the broader ERO Enterprise and communicate solidarity with the overall enterprise-wide program objectives, methods, and practices.

The ERO Enterprise is aimed at achieving the following goals:

<u>Action item 1</u> – NERC includes in its review of Regional Entity business plans adequacy of resources and alignment of the plans for achieving delegated function objectives and outcomes described in the three-year plan.

<u>Action item 2</u> – NERC, in collaboration with Regional Entities:

- ***a) develops a comprehensive overarching design and set of controls, reporting requirements, and feedback mechanisms for each delegated statutory function, including the essential oversight elements listed above;***
- ***b) reevaluates its organizational structure and leadership qualifications necessary to provide effective design and oversight of statutory activities;***

c) identifies functional qualifications for select delegated activities, such as auditors and investigators; and,

d) adopts risk-based approaches to monitoring performance of delegated functions and providing effective feedback and coaching to continuously improve overall ERO Enterprise performance;

Action item 3 – Regional Entities:

a) work in a coordinated fashion to support NERC in the development of comprehensive functional program designs and controls;

b) adapt existing regional programs for delegated functions to conform with emerging program designs provided by NERC; and

c) ensure Regional Entity staffs meet qualification and training requirements.

To improve the delegation process, NERC and the Regional Entities should work together to update and refine the delegation agreements, which are due for renewal in May 2015, to provide a clearer division of responsibilities, both related to the division of performance of statutory functions and oversight of those functions, and to provide effective mechanisms to resolve routine differences.

Coordinated Strategic and Business Planning

There has been significant progress, achieved through collaboration among senior executives of NERC and the regions, in developing a shared, rolling three-year strategic plan for the ERO Enterprise. Adoption of the ERO Enterprise goals and objectives into business plans across all of the regions has been varied and incomplete. Common performance measures are just emerging and have not yet been adopted into performance management systems across the ERO Enterprise.

The end state for enabling excellence in the execution of statutory reliability activities is that NERC and the eight Regional Entities must work from a common strategic plan, with success measured by a shared set of performance metrics. A common strategic plan and measures does not suggest performing every activity in lock step, but every activity must be coordinated across the enterprise and must be performed consistently. For example, several regions have been working on pilot programs to develop and demonstrate RAI methods as well as the transition to the CIP Version 5 standards.

Action item 4 – NERC and Regional Entities develop and maintain a joint three-year strategic plan for the ERO Enterprise describing the goals and deliverables for statutory functions and this plan should guide the development of each Regional Entity's annual business plans. Additional goals and deliverables that are complimentary or supplemental to the strategic plan may be developed at the Regional Entity level.

Action item 5 – NERC and Regional Entities develop and transparently report results based on a common set of performance measures focused on bulk power system reliability outcomes and effectiveness of the statutory programs. These measures are considered in the performance management program at each entity.

Coordinated Operational Decision-Making

The current model allows and depends on successful delegation of activities. Although statutory functions are delegated, there remains substantial need to coordinate operational decisions that arise in the execution of these duties.

Improving Coordinated Operations Across The Electric Reliability Organization (ERO) Enterprise

February 2014

NERC and the Regional Entities have institutionalized a number of mechanisms to coordinate operational decisions across the enterprise. Note that this discussion and the ensuing recommendations focus on operational decisions that need to be made regarding implementation of statutory functions across the ERO Enterprise and is not intended to reach into the internal management decisions of each organization.

For policy and directional decisions, NERC and Regional Entity CEOs have been meeting periodically for most of the lifetime of the ERO Enterprise although more sporadically in the beginning. In the most recent two years, coordination meetings have been at least monthly, including 6-8 face to face meetings annually. There is an agreed upon protocol for reaching consensus decisions. Although this process has seen partial success, it is still a work in progress. The group is still working on issues such as what level of decisions should be brought to the CEO group for consensus decisions.

In addition to senior leadership coordination, there are approximately two dozen working groups collaborating across various functional areas of the ERO Enterprise. There are groups coordinating compliance monitoring and audits, enforcement, legal, finance, registration, and reliability assessments, just to name a few. Generally these groups are effective in working out common templates for information sharing and resolving common practices and methods at the working level. As with the senior leadership group, most of these groups have achieved good results and are effective in coordinating practices, methods and formats, but there remain opportunities for improvement. One challenge is shifting these working groups from being mainly self-directed problem solvers to being more focused on the strategic plan objectives and having accountability to the CEO leadership team. Also there are concerns that need to be addressed regarding the magnitude of the staff resource commitments stemming from these coordinating activities.

The preferred approach is to proactively establish a more collaborative model and recognize that regional staffs for most functions typically have valuable first-hand experience in implementing the activities on the front lines with registered entities. However, success depends on collaboration that results in timely and effective decisions that all entities in the enterprise agree to implement, and the avoidance of unilateral decision-making that steers portions of the ERO Enterprise off into alternative methods and practices for delegated functions.

<u>Action item 6</u> – ERO Enterprise senior leadership (ERO-Executive Management Group or "ERO-EMG") continues maturing the collaborative decision-making process and setting the direction and policy for the enterprise as well as driving this collaboration throughout the ERO Enterprise organizations.

<u>Action item 7</u> – All nine ERO entities abide by the joint enterprise decisions of the ERO-EMG, and the NERC CEO should make final determinations if consensus is otherwise not achievable for an action that is required.

Achieving Consistency

Consistency of methods, practices, procedures, and tools has been a challenge since the onset of the ERO Enterprise. Consistency is defined by the ERO Enterprise as the use of common methods, practices and tools. The principle initial challenge was that the majority of processes were new and NERC did not foresee the importance of developing common processes and procedures in effective oversight. Instead NERC relied on the Rules of Procedure and the Delegation Agreement to deliver a basic level of consistency which has failed to meet the expectations of industry. Therefore, given the lack of common processes and procedures from NERC, Regional Entities developed their own methods, practices, procedures and tools. While there has been significant progress in working out substantive differences through the leadership and working group processes described previously, there also remain significant variations in methods, practices, procedures, and tools across all nine entities. Today, the biggest challenge in addressing consistency is gaining common agreement on processes and procedures with the backdrop of years of institutionalized differences among NERC and the Regions. Over the past few years there has been significant work toward converging disparate practices across the enterprise. The recent RAI activity, for example, has resulted in some convergence of methods and practices in compliance. In 2013, joint projects saw the completion of a common auditor checklist and an auditor handbook.. A common business process has been developed for managing exceptions to the Bulk Electric System definition. Regions are implementing a common event analysis program and root cause analysis tools.

Some convergence has also been initiated through the use of common electronic tools. Early in the formative years of the ERO Enterprise some of the regions began to deploy common portals to manage compliance information. While these tools helped drive more consistent reporting of results from the regions, even today all nine entities are not using the same information management tools. Tools and infrastructure are covered in more detail in the next section.

Therefore, progress has been made but if common methods, practices, procedures and tools are the yardstick, the enterprise remains very immature. The ultimate success of the ERO Enterprise depends on there being one compliance program, one enforcement program, one event analysis program, etc. Regulated entities will have greater confidence and trust in the ERO Enterprise if they believe their regulatory oversight is not subject to arbitrary variations and possible discrimination from one region to the next. Outcomes will be more predictable and consistent if each statutory function is operated in a unified fashion across the ERO Enterprise. Outcomes will also be more readily measurable to demonstrate the reliability impacts and benefits of the enterprise programs. In the long term, getting past the transition from legacy approaches, there will be significant efficiencies. Such a transition requires the development of a core set of common methods, practices, procedures, and tools, which are principally the responsibility of NERC to produce, but in collaboration with Regional Entities.

Achieving consistency in the end state does not necessarily require identical internal procedures at each Regional Entity, although efficiency would dictate there should be more commonality than exists today. Consistency does not require that each Regional Entity produce identical outcomes given a particular set of circumstances. However, consistency does mean that the approach, methods and practices are the same across the ERO Enterprise and that outcomes produced from the application of local and regional expertise and judgment of the Regional Entity staff are fair, reasonable, and without bias. The goal is consistent methods, practices, procedures and tools that deliver fair and reasonable outcomes.

While consistency is desired, the ERO Enterprise must flexible to permit progress through innovation. Therefore, some variations may be necessary in the interest of progress. However, Regional Entity and NERC leadership need to be prepared to adapt to new approaches, methods, and practices. Some regional variations can actually have value, when implemented on a planned and coordinated basis. Differences for the purpose of testing new approaches, such as during the current RAI pilots and CIP Version 5 pilots, can be helpful in advancing innovation and experimenting with alternative methods. There may also be appropriate variations due to regional differences. An example would be the unique framework in Texas for involving the utility commission in review of enforcement actions. The drive to consistent methods, practices, procedures and tools should not inhibit innovation and the emergence of continuous learning and adaptation. However, managing the balance between consistent approaches and regional differences driven by necessity or creative adaptation should not succumb to the tendency to hold tightly to legacy methods. This shift must remain under the close scrutiny of the ERO-EMG, with accountability for progress to the respective boards, and all entities must be prepared to adopt changes to drive to more consistent methods, practices, procedures, and tools.

Action item 8 – With NERC leading, the ERO Enterprise develops a core set of methods, practices, procedures, and tools to support unified implementation of the major statutory functions of NERC. In doing so, the ERO Enterprise commits to put the best talent available throughout the collective organizations to achieve this goal.

Sharing Tools and Infrastructure for Delegated Functions

As previously described, the infrastructure and electronic tools used by NERC and the eight Regional Entities to implement delegated functions began the ERO era as nine islands. In 2008, the Regional Entities started collaborating on the sharing of portals in an effort to converge onto best practices and provide efficiencies. From this effort emerged two primary platforms for the management of information to support delegated functions. There are two systems which support regional CMEP work:

- OATI webCDMS. The Compliance Data Management System (CDMS) was internally developed by MRO and SPP during the voluntary compliance era of standards. The system was transferred to OATI, a Minneapolis-based software company, in 2008 and became webCDMS. The OATI webCDMS is used by MRO, RFC, WECC, TRE and SPP.
- Guidance. A portal system initially developed by SERC through Guidance a software company in Southern California. SERC, FRCC, and NPCC use the Guidance system.

These early implements were principally focused on compliance information management.

Beginning in 2009, NERC became engaged and built the Compliance Reporting and Tracking System (CRATS) as a further development of the Guidance portal solution. An interface was built to allow data from the CDMS solution to flow into CRATS. Since this time a majority of the regions use the CDMS solution, further emphasizing the importance of this data interface. For several years the flow of compliance information was subject to breakdowns and was very labor intensive for NERC and regional staffs to find the disconnects blocking the consistent flow of compliance information. In late 2012 and 2013 NERC contracted with OATI to manage the CRATS system and staffs across the enterprise were able to resolve the vast majority of information disconnects so that the compliance information flow today is reasonably satisfactory and consistent, albeit built on a patchwork underlying system.

During this evolution, each entity of the enterprise developed other tools as needed to implement activities. For example, NERC developed a tool for maintaining records of the standards registered ballot body and for the conduct of ballots on reliability standards. There are portals at NERC and some of the regions for issuing alerts and tracking recommendations. For the most part, these various applications were developed in isolation from other applications, using various contractors or using in-house resources. Many of these applications are running to the end of their lives and becoming increasingly difficult to maintain at an expected level of functionality.

In 2011 a shift started to take place from the top. The senior leadership across the ERO Enterprise began to articulate a common vision in support of unifying and modernizing the infrastructure and applications needed to support NERC statutory functions. Arriving at an integrated set of applications for management of information in each of the principle delegation areas would enable the enterprise to leverage future efficiencies and eliminate manual data manipulation and validation that is prevalent in the existing tools. Integrated applications across the enterprise would also lead to greater consistency and trust in the NERC processes, and registered entities would see a more seamless interface on which to manage all of its interactions with the ERO Enterprise. Another benefit, lacking today, would be the sharing of information across functional activities, such as information from event analysis and compliance providing useful feedback to standards development.

As part of this shift, NERC hired a contractor in 2011 to conduct a comprehensive study of the ERO Enterprise functional processes and needs. The final report at the end of 2011 led to the formation of an ERO Enterprise Project Management Organization (PMO) that was staffed by NERC but focused on enterprise-wide applications and enabling infrastructure and support services. A first application, the bulk electric system (BES) exception management tool, has been developed and tested ready to handle the expected flow of industry requests in response to the new BES definition. Plans and projects are underway for enterprise-wide applications to manage reliability assessments, event analysis, and establish a common database for information sharing.

In parallel NERC is developing several applications that are uniquely tied to NERC's responsibilities, such as standards information management and balloting tools. The path forward is that, where appropriate, enterprise-wide tools are being developed by NERC through the PMO under the oversight of the ERO-EMG and NERC is developing compatible applications on the same platform for NERC-only activities.

The vision of a comprehensive set of integrated and seamless applications to support the core delegated functions of the ERO Enterprise is essential for the future success of the entire enterprise. The necessary sharing of information between Regional Entities and NERC is essential and the efficiencies and consistencies in methods and practices will be unachievable without the infrastructure to manage extraordinarily large volumes of data that need to be converted into useful information for the purpose of identifying and managing bulk power system risks. However, any enterprise-wide systems approach presents significant risk itself and requires that the projects be executed well and the resulting applications fully meet the needs of the enterprise. A usable, uniform set of tools will drive consistency and lower costs across the ERO Enterprise.

<u>Action item 9</u> - The ERO EMG develops ERO Enterprise IT Applications, where appropriate, to support common processes, to enhance the efficiency and effectiveness of Regional Entities' practices, to increase the consistency of the interface with registered entities, and to facilitate NERC's oversight function.

Coordinating External and Cross – ERO Enterprise Communications

Communications are important to the effectiveness of the ERO Enterprise. Communications can help set expectations for registered entities and stakeholders and demonstrate a common and consistent approach for regulators and the public.

Starting in May 2013, the NERC Board of Trustees initiated a practice of meeting twice yearly as a group with all of the chairs and vice chairs of the Regional Entities. A portion of the meeting is conducted with the NERC and regional CEOs present, followed by a session in-camera. This high level outreach among the nine boards holds significant promise in communicating common purpose and direction, and sharing any concerns among the boards of the ERO Enterprise. These meetings will further help to ensure the mutual accountability previously described that is essential to the successful operation of an enterprise comprised of nine distinct organizations.

A communications working group has been active for several years, coordinating consistent messaging across the ERO Enterprise, particularly with regard to media relations, incident response, and external branding.

NERC and Regional Entities have also coordinated outreach to FERC Commissioners and staff, and Canadian governments. These efforts are typically coordinated through the NERC Office of External Affairs.

The more challenging aspect of coordinating communications is around the operations of the enterprise and key initiatives, such as RAI. Although recent efforts to coordinate key messages and direction have been successful, there remain too many instances of disjointed communications across the entire spectrum of the enterprise. This creates confusion and anxiety with stakeholders and rather than gaining support for necessary initiatives, it creates concern and pushback over the uncertainty of direction.

***Action item 10** – All parties of the ERO Enterprise, including leadership and staffs, convey shared and consistent messages from the enterprise perspective and communicate together to minimize messages emphasizing self-importance or uniqueness.*

***Action item 11** – NERC and Regional Entities continue the joint board coordination to ensure oversight and accountability of all elements of the enterprise, and should continue to refine and expand coordinated outreach to government entities in the U.S. and Canada, stakeholders, and media.*

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.
3000 BAYPORT DRIVE, SUITE 600
TAMPA, FLORIDA 33607-8411
PHONE 813.289.5644 • FAX 813.289.5646
WWW.FRCC.COM

D R A F T

2015 Business Plan and Budget

Florida Reliability Coordinating Council, Inc.

DATE: 5/16/2014 D R A F T

Table of Contents

Introduction 3

Organizational Overview 3

Membership and Governance 4

Statutory Functional Scope 5

2015 Goals and Key Deliverables (Regional Entity Division) 7

2014 Statutory Budget and Projection and 2015 Budget Comparisons 12

Section A – Statutory Programs 13

Reliability Standards Development Program 14

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program 18

Reliability Assessment and Performance Analysis Program 24

Training, Education, and Operator Certification Program 29

Situation Awareness and Infrastructure Security Program 33

General and Administrative 36

Section B – Supplemental Financial Information 40

Reserve Balance 41

Breakdown by Statement of Activity Sections 42

Section C – Non-Statutory Activities 48

2014 Member Services Budget and Projection and 2015 Budget Comparisons 55

Section D – Additional Consolidated Financial Statements 58

Introduction

TOTAL RESOURCES (in whole dollars)	2015 Budget	U.S.	Canada	Mexico
Statutory FTEs	30.91			
Non-statutory FTEs	18.35			
Total FTEs	49.26			
Statutory Expenses	$ 7,179,844			
Non-Statutory Expenses	$ 8,422,053			
Total Expenses	$ 15,601,897			
Statutory Inc(Dec) in Fixed Assets	$ (17,611)			
Non-Statutory Inc(Dec) in Fixed Assets	$ (30,071)			
Total Inc(Dec) in Fixed Assets	$ (47,682)			
Statutory Working Capital Requirement*	**(657,395)**			
Non-Statutory Working Capital Requirement**	**122,583**			
Total Working Capital Requirement	**(534,812)**			
Total Statutory Funding Requirement	$ 6,504,838			
Total Non-Statutory Funding Requirement	$ 8,514,565			
Total Funding Requirement	$ 15,019,403			
Statutory Funding Assessments	$ 6,237,838	$ 6,237,838		
Non-Statutory Fees	$ 8,240,106	$ 8,240,106		
NEL				
NEL%				

*Refer to Table B-1 on page 42 in Section B.
**Refer to the Reserve Analysis on page 58 in Section C.

Organizational Overview

The Florida Reliability Coordinating Council (FRCC) is a Florida not-for-profit corporation that was formed in 1996 and is one of the eight regions of the North American Electric Reliability Corporation (NERC). The FRCC's mission is to ensure and enhance the reliability and adequacy of the Bulk Electric System (BES) in Florida now and into the future. The FRCC's Web site is www.frcc.com. The FRCC Region is comprised of all of Florida east of the Apalachicola River. Florida's unique geography and its highly integrated transmission system coupled with its single interface boundary to the rest of the Eastern Interconnection required the development of a reliability focus in the FRCC Region. Membership in the FRCC's Regional Entity Division is open to any entity, without cost, that has a material interest in the reliability of the BES in the FRCC Region. Currently there are 69 Registered Entities within the FRCC

Region. The FRCC is governed by a balanced stakeholder Board of Directors, and accomplishes its activities through qualified professional staff and standing committees which also have balanced stakeholder governance.

The FRCC provides the statutory functions and services for the FRCC Region through its Regional Entity Division. Non-statutory services for the FRCC Region are provided through its Member Services Division. This divisional structure is an efficient and effective means of clearly separating statutory and non-statutory activities and related funding for each. The revised FRCC Bylaws, creating this divisional structure, were first approved by the Federal Energy Regulatory Commission ("FERC") on March 21, 2008.

The FRCC Regional Entity Division works to enhance the reliability of the BES in the FRCC Region pursuant to the approved Regional Delegation Agreement with NERC, as the Electric Reliability Organization ("ERO"), under the authority of the FERC. The functions performed by the FRCC Regional Entity Division include regional reliability standards development, compliance monitoring and enforcement of reliability standards, reliability assessment and performance analysis, event analysis and reliability improvement, training and education, situation awareness and infrastructure security. The Regional Entity division of the FRCC has one standing committee, the FRCC Regional Entity Committee and Compliance Forum (RECCF). This committee provides input to the FRCC in support of the delegated activities and functions.

The Member Services division of the FRCC provides, coordinates and administers a variety of services relating to the reliable planning and operation of the BES within the FRCC Region. These services are carried out by the FRCC Planning Committee (PC) and the FRCC Operating Committee (OC) and their various subcommittees, task forces and working groups, as well as FRCC Staff.

The FRCC PC and OC actively participate in the development and approval of their committee's budget. The budgets reflect activities of each committee's responsibilities, such as reliability coordination, resource adequacy, stability studies, transmission studies, operations tools, telecommunication tools and infrastructure.

Each year, the total FRCC budget is presented to the FRCC Board of Directors early in the second quarter for informational purposes prior to final approval in June. This process gives all FRCC members advanced indication of the funding level, both statutory and non-statutory, which will be required for the coming fiscal year (January 1 – December 31). This allows for timely inclusion of each member's funding responsibility in their individual budgeting process. The final budget is presented for approval to the FRCC Board of Directors in June of each year and is then submitted to NERC for approval by the NERC Board of Trustees and then by FERC.

Membership and Governance

The FRCC's members (in both divisions) include investor-owned utilities, cooperative utilities, municipal utilities, power marketers, independent power producers and others. Membership is currently 30 FRCC members in the Regional Entity Division and 23 FRCC members in the Member Services Division including affiliate and adjunct members.

The FRCC has six (6) membership sectors which include the following:

- Non-Investor Owned Utility Wholesale
- Load Serving Entity
- Generating Load Serving Entity
- Investor Owned Utility
- Suppliers
- General

There are currently two (2) members in the General Sector of the Regional Entity Division and no members in the General Sector of the Member Services Division.

The activities of FRCC are governed by its Board of Directors. The Board is comprised of senior level executives from members of FRCC.

As part of its responsibilities, NERC, as the ERO, delegates its authority to Regional Entities to perform certain functions through delegation agreements. On October 21, 2010, FERC approved revised delegation agreements between NERC and the eight (8) Regional Entities that became effective January 1, 2011 and will expire at the end of 2015. These delegation agreements describe the responsibility and authority delegated to the Regional Entities. NERC and the Regional Entities revised the delegation agreements in 2010 to improve the efficiency, transparency, quality and effectiveness of the combined NERC and Regional Entity operations. The funding for Regional Entities is approved separately with each Regional Entity submitting its own business plan and budget for consideration by NERC and FERC.

Statutory Functional Scope

The FRCC carries out its delegated functions as outlined and detailed in Exhibits A, B, C, D and E of the delegation agreement. NERC and the Regional Entities will continue to work under the existing regulatory framework governing the establishment and enforcement of reliability standards for the BPS. The existing delegation agreements expire on January 1, 2016. NERC and the Regional Entities will work collaboratively to identify any necessary revisions to the delegation agreements as renewal efforts begin in 2014 and continue through 2015. The delegated functions as defined by the NERC Rules of Procedures include:

- Reliability Standards Development (“RSD”) - Section 300
- Compliance Monitoring and Enforcement (“CMEP”) - Section 400
- Organization Registration and Certification - Section 500 (This program budget has been combined with the Compliance Monitoring and Enforcement function budget.)
- Reliability Assessment and Performance Analysis (“RA”) - Section 800 (including necessary data gathering activities and Events Analysis)
- Training, Education and Operator Certification (“TE”) - Section 900
- Situation Awareness and Infrastructure Security (“SA”) - Section 1000

2015 Key Assumptions

The NERC and Regional Entity business plans and budgets reflect a set of common assumptions (see Exhibit A of the 2015 NERC Business Plan and Budget) developed jointly by NERC and the Regional Entities as part of the annual business plan and budget process. The significant assumptions underlying FRCC's 2015 business plan include:

- NERC will provide oversight of the Regional Entities performance of their delegated functions to ensure that the delegated responsibilities are adequately performed. The Regional Entities are expected to continue to have the primary responsibility for day-to-day operations and interactions with Registered Entities. NERC and the Regional Entities will also work to refine and revise procedures and processes to eliminate duplication, increase operational efficiencies, to enhance ERO-wide consistency and to achieve measurable reliability outcomes, consistent with their respective roles and responsibilities.
- Cost pressures may affect some stakeholder resources available to participate in NERC and Regional Entity activities. However, the assumption of continued industry participation in support of key program areas such as event analysis, reliability assessments and standards development is included in this business plan and budget. NERC and the Regional Entities will evaluate projected initiatives involving stakeholder participation to determine the availability and adequacy of industry resources to support these undertakings.
- The effective date for compliance with the CIP Version 5 standards will be April 1, 2016 for High and Medium impact assets and April 1, 2017 for Low impact assets. The transition between V3 to V5 will be a mission critical activity in 2015. The Regional Entities must plan to support the ongoing CIP v5 transition plans and should anticipate an expansion in the number of Registered Entities that require guidance during 2015. For most CIP activities, the resource demands are expected to increase throughout the planning period.
- The implementation of a BES exception process will require the allocation of resource requirements from several FRCC departments. Resources are expected to manage the process execution, technical validation of the definition and exception requests, and requests for registration and certification reviews. However, the long-term impact cannot be fully assessed at this time as the resource requirements will be based on the number and complexity of exception and registration requests received.
- NERC will continue to budget and incur costs to operate and maintain the software applications and systems known as Situational Awareness for FERC, NERC, and Regional Entities ("SAFNR"). Additional resource investments may be required to enhance the capabilities of SAFNR throughout the planning period; however, there will be no increased cost to the Regional Entities. NERC will continue to review the appropriateness of continued funding of existing reliability tools, with any proposed changes thereto subject to review and input from the Regional Entities, appropriate NERC Committees and working groups, and other affected parties.
- NERC and the Regional Entities will collaboratively work to build and develop ERO Enterprise applications supporting both NERC and Regional Entity operations that will maximize efficiency of technology hardware, consistency of application, resources and data security. These will be managed by a single Project Management Office (PMO) at

NERC. ERO Enterprise funding for the development and maintenance of Enterprise applications will be subject to the budget and funding limits set forth in the approved Business Plan and Budget. The FRCC will also continue to fund applications and systems to satisfy our regional business needs.

- Improved disaster recovery mechanisms and improved IT security procedures will increase capital and operating costs at the Regional Entities.

2015 Goals and Key Deliverables (Regional Entity Division)

- Support NERC's goals that will continue to improve the quality and content of Reliability Standards, including a cost effectiveness assessment of proposed standards.
- Continue to encourage stakeholder awareness and participation in the NERC standards development process through educational outreach efforts and participation in Standard Drafting Teams, the NERC Standards Committee and related subcommittees. Support NERC's efforts to develop the bulk power system risk profile and assess standards compared to the profile and address the most important risk gaps.
- Work with NERC and the other Regional Entities, to continue refinement, improvement and prioritization of risk based compliance monitoring efforts. Continue support of the Reliability Assurance Initiative, including providing the necessary training for compliance and enforcement staff.
- Work with NERC and the other Regional Entities to register entities commensurate with risk to the Bulk Power System (BPS). Support the implementation of any changes resulting from the registration review that began in 2014.
- Continue the implementation of the BES exception process which began mid-2014.
- Work with NERC and the other Regional Entities to hold the industry accountable for violations that create serious risk to the BPS. Improve consistency, quality, and timeliness of compliance monitoring and enforcement activities while utilizing more enforcement discretion for those violations that have minimal impact to the reliability of the BES.
- Continue to be a strong enforcement authority that is independent, without conflict of interest, objective and fair, using enforcement discretion when warranted and imposing penalties and sanctions that are commensurate with risk.
- Support an ERO culture of reliability excellence. Work with NERC and the other Regional Entities to facilitate a learning environment throughout the industry. Work to improve event causal analysis, communication of lessons learned, tracking of recommendations, and implementation of best practices.
- Continue to improve consistency, quality, timeliness and cost effectiveness of NERC and Regional Entity data collection, analysis systems and capabilities through process improvements and more effective coordination and collaboration.
- Support NERC's efforts to move toward and implement an outcome based approach in Reliability Assessments to achieve measureable improvements in the BES reliability. Risks will be identified and prioritized based on reliability impacts, cost/practicality assessments, projected resources, and emerging issues.

- Work closely with the other Regional Entities and NERC to ensure that the delegated functions are implemented consistently and rationally and to promote the success of the ERO as a collaborative enterprise. Perform delegated functions with independence, without conflict of interest, with objectivity and fairness and with increased transparency.
- Support the ERO in addressing and mitigating reliability risks. Work with NERC and the other Regional Entities and the industry to effectively address security vulnerabilities and threats. During crisis situations, support ERO sharing of information among industry, Regions, and government.

2015 Overview of Cost Impacts

The FRCC's proposed 2015 Regional Entity budgeted expenses and net fixed assets (see page 12) is $7,162,233, which is a $368,944 or 5.4% increase over the 2014 budget. The major drivers of this increase are the net effect of:

- Increased compliance software maintenance and development to reflect current costs from the vendor, implement changes necessary to implement RAI and for needed portal efficiencies and program improvements.
- Increased allocated General and Administrative expense due to implementing succession plans for key functions involving a temporary increase of 1 FTE for training to succeed an anticipated retirement
- Budgeted 3% annual merit increase.
- Reduced Medical Benefits expense based on actual experience.
- Decrease in legal fees due to in house legal support.

Statutory Accounting Methodology

The FRCC, in order to be consistent with all the regions, has modified its accounting reporting as follows:

- ERO assessments needed to fund working capital are reflected in the General and Administrative Program within Administrative Services.
- The majority of the Operating Expenses are accounted for within their related department's budget. If an expense cannot be specifically linked to a department, it is included in the General and Administrative Program, within Administrative Services.
- All expenses for the Administrative Services Programs, referred to as indirect expenses for 2015, are allocated to the delegated program areas by their respective FTEs and are shown on one line of each delegated program area Statement of Activities as "Indirect Expenses".
- Capital expenditures are broken out as fixed assets at the end of each statement of activities rather than being included in their related lines in the operating expenses section.
- Expenses include depreciation, but since funding is not being requested for depreciation expense, it has been deducted from the funding requirement for capital expenditures.

2015 Key Deliverables by Program

In 2015, FRCC will achieve the following key deliverables:

- **Reliability Standards Development** — Continue support of NERC in its efforts to improve the quality and content of Reliability Standards and to support NERC's implementation of a cost effectiveness assessment of proposed standards. Support NERC in its efforts to evaluate significant BPS events (Category 3 and above) to identify gaps in standards and address any gaps identified. Support NERCs plan to develop or modify the Reliability Standard Audit Worksheets (RSAWs) by the time a Reliability Standard is balloted. Develop regional reliability standards as needed to support NERC's prioritized work plan and provide increased coordination of standards development activities.
- **Compliance Monitoring and Enforcement** — Continue to support the development and implementation of the Reliability Assurance Initiative, including implementation of the ERO Auditor Handbook and Manual and implementation of the common methodology to assess risk and determine the scope of monitoring activities. Ensure timely and thorough mitigation of all violations of mandatory reliability standards with the most focus on those violations that create serious risk to the Bulk Electric System. Promote a strong culture of compliance excellence, reliability improvement, and risk-based methods among all registered entities in the FRCC Region.
- **Event Analysis** — Continue to support improved reliability through reporting and categorizing of system events and security incidents. Consistently analyze events and system performance for sequence, cause, and remediation to identify reliability risks and trend, and to inform standards, compliance, and other programs. Work to ensure that the industry is well informed of system events, emerging trends, risk analysis, lessons learned and expected actions. Provide timely written lessons learned and recommendations from events and provide all BPS system event reports to the industry through a secure portal.
- **Critical Infrastructure Protection and Cyber Security** — Facilitate, educate and support Registered Entities in complying with CIP reliability standards and responding to cyber security alerts. Facilitate a proactive action plan by industry that demonstrates effective identification and mitigation of security risks, including safeguarding of assets, developing mitigation alternatives, and preparing and testing recovery plans. Support the transition from CIP V3 to V5 including provision of necessary training to FRCC staff, and providing education and outreach to stakeholders to ensure their understanding of the technical aspects of the requirements.
- **Reliability Assessments** — Provide annual, seasonal, probabilistic, scenario and special reliability assessments of the reliability of the FRCC BES in accordance with definitions and requirements. Work with NERC and the other Regional Entities to develop and demonstrate BES performance metrics for the purpose of analyzing and trending reliability improvements and benefits, as well as risk/severity based methods. Work with NERC and the other Regional Entities to support the exception process for the evaluation of Exception Requests as permitted by the revised definition of the BES and the NERC Rules of Procedure.

- **Situation Awareness** — Continue to support NERC in maintaining and enhancing the current and future situation awareness capabilities that include near real-time information and communications protocols that meet the needs of FERC, NERC, and applicable Registered Entities. Issue and track security recommendation to protect the Bulk Power System. Share information learned in Situation Awareness with the Events Analysis program to develop relevant lessons learned.
- **Effective Financial Controls** — Continue to provide rigorous cost controls and efficient management of resources to remain an efficient provider of ERO delegated functions.

Long Term Business Planning

NERC and the Regional Entities continue to work together to improve the overall ERO business planning and budgeting process, including long-term resource and financial planning. The 2015 Business Plan and Budget process builds upon the improvements made over the past several years including face-to-face meetings, conference calls and exchanges of documentation among senior management and staff of NERC and Regional Entities regarding budget assumptions, resource requirements, and opportunities to improve operational efficiency and effectiveness.

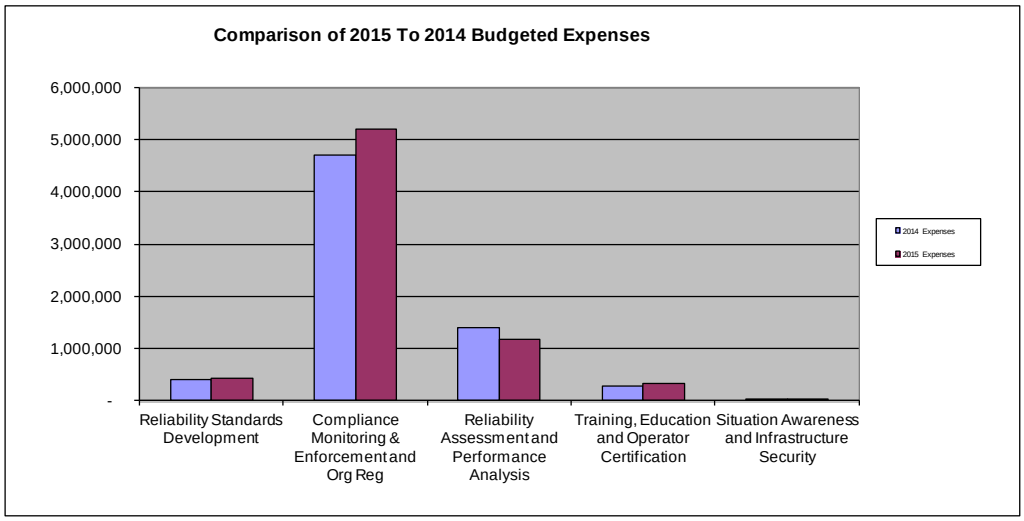
Throughout 2013 and into early 2014, NERC and the Regional Entities worked to develop a common operating model with defined roles and responsibilities that align with business planning goals, objectives, metrics and assumptions for the ERO Enterprise. As part of updating the ERO Strategic Plan, NERC and the Regional Entities consolidated five goals within the existing focus areas of standards; compliance, registration and certification; risks to reliability; and coordination and collaboration. A number of objectives and deliverables expected of the ERO Enterprise were identified. NERC and the Regional Entities added four overarching performance metrics to assess the overall effectiveness of the ERO Enterprise in addressing risk to the Bulk Power System and improving reliability. With the ERO Strategic Plan, the developed performance metrics, and the set of common assumptions, the 2015 Business Plan and Budgets of NERC and the Regional Entities will support and complement each other. The Shared Business Plan and Budget Assumptions (Exhibit A of the 2015 NERC Business Plan and Budget) incorporate assumptions affecting resource demands through the 2017 planning horizon.

NERC and the Regional Entities continue to work together to develop, strengthen and improve an integrated long term ERO business plan and budget that leverages and builds on the combined strengths and resources of NERC and the Regional Entities to improve the overall effectiveness and efficiency of ERO operations and improve the reliability of the BES of North America.

Detailed Business Plans and Budgets by Program

Details of the planning, operation, review, and adjustment for each program area are included in Section A. The corresponding budget details are shown in Section B. Below is an overall summary of the changes by program area.

Funding by Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards Development	409,591	409,592	423,143	13,552	3.3%
Compliance Monitoring & Enforcement and Org Reg	4,702,351	4,702,351	5,211,874	509,523	10.8%
Reliability Assessment and Performance Analysis	1,391,299	1,391,299	1,182,409	(208,890)	-15.0%
Training, Education and Operator Certification	272,310	297,679	321,525	49,215	18.1%
Situation Awareness and Infrastructure Security	19,380	19,380	23,281	3,901	20.1%
Total Funding All Sources	6,794,932	6,820,302	7,162,233	367,301	5.4%



This graphical representation does not include an allocation of working capital requirements among the Program Areas.

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
STATUTORY						
Operational Programs						
Reliability Standards Development	1.74	1.33	1.71		1.71	-0.03
Compliance Monitoring & Enforcement and Org Reg	19.26	18.25	19.77		19.77	0.51
Reliability Assessment and Performance Analysis	5.29	4.26		4.40	4.40	-0.89
Training, Education and Operator Certification	0.67	0.50		0.90	0.90	0.23
Situation Awareness and Infrastructure Security	0.08	0.06		0.09	0.09	0.01
Total FTEs Operational Programs	**27.04**	**24.40**	**21.48**	**5.39**	**26.87**	**-0.17**
Administrative Programs						
General & Administrative	3.36	3.57		4.04	4.04	0.68
Total FTEs Administrative Programs	**3.36**	**3.57**	**0.00**	**4.04**	**4.04**	**0.68**
Total FTEs	**30.40**	**27.97**	**21.48**	**9.43**	**30.91**	**0.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

2014 Statutory Budget and Projection and 2015 Budget Comparisons

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget

STATUTORY

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 5,488,057	$ 5,488,058	$ 0	6,237,838	$ 749,781
Penalty Sanctions	343,000	343,000	-	153,000	(190,000)
Total ERO Funding	**$ 5,831,057**	**$ 5,831,058**	**$ 0**	**$ 6,390,838**	**$ 559,781**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	24,000	24,000	-	24,000	-
Workshops	90,000	115,369	25,369	90,000	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 5,945,057**	**$ 5,970,427**	**$ 25,369**	**$ 6,504,838**	**$ 559,781**
Expenses					
Personnel Expenses					
Salaries	$ 3,806,631	3,630,346	$ (176,285)	$ 4,082,307	$ 275,676
Payroll Taxes	239,599	231,599	(8,000)	253,874	14,275
Benefits	657,255	608,521	(48,734)	579,483	(77,772)
Retirement Costs	602,881	594,403	(8,478)	666,669	63,788
Total Personnel Expenses	**$ 5,306,366**	**$ 5,064,869**	**$ (241,497)**	**$ 5,582,333**	**$ 275,967**
Meeting Expenses					
Meetings	$ 80,930	$ 48,138	$ (32,792)	$ 69,292	$ (11,638)
Travel	167,209	137,943	(29,266)	191,753	24,544
Conference Calls	18,771	14,732	(4,039)	9,482	(9,289)
Total Meeting Expenses	**$ 266,910**	**$ 200,813**	**$ (66,097)**	**$ 270,527**	**$ 3,617**
Operating Expenses					
Consultants & Contracts	$ 348,768	$ 416,262	$ 67,494	$ 393,718	$ 44,950
Office Rent	555,089	554,412	(677)	547,586	(7,503)
Office Costs	118,343	122,974	4,631	132,069	13,726
Professional Services	116,642	41,315	(75,327)	51,324	(65,318)
Miscellaneous	-	-	-	-	-
Depreciation	110,490	157,036	46,546	202,287	91,797
Total Operating Expenses	**$ 1,249,332**	**$ 1,291,999**	**$ 42,667**	**$ 1,326,984**	**$ 77,652**
Total Direct Expenses	**$ 6,822,608**	**$ 6,557,681**	**$ (264,927)**	**$ 7,179,844**	**$ 357,236**
Indirect Expenses	**$ (1,643)**	**$ -**	**$ 1,643**	**$ 0**	**$ 1,643**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 6,820,965**	**$ 6,557,681**	**$ (263,284)**	**$ 7,179,844**	**$ 358,879**
Change in Assets	**$ (875,908)**	**$ (587,254)**	**$ 288,653**	**$ (675,006)**	**$ 200,902**
Fixed Assets					
Depreciation	$ (110,490)	$ (157,036)	$ (46,546)	$ (202,287)	$ (91,797)
Total Fixed Asset Purchases	82,814	129,422	46,608	184,676	101,862
Change in Fixed Assets	**27,676**	**27,614**	**(62)**	**17,611**	**(10,065)**
TOTAL BUDGET	$ 6,793,289	$ 6,530,067	$ (263,222)	$ 7,162,233	$ 368,944
TOTAL CHANGE IN WORKING CAPITAL	**$ (848,232)**	**$ (559,640)**	**$ 288,591**	**$ (657,395)**	**$ 190,837**
FTEs	30.40	27.97	(2.43)	30.91	0.51

Section A – Statutory Programs
2015 Business Plan and Budget

Reliability Standards Development Program

Reliability Standards Development Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.74	1.71	(0.03)
Direct Expenses	$ 369,582	$ 370,389	$ 807
Indirect Expenses	$ 40,021	$ 49,808	$ 9,787
Inc(Dec) in Fixed Assets	$ (12)	$ 2,946	$ 2,958
Total Funding Requirement	$ 409,591	$ 423,143	$ 13,552

Program Scope and Functional Description

The FRCC may develop, through the FRCC Regional Reliability Standards Development Process, separate Regional Reliability Standards that are specific to the FRCC Region and go beyond, add detail to, or implement NERC Reliability Standards. FRCC Regional Reliability Standards will not be inconsistent with or less stringent than NERC Reliability Standards.

The FRCC Regional Reliability Standards Development Process is an open, balanced and fair process that ensures all interested and affected parties have an opportunity to participate in the development of FRCC Regional Reliability Standards for the FRCC Region.

While the FRCC may develop separate Regional Reliability Standards, the preference is to support the development of continent wide reliability standards. The FRCC staff follows and participates in NERC's Standards Development Process. This includes FRCC standards staff participation in the NERC Standards Committee, the NERC Standards Committee Process Subcommittee, and NERC standards drafting teams as appropriate. In addition, the FRCC supports and encourages stakeholder awareness and participation in the NERC standards development process through educational outreach efforts at workshops, webinars and committee meetings.

2015 Key Assumptions

The key assumptions included in the Shared Business Plan and Budget Assumptions, Exhibit A, affecting the Reliability Standards Program include:

1. NERC will continue to focus on reaching a steady state, and improving quality and content of Reliability Standards. This will require the allocation of resources from NERC and the Regional Entities. The implementation of a cost effectiveness assessment of proposed standards and other reform activities are expected to require additional resources however the impacts are not fully known at this time.

2. The number of projects contained in NERC's Reliability Standards Development Plan is expected to increase over the planning period reflecting the transformation of standards to

a steady-state. However, the scope of these projects is expected to narrow as regulatory obligations in the form of directives and five-year reviews, Paragraph 81, and other recommendations are addressed.

3. The focus on improving the quality and content of standards will likely increase the demand on NERC, the Regional Entities and stakeholders to review and comment on proposed revisions to standards, support regulatory filings and support successful implementation of new standards as they become effective.

4. The number of interpretation and guidance requests is expected to remain low, reflecting the initiative to reach steady state and implementation of the Reliability Assurance Initiative (RAI).

5. NERC and the Regional Entities must provide sufficient resources to develop or modify the RSAWs by the time a Standard is balloted which is required to support the Reliability Standards Development Plan.

6. Activity associated with FRCC Regional Reliability Standards development is expected to remain low. FRCC will continue to keep several regional standards development projects on hold while NERC development, on standards addressing the same reliability issues, proceeds to a conclusion.

7. NERC and the Regional Entities will continue to provide communication and outreach opportunities, project level communications and will continue education and training for new or revised standards.

2015 Goals and Key Deliverables

The Standards Program objectives for 2015 are outlined below:

- Continue to follow and participate in NERC's Standards Development Process. This includes FRCC standards staff participation in the NERC Standards Committee, the NERC Standards Committee Process Subcommittee and on NERC standards drafting teams as appropriate.
- Continue to encourage stakeholder awareness and participation in the NERC standards development process.
- Continue to monitor the need for development of Regional Reliability Standards that are required by NERC Reliability Standards or are needed for reliability within the FRCC region.
- Assist the FRCC members and registered entities in following and understanding NERC standards development activities by increasing education and outreach programs to include:
    - Development and presentation at Standards Workshops, Webinars and committee meetings to address continent-wide and regional reliability issues.
    - Develop and deliver project level communications, education and training for new or revised reliability standards.
    - Review, analyze and identify potential Regional concerns associated with NERC Reliability Standards under development.

- Establish a stronger relationship with the FRCC Regional Entity Committee to fully vet and identify any concerns and assist in articulating the concern to standard drafting teams as appropriate.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The slight decrease in the number of FTEs is due to the expectation of more time being spent in Reliability Assessment program implementing the NERC BES Definition and the BES Definition Exception Process and the expectation of more time being spent in review of Registered Entity registration. The increase in personnel expenses is due to budgeted annual merit increases partially offset by a reduction in Medical Benefit expense.
- **Meeting Expenses** - Less travel is expected in 2015 with the BES Standards Writing Project being complete.
- **Operating Expenses** – The decrease in Operating Expenses is primarily the anticipated decrease in legal fees partially offset by increased contract costs included in Contracts, Consultants and Software for a security improvement initiative.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased physical and cyber security measures and planned replacement of old computer equipment.

Reliability Standards Development Program

Funding sources and related expenses for the reliability standards section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
Reliability Standards Development

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 387,520	$ 387,520	$ 0	$ 413,407	$ 25,887
Penalty Sanctions	$ 22,072	$ 22,072		9,737	(12,335)
Total ERO Funding	**$ 409,591**	**$ 409,592**	**$ 0**	**$ 423,143**	**$ 13,552**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 409,591**	**$ 409,592**	**$ 0**	**$ 423,143**	**$ 13,552**
Expenses					
Personnel Expenses					
Salaries	$ 217,880	$ 173,035	$ (44,845)	$ 225,465	$ 7,585
Payroll Taxes	13,714	11,039	(2,675)	14,021	307
Benefits	33,809	23,651	(10,158)	32,602	(1,207)
Retirement Costs	34,595	28,420	(6,175)	36,074	1,479
Total Personnel Expenses	**$ 299,998**	**$ 236,145**	**$ (63,853)**	**$ 308,162**	**$ 8,164**
Meeting Expenses					
Meetings	$ 2,080	$ 969	$ (1,111)	$ 2,606	$ 526
Travel	24,913	16,324	(8,589)	17,469	(7,444)
Conference Calls	174	456	282	203	29
Total Meeting Expenses	**$ 27,167**	**$ 17,749**	**$ (9,418)**	**$ 20,278**	**$ (6,889)**
Operating Expenses					
Consultants & Contracts	$ 4,529	$ 5,222	$ 693	$ 7,381	$ 2,852
Office Rent	23,230	19,312	(3,918)	21,993	(1,237)
Office Costs	6,324	5,968	(356)	7,681	1,357
Professional Services	7,482	2,257	(5,225)	3,261	(4,221)
Miscellaneous	-	-	-	-	-
Depreciation	852	1,073	221	1,633	781
Total Operating Expenses	**$ 42,417**	**$ 33,832**	**$ (8,585)**	**$ 41,949**	**$ (468)**
Total Direct Expenses	**$ 369,582**	**$ 287,726**	**$ (81,856)**	**$ 370,389**	**$ 807**
Indirect Expenses	**$ 40,021**	**$ 37,186**	**$ (2,835)**	**$ 49,808**	**$ 9,787**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 409,603**	**$ 324,912**	**$ (84,691)**	**$ 420,197**	**$ 10,594**
Change in Assets	**$ (12)**	**$ 84,680**	**$ 84,692**	**$ 2,946**	**$ 2,958**
Fixed Assets					
Depreciation	$ (852)	$ (1,073)	$ (221)	$ (1,633)	$ (781)
Total Fixed Asset Purchases	840	371	(469)	4,579	3,739
Change in Fixed Assets	**$ 12**	**$ 702**	**$ 690**	**$ (2,946)**	**$ (2,958)**
TOTAL BUDGET	$ 409,591	$ 324,210	$ (85,381)	$ 423,143	$ 13,552
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 85,382**	**$ 85,382**	**$ -**	**$ -**
FTEs	1.74	1.33	(0.41)	1.71	(0.03)

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program

Compliance Monitoring and Enforcement and Organization Registration and Certification Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	19.26	19.77	0.51
Direct Expenses	$ 4,281,909	$ 4,658,890	$ 376,981
Indirect Expenses	$ 442,994	$ 575,856	$ 132,862
Inc(Dec) in Fixed Assets	$ (22,552)	$ (22,872)	$ (320)
Total Funding Requirement	$ 4,702,351	$ 5,211,874	$ 509,523

Program Scope and Functional Description

Monitoring, evaluating, investigating and enforcing compliance with Reliability Standards by owners, operators and users of the BES, as well as the development and adoption of the reliability standards themselves, are at the core of FRCC's mission. Reliable operation of the BES is in the public interest, because it will benefit all owners, operators and users of the BES, and, ultimately, all users and consumers of electric power in the FRCC Region.

Compliance and Enforcement activities are carried out by the FRCC compliance staff and are independent of all users, owners and operators of the BES. Compliance activities are governed by the delegation agreement between the North American Electric Reliability Corporation (NERC) and the FRCC. Through a risk-based program of monitoring, evaluating, enforcing, and if necessary, the imposition of penalties and sanctions for noncompliance with Reliability Standards, FRCC will strive to increase the level of reliable operation of the BES in the FRCC Region.

The NERC Compliance Monitoring and Enforcement Program (CMEP) is the program used by the FRCC to monitor, assess, and enforce compliance with Reliability Standards within the FRCC Region. The FRCC compliance staff works with the compliance staff of the other Regional Entities and with NERC to achieve as much consistency and transparency as possible in the implementation of the CMEP. The development and implementation of the Reliability Assurance Initiative (RAI) throughout 2014 and into early 2015 provides the foundation and guidance for NERC and the Regional Entities in moving to a risk-based environment aimed at focusing on those risks that are most important to the reliability of the BES.

2015 Highlights Compliance Monitoring and Enforcement Processes

In 2015 the FRCC will monitor, assess and enforce compliance with Reliability Standards using seven (7) monitoring processes (Compliance Audits, Self-Certifications, Spot Checking, Compliance Investigations, Self-Reporting, Periodic Data Submittals, and Complaints) to collect information in order to make assessments of compliance to Reliability Standards. However as risk based monitoring activities increase, strong consideration will be given by NERC and the

Regions to modify the current three (3) and six (6) year audit cycles for registered entities. The rigor, scope, depth and recurrence of audits and spot checks will be assessed by the reliability risk and not a predetermined schedule.

Registration and Certification

The FRCC has registered the organizations responsible for complying with Reliability Standards in accordance with Section 500 of the NERC Rules of Procedure. Currently there are 69 Registered Entities with a total of 244 registered functions. Maintaining a complete and accurate registration database will be an ongoing activity. The FRCC will develop, maintain and provide to NERC accurate information on entity registration within the FRCC Region with updates as changes occur. NERC and the Regional Entities began a review of the organization registration process in 2014 which may result in changes to the registration process that could begin in 2015. While expectations of increased activity are associated with the implementation of the BES Exception Process mid-2014, there is some uncertainty in the amount of activity associated with registration and certification of registered entities. The FRCC may consider the reallocation of existing resources should the need arise for additional support in this area.

Enforcement and Mitigation

Enforcement actions taken by FRCC may include the imposition of remedial action directives, sanctions and penalties which are applied per the NERC Rules of Procedure. Mitigation of violations of the approved Reliability Standards remains central to the FRCC's reliability focus. Registered Entities found in violation of a Reliability Standard will be required to fully mitigate the violation regardless of any enforcement actions taken. The year 2014 continued to bring advances in enforcement discretion of violations with minimal impact to the reliability of the BES. This additional discretion will continue in 2015 through the development and implementation of the NERC Reliability Assurance Initiative allowing for more focus being placed on those violations that pose a more serious risk to the reliability of the BES.

2015 Key Assumptions

- Audits are expected to continue under the current three and six year schedules until NERC and the Regional Entities transition to a more risk-based approach to compliance monitoring as developed in the Reliability Assurance Initiative (RAI).
- Reliability risk profiles for all Registered Entities will be developed and audit scopes will be tailored to the risk profiles which may increase the depth and complexity of some audits and decrease the depth and complexity of others. The consistent approach to audit scope methodology being developed as part of the RAI in 2014 is expected to be used in early 2015.
- Integration of the assessment of Registered Entity internal controls programs as part of the compliance monitoring program will allow NERC and the Regional Entities to further prioritize risk based compliance monitoring activities. Greater emphasis on internal controls provides positive incentives for industry to demonstrate effective management of compliance programs that are focused on reliability, as well as place downward pressure on compliance resource requirements for industry, NERC and the Regional Entities.
- The use of spot checks and self-certifications is expected to increase as risk-based monitoring is implemented, but that should have little effect on FRCC's overall resource requirements. The implementation of the Reliability Assurance Initiative and the

expansion of the Find Fix and Track (FFT) process will require resources to complete the design and to begin implementing RAI for both compliance and enforcement.

- The approval of CIP V5 is anticipated to significantly increase the compliance monitoring activities. The effective date for compliance with the CIP Version 5 standards will be April 1, 2016 for High and Medium impact assets and April 1, 2017 for Low impact assets. The transition between V3 to V5 will be a mission critical activity for the ERO Enterprise in 2015. FRCC plans to support the ongoing CIP v5 transition plans and anticipates an expansion in the number of Registered Entities that require guidance during 2015. Additional training requirements will be necessary to support the transition and will affect the annual training commitments. For most CIP activities, the resource demands are expected to increase throughout the planning period.
- The number of non-CIP violations is expected to decrease as most registered entities have been audited and the standards and RSAWs have matured.
- The Technical Feasibility Exception (TFE) program will continue however the processing per the revised Appendix 4D, of the NERC Rules of Procedure, is expected to drive a less onerous process for TFE reporting and reviewing.
- Applications planned to be centralized, such as a common audit management tool, at NERC to improve consistency and efficiency, will require Regional Entity support and resources for development and implementation. A significant multiyear investment will be required to develop and implement the system which will be funded by NERC.
- NERC and the Regional Entities are expected to utilize consistent audit practices and focus on higher target reliability risks to increase efficiency and mitigate overall compliance costs.
- NERC and the Regional Entities will provide sufficient resources to develop or modify the RSAWs by the time a Standard is balloted which is required to support the Reliability Standards Development Plan.
- NERC and the Regional Entities must plan to support the training requirements necessary to meet the criteria set forth by the ERO Auditor Manual and Handbook and the Compliance Auditor Capabilities and Competency Guide. Regional Entities will be expected to provide training documents and other related compliance guidance to compliance staff, review Auditor job descriptions and properly reflect the guidance provided in the Compliance Auditor Capabilities and Competency Guide, perform a gap analysis to identify both individual training needs and organizational compliance resource needs, provide an assessment process to evaluate audit team competencies and capability needs, and put a training program in place that addresses initial and continuing training for capability and competency development.
- NERC will continue to budget and incur the cost of a unified learning management system (LMS) for the regional audit staff and work with the Regional Entities to consolidate training resources and promote better coordination, planning, delivery and management of training efforts across the ERO.
- Additional resources will be required, and increases to NERC and Regional Entity training budgets are expected to support certain training initiatives of the RAI. Regional Entities are expected to allocate resources to meet the training requirements for the compliance and enforcement staff that are associated with the implementation of the RAI.

- Maintaining budgeted qualified compliance and enforcement staff will continue to be a challenge driven by a limited pool of qualified people and an aging work force. Investments in training less experienced personnel are likely to increase.

2015 Goals and Key Deliverables

The Compliance Monitoring and Enforcement Program objectives for 2015 are outlined below:

- Continue to assess and update entity registration and certification. The FRCC will support the implementation of the changes resulting from the registration review that began in 2014.
- Support the development and implementation of NERC's Reliability Assurance Initiative, including providing the necessary training for compliance and enforcement staff. Enforce compliance with mandatory reliability standards in accordance with the CMEP and ROP while improving consistency, quality, timeliness and utilizing more enforcement discretion for those violations that have minimal impact to the reliability of the BES.
- Develop and maintain reliability risk profiles of all registered entities in the FRCC Region for use in the continued transition to a more risk-based compliance monitoring.
- Implement the ERO Auditor Handbook and Manual and continue to work with NERC Compliance staff and other Regional Entity Compliance staff to modify compliance procedures to increase consistency in the determination of violations and penalties.
- Implement the common methodology developed in 2014 to assess risk and determine scope of monitoring activities. Conduct periodic audits, spot checks, self-certifications, and compliance investigations as required by the NERC Compliance Monitoring and Enforcement Program.
- Continue to promote the self-identification of non-compliance by Registered Entities and utilize increased discretion as appropriate. Ensure timely and thorough mitigation of all violations of mandatory reliability standards.
- Promote a culture of compliance excellence through education, transparency, information sharing and incentives.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs and personnel expense can be primarily attributed to expected increased effort in the Organization Registration Program and the effect of having an addition to staff budgeted for May of 2014 for a full year in 2015. The increase in personnel expense is also due to a budgeted annual merit increase. These increases are partially offset by reduced expected benefit expenses based from medical expenses being less than anticipated in the 2014 budget.
- **Meeting Expenses** – Increased travel is expected in 2015 to meet expectations of NERC for meetings to ensure consistent implementation of the Reliability Assurance Initiative (RAI), RAI associated updates to the Auditor Handbook, and to support ERO IT development projects.
- **Operating Expenses** – Anticipated increased cost of the Compliance Software to implement RAI and NERC business rules, increased contract costs included in Contracts,

Consultants and Software for a security improvement initiative and the increased depreciation effect of the additions of same in 2014 and 2015 partially offset by an anticipated decrease in legal fees.

- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased cost in enhancements of the Compliance Software, increased physical and cyber security measures and planned replacement of old computer equipment.

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program

Funding sources and related expenses for the compliance enforcement and organization registration and certification section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital 2014 Budget & Projection, and 2015 Budget

Compliance Monitoring & Enforcement and Organization Registration & Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 4,458,040	$ 4,458,040	$ -	$ 5,099,302	$ 641,262
Penalty Sanctions	244,311	244,311	-	112,572	(131,739)
Total ERO Funding	**$ 4,702,351**	**$ 4,702,351**	**$ -**	**$ 5,211,874**	**$ 509,523**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Federal Grants	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 4,702,351**	**$ 4,702,351**	**$ -**	**$ 5,211,874**	**$ 509,523**
Expenses					
Personnel Expenses					
Salaries	$ 2,411,701	$ 2,368,964	$ (42,737)	$ 2,611,174	$ 199,473
Payroll Taxes	151,798	151,129	(669)	162,386	10,588
Benefits	452,812	421,727	(31,085)	385,976	(66,836)
Retirement Costs	382,958	389,089	6,131	431,288	48,330
Total Personnel Expenses	**$ 3,399,269**	**$ 3,330,909**	**$ (68,360)**	**$ 3,590,824**	**$ 191,555**
Meeting Expenses					
Meetings	$ 4,915	$ 7,412	$ 2,497	$ 12,729	$ 7,814
Travel	92,966	81,240	(11,726)	122,194	29,228
Conference Calls	4,565	8,805	4,240	4,390	(175)
Total Meeting Expenses	**$ 102,446**	**$ 97,457**	**$ (4,989)**	**$ 139,313**	**$ 36,867**
Operating Expenses					
Consultants & Contracts	$ 119,235	$ 225,494	$ 106,259	$ 214,984	$ 95,749
Office Rent	406,366	413,633	7,267	404,082	(2,284)
Office Costs	69,926	74,111	4,185	80,150	10,224
Professional Services	83,069	30,900	(52,169)	37,762	(45,307)
Miscellaneous	-	-	-	-	-
Depreciation	101,598	148,536	46,938	191,775	90,177
Total Operating Expenses	**$ 780,194**	**$ 892,674**	**$ 112,480**	**$ 928,753**	**$ 148,559**
Total Direct Expenses	**$ 4,281,909**	**$ 4,321,040**	**$ 39,131**	**$ 4,658,890**	**$ 376,981**
Indirect Expenses	**$ 442,994**	**$ 509,116**	**$ 66,122**	**$ 575,856**	**$ 132,862**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 4,724,903**	**$ 4,830,156**	**$ 105,253**	**$ 5,234,746**	**$ 509,843**
Change in Assets	**$ (22,552)**	**$ (127,805)**	**$ (105,253)**	**$ (22,872)**	**$ (320)**
Fixed Assets					
Depreciation	$ (101,598)	$ (148,536)	$ (46,938)	$ (191,775)	$ (90,177)
Total Fixed Asset Purchases	79,046	127,708	48,662	168,903	89,857
Change in Fixed Assets	**$ 22,552**	**$ 20,828**	**$ (1,724)**	**$ 22,872**	**$ 320**
TOTAL BUDGET	$ 4,702,351	$ 4,809,328	$ 106,977	$ 5,211,874	$ 509,523
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ (106,977)**	**$ (106,977)**	**$ -**	**$ -**
FTEs	19.26	18.25	(1.01)	19.77	0.51

Reliability Assessment and Performance Analysis Program

Reliability Assessment and Performance Analysis Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	5.29	4.39	(0.90)
Direct Expenses	$ 1,270,439	$ 1,049,392	$ (221,047)
Indirect Expenses	$ 121,674	$ 127,871	$ 6,197
Inc(Dec) in Fixed Assets	$ (814)	$ 5,146	$ 5,960
Total Funding Requirement	$ 1,391,299	$ 1,182,409	$ (208,890)

Program Scope and Functional Description

The FRCC will assess the reliability of the BES in the FRCC region and will continue to ensure that the planned system is robust, reliable and stable. The FRCC will participate in Event Analysis Teams to analyze any disturbances that may occur within the FRCC region.

The FRCC performs transmission reliability studies in order to provide an assessment to NERC for its periodic NERC Reliability Assessments. These studies evaluate regional and inter-regional facilities. The FRCC prepares a minimum of three reliability assessments each year and a probabilistic assessment every other year in support of NERC Reliability Assessments:

- A 20 year long-term reliability assessment report
- A summer assessment report
- A winter assessment report
- A probabilistic long-term reliability assessment (biennial)

These reports evaluate electricity demand, the adequacy of supply and its deliverability, fuel reliability and the adequacy of the transmission system within the FRCC. The FRCC will prepare special reliability assessment reports as conditions warrant.

The FRCC Reliability Assessment and Performance Analysis Program (RA) will support NERC's efforts to move toward and implement an outcome based approach in Reliability Assessments to achieve measureable improvements in the BES reliability. Risks will be identified and prioritized based on reliability impacts, cost/practicality of assessments, projected resources, and emerging issues. The FRCC will support NERC's efforts for collection and analysis of data, as well as support any of NERC's special reliability assessments and the efforts related to the collection of data via the Generation Availability Data System (GADS), Transmission Availability Data System (TADS) and Demand Response Availability Data System (DADS). In addition, the FRCC will work with NERC to gather data and/or complete

analysis in support of U.S. Federal initiatives, including high impact/low frequency events such as geomagnetic disturbances, system frequency response analysis, climate change and other environmental regulations.

The FRCC will support a new ERO initiative focused on identifying essential reliability services and providing the industry with technical papers and guidelines as appropriate.

The FRCC actively participates in the Eastern Interconnection Reliability Assessment Group (ERAG) which is responsible for the Eastern Interconnection transmission models and inter-regional studies. The FRCC will support NERC's and ERAG's efforts to improve the data quality of the Eastern Interconnection (EI) transmission models and validate the performance of these models compared to system events. The FRCC is an active participant on the NERC Reliability Assessment Subcommittee which is responsible for performing an independent review of reliability assessments.

The FRCC Events Analysis Program will analyze or support the analysis of significant events and system performance that impact the BES within the FRCC Region. The FRCC will facilitate consistent identification of sequence, root cause and remediation to identify reliability risks and trends, and lessons learned. FRCC's analysis will result in the identification of any gaps in standards, compliance effectiveness, registration and risk controls effectiveness. The FRCC will provide lessons learned and recommendations from events and identified risks.

The FRCC will support NERC to improve event causal analysis, communication of lessons learned, tracking of recommendations, and implementation of best practices. The FRCC will support NERC to continue to improve consistency, quality, timeliness and cost effectiveness of NERC and Regional Entity data collection, analysis systems and capabilities through process improvements and more effective coordination and collaboration.

2015 Key Assumptions

- NERC will continue to incrementally improve definitions, refine data reporting requirements for Registered Entities and review adequate level of reliability related metrics used in reliability assessments.
- NERC and Regional Entities will be requested to gather data or perform analysis in support of federal initiatives related to critical infrastructure protection including high impact/low frequency, climate change, environmental regulations, and/or renewable energy initiatives. Generation Availability Data System (GADS), Spare Equipment Database (SED) and Demand Response Data System (DADS) collection will continue to be mandatory in 2015.
- NERC and the Regional Entities are expected to provide independent reviews of assessments to assure a high level of technical rigor.
- Implementation of the BES exception process will require the re-allocation of resources from several NERC and Regional Entity departments. The resources will be expected to manage the process execution, technical validation of the definition and exception requests, self-determined notification submittals and requests for registration and certification review. The resource impacts are not fully known at this time, but are expected to be driven by the number and complexity of exception requests, self-determined notification submittals and registration requests received.

- NERC has established an Essential Reliability Services Task Force that may have an impact on resource requirements in order to support the work of this task force which is expected to have weekly conference calls and two or three in person meetings.
- NERC will sustain a Reliability Assessment and Performance Analysis team with representatives from the Regional Entities to:
    - Develop and implement improved enterprise-based data collection and analysis systems and capabilities
    - Support the integration of RAPA information systems for modeling and data requirements and achieve timelines for delivering high quality reports
    - Develop, verify and validate quality reliability assessment and analyses model and data quality characteristics
    - Address impacts of new technologies, changing resource or demand resource composition, and environmental related regulations or legislation
    - Support the compilation of long-term sustainable Eastern Interconnection models
    - Provide technical resources and expertise to perform analyses as needed for standards development, compliance and enforcement activities
    - Support quality analysis and overall assessment of the geomagnetic disturbance (GMD) vulnerability, planning guides and planning standards.
- The number of "qualified system events" as defined in the NERC Events Analysis Process, is expected to remain steady (approximately 10 per month across North America). Greater collaboration with the region and the registered entity is leading to more detailed analysis and supporting the identification of reliability issues and challenges.

2015 Goals and Key Deliverables

The Reliability Assessment and Performance Analysis Objectives for 2015 are outlined below:

- Perform a reliability assessment of the FRCC Region to determine if the planned resources and proposed transmission expansion plans will meet the needs of the projected demand throughout the planning horizon.
- Support NERC in preparing its reliability assessment reports.
- Support the implementation of the BES exception process. This will include providing a technical review of exception requests that are submitted by the registered entities.
- Support the work of the newly created Essential Reliability Services Task Force by assigning an FRCC Staff person to support this NERC initiative.
- Evaluate, track and assess severity/risk and reliability metrics and risk indices – including providing support to update reliability metrics and risk indices.
- Support data gathering and reporting efforts for the Generating Availability Data System (GADS), the Transmission Availability Data System (TADS), Spare Equipment Database (SED) and Demand Response Availability Data System (DADS).

- Strengthen data collection and validation processes by designing, creating, testing and implementing data checking systems to accommodate the increasing amount of data NERC collects for its long-term, seasonal, operational, scenarios and special reliability assessments along with the databases supporting reliability performance assessments.
- Review and/or analyze significant events that impact the FRCC BES and work with NERC to identify the root causes of events that may be precursors of potentially more serious events.
- Assess past reliability performance for potential lessons learned.
- Maintain relationships with NERC, regulatory and governmental organizations involved with BES reliability (e.g., Florida Public Service Commission (FPSC), Department of Energy (DOE), FERC, Energy Information Administration (EIA), etc.).
- Maintain a databank of power flow, short circuit and dynamic models to use in planning and evaluating future systems and current operating conditions.
- Work with ERAG Multi-Area Modeling Working Group (MMWG) to develop Eastern Interconnection steady-state and dynamics models and develop model validation processes.
- Conduct Loss of Load Probability and the Scenario Analysis studies as needed.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – In 2014, the committee structure was streamlined to reduce the amount of time that staff spent preparing for meetings and participating in meetings. Previously, the FRCC conducted business associated with Reliability Assessments in both the Operating Committee and the Planning Committee. This approach resulted in staff members attending multiple meetings each month to cover the same topics. With the revised structure, all Regional Entity activities will be conducted in one forum; the new Regional Entity Committee and Compliance Forum (RECCF). In addition to consolidating the Regional Entity activities under the RECCF, it was also determined that the RECCF will not need to meet monthly, but will meet face-to-face six times in 2015. This new construct will allow FRCC staff to complete the Reliability Assessment deliverables much more efficiently and drives the decrease to FTEs and personnel expenses.
- **Meeting Expenses** – With the formation of the RECCF, there will be fewer meetings required to complete the RA deliverables decreasing Meeting Expenses.
- **Operating Expenses** –The decrease is due to an anticipated decrease in legal fees and a reduction in certain consultant expenses which have been consistently over-budgeted.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased physical and cyber security measures and planned replacement of old computer equipment.

Reliability Assessment and Performance Analysis Program

Funding sources and related expenses for the reliability assessment and performance analysis section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital 2014 Budget & Projection, and 2015 Budget

Reliability Assessment and Performance Analysis

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 1,300,196	$ 1,300,196	$ -	$ 1,133,412	$ (166,784)
Penalty Sanctions	67,103	67,103	-	24,997	(42,106)
Total ERO Funding	**$ 1,367,299**	**$ 1,367,299**	**$ -**	**$ 1,158,409**	**$ (208,890)**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	24,000	24,000	-	24,000	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 1,391,299**	**$ 1,391,299**	**$ -**	**$ 1,182,409**	**$ (208,890)**
Expenses					
Personnel Expenses					
Salaries	$ 662,404	$ 552,292	$ (110,112)	$ 580,711	$ (81,693)
Payroll Taxes	41,693	35,234	(6,459)	36,114	(5,579)
Benefits	99,378	84,437	(14,941)	82,646	(16,732)
Retirement Costs	105,185	90,711	(14,474)	92,914	(12,271)
Total Personnel Expenses	**$ 908,660**	**$ 762,674**	**$ (145,986)**	**$ 792,385**	**$ (116,275)**
Meeting Expenses					
Meetings	$ 6,674	$ 1,307	$ (5,367)	$ 1,612	$ (5,062)
Travel	43,265	34,637	(8,628)	47,375	4,110
Conference Calls	8,543	1,437	(7,106)	447	(8,096)
Total Meeting Expenses	**$ 58,482**	**$ 37,381**	**$ (21,101)**	**$ 49,434**	**$ (9,048)**
Operating Expenses					
Consultants & Contracts	$ 192,989	$ 130,637	$ (62,352)	$ 122,547	$ (70,442)
Office Rent	70,623	61,640	(8,983)	56,646	(13,977)
Office Costs	13,480	12,843	(637)	14,617	1,137
Professional Services	22,829	7,204	(15,625)	8,398	(14,431)
Miscellaneous	-	-	-	-	-
Depreciation	3,376	4,213	837	5,365	1,989
Total Operating Expenses	**$ 303,297**	**$ 216,537**	**$ (86,760)**	**$ 207,573**	**$ (95,724)**
Total Direct Expenses	**$ 1,270,439**	**$ 1,016,592**	**$ (253,847)**	**$ 1,049,392**	**$ (221,047)**
Indirect Expenses	**$ 121,674**	**$ 118,694**	**$ (2,980)**	**$ 127,871**	**$ 6,197**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 1,392,113**	**$ 1,135,286**	**$ (256,827)**	**$ 1,177,263**	**$ (214,850)**
Change in Assets	**$ (814)**	**$ 256,013**	**$ 256,827**	**$ 5,146**	**$ 5,960**
Fixed Assets					
Depreciation	$ (3,376)	$ (4,213)	$ (837)	$ (5,365)	(1,989)
Total Fixed Asset Purchases	2,562	1,186	(1,376)	10,511	7,949
Change in Fixed Assets	**$ 814**	**$ 3,027**	**$ 2,213**	**$ (5,146)**	**$ (5,960)**
TOTAL BUDGET	$ 1,391,299	$ 1,132,259	$ (259,040)	$ 1,182,409	$ (208,890)
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 259,040**	**$ 259,040**	**$ -**	**$ -**
FTEs	5.29	4.26	(1.03)	4.40	(0.89)

Training, Education, and Operator Certification Program

Training, Education and Operator Certification Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.67	0.91	0.24
Direct Expenses	$ 257,163	$ 295,452	$ 38,289
Indirect Expenses	$ 15,410	$ 26,506	$ 11,096
Inc(Dec) in Fixed Assets	$ (263)	$ (433)	$ (170)
Total Funding Requirement	$ 272,310	$ 321,525	$ 49,215

Program Scope and Functional Description

The FRCC is a NERC-approved Continuing Education (CE) Provider. The FRCC System Operator Subcommittee (SOS) develops and delivers training in which FRCC grants NERC CE hours to those individuals who successfully complete a course. FRCC will utilize the NERC database to accommodate the recordkeeping requirements for the continuing education program. Maintaining the reliability of the BES requires informed and trained personnel. The FRCC supports training activities through its staff and its System Operator Subcommittee which reports to the FRCC Operating Committee.

The FRCC provides educational workshops and web based seminars to improve Registered Entity understanding of the FRCC CMEP, NERC Standards Development and CIP topics and trends. These outreach efforts are aimed at improving the effectiveness, understanding of and adherence to NERC reliability initiatives. The workshops also improve the working relationships between the FRCC Regional Entity program areas and the Registered Entities within the FRCC region.

System Operator Certification Program

The FRCC SOS identifies and manages annual training activities for the FRCC System Operators and provides information to FRCC members regarding the NERC training standards and any issues they may have related to system operators obtaining/retaining required NERC Certification.

The training and education program activities are carried out by FRCC's professional/technical staff and SOS members possessing the appropriate technical knowledge and competencies. In addition, vendors that specialize in System Operator training are also used. Providing the FRCC training and education programs helps to achieve a high level of knowledge and competence among the operating personnel in the performance of their reliability-related functions.

Compliance Workshops

Compliance workshops will be held in the spring and fall of 2015 consisting of three (3) sessions each. These workshops will be aimed at providing updates to the Registered Entities on

compliance procedures, instructions on changes to FRCC compliance website, lessons learned for previous violations and providing sufficient and appropriate evidence in a compliance audit. The entities will also be apprised of changes in rules and expectations of NERC and FERC with regard to the CMEP. The effect on compliance monitoring as a result of on-going changes in the NERC and Regional Reliability Standards will also be addressed.

In addition, there will be at least one (1) CIP Compliance Workshop that will address technical aspects of the CIP Reliability Standards, including, providing quality evidence, lessons learned and compliance processes specific to the monitoring and enforcement of the CIP standards. In addition, particular focus will be made on the transition from CIP V3 to CIP V5 standards.

In addition to the face to face venues, in 2015 FRCC compliance staff projects holding at least three (3) webinars (two sessions each) that will address specific topics that may be identified by registered entities or by emerging trends within the FRCC.

Standards Workshops

The FRCC Standards Department will be supporting and participating in various FRCC sponsored workshops (e.g., FRCC Compliance Workshops and FRCC SOS seminars) throughout 2015. The Standards Department contribution to the workshops will be designed to promote stakeholder awareness of Reliability Standards activities as well as education and training for new or revised Reliability Standards. In addition, the FRCC Standards Department plans to hold at least four (4) workshops or webinars that will educate stakeholders on the NERC Reliability Standards Development Procedure, and specific changes to existing reliability standards or specifics on new reliability standards. To help encourage stakeholder participation at the continent-wide level, the workshops will provide stakeholders with details of associated NERC Reliability Standards Development Projects, identifying key areas that may be of concern or interest to the stakeholders and identifying areas that are in need of industry support.

2015 Key Assumptions

- The Operating Personnel Certification program is expected to remain at steady state therefore no significant changes are expected in System Operator Certification CEH requirements through 2015.
- The System Operator Certification Program and Continuing Education Program will continue to be self-funded through a fee based structure for the exams and applications for approval of continuing education activities.
- The Regional Entities are expected to help determine training needs and anticipate areas of support for standards, compliance monitoring and enforcement and information technology (IT) for their staffs and stakeholders.

2015 Goals and Key Deliverables

The training, education and operator certification program objectives for 2015 are outlined below:

- Provide assistance to Regional Entity members in any issues they may have related to System Operator Certification.

- Conduct the annual system operator training seminars over a five (5) week period, with two (2) days each for the training. The training seminars involve from two (2) to four (4) FRCC staff members, as well as industry volunteers who participate as presenters. This activity is funded primarily through registration fees.
- Host FRCC Compliance Workshops and Webinars open to all FRCC Members and Registered Entities aimed at providing updates on compliance procedures, instructions on changes to compliance tools, changes associated with the implementation of the RAI and guidance on the providing of appropriate and sufficient evidence in a compliance audit.
- Host Reliability Standards Workshops and Webinars open to all FRCC Members and Registered Entities aimed at providing information concerning reliability standards under development, as well as the identification of technical concerns or issues that may impact the reliability of the FRCC BES.
- Conduct FRCC Reliability Standards Department presentations to support multiple training objectives (i.e., FRCC Compliance Workshops and FRCC SOS Seminars) to promote stakeholder awareness of continent wide and regional standards activities.
- Work with NERC and the other Regional Entities to achieve improvements in the coordination, content and manner of internal and external training programs.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs and Personnel Expenses is due to more time planned to be spent on training and education of registered entities in elements pertaining to the Reliability Assurance Initiative and in expectation of the transition to CIP Version 5. The increase in personnel expense is also due to a budgeted annual merit increase.
- **Meeting Expenses** – The decrease in Meeting Expenses is due to the anticipation that the cost for the SOS meeting facility will be less than it has been in the past.
- **Operating Expenses** –The increase in Operating Expenses is due to the cost of a security improvement initiative offset by an anticipated decrease in legal fees.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.

Training, Education, and Operator Certification Program

Funding sources and related expenses for the training, education, and operator certification section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital 2014 Budget & Projection, and 2015 Budget

Training, Education and Operator Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 173,812	$ 173,812	$ -	$ 226,344	$ 52,532
Penalty Sanctions	8,499	8,499	-	5,182	(3,317)
Total ERO Funding	**$ 182,310**	**$ 182,310**	**$ -**	**$ 231,525**	**$ 49,215**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	90,000	115,369	25,369	90,000	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 272,310**	**$ 297,679**	**$ 25,369**	**$ 321,525**	**$ 49,215**
Expenses					
Personnel Expenses					
Salaries	$ 83,896	$ 65,388	$ (18,508)	$ 119,243	$ 35,347
Payroll Taxes	5,281	4,171	(1,110)	7,416	2,135
Benefits	11,616	20,293	8,677	14,228	2,612
Retirement Costs	13,325	10,740	(2,585)	19,079	5,754
Total Personnel Expenses	**$ 114,118**	**$ 100,592**	**$ (13,526)**	**$ 159,966**	**$ 45,848**
Meeting Expenses					
Meetings	$ 67,248	$ 38,432	$ (28,816)	$ 52,311	$ (14,937)
Travel	5,996	5,674	(322)	4,616	(1,380)
Conference Calls	5,481	4,013	(1,468)	4,433	(1,048)
Total Meeting Expenses	**$ 78,725**	**$ 48,119**	**$ (30,606)**	**$ 61,360**	**$ (17,365)**
Operating Expenses					
Consultants & Contracts	$ 29,259	$ 51,473	$ 22,214	$ 37,104	$ 7,845
Office Rent	8,945	7,298	(1,647)	11,632	2,687
Office Costs	22,610	26,705	4,095	22,613	3
Professional Services	2,916	853	(2,063)	1,725	(1,191)
Miscellaneous	-	-	-	-	-
Depreciation	590	774	184	1,052	462
Total Operating Expenses	**$ 64,320**	**$ 87,103**	**$ 22,783**	**$ 74,126**	**$ 9,806**
Total Direct Expenses	**$ 257,163**	**$ 235,814**	**$ (21,349)**	**$ 295,452**	**$ 38,289**
Indirect Expenses	**$ 15,410**	**$ 14,055**	**$ (1,355)**	**$ 26,506**	**$ 11,096**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 272,573**	**$ 249,869**	**$ (22,704)**	**$ 321,958**	**$ 49,385**
Change in Assets	**$ (263)**	**$ 47,810**	**$ 48,073**	**$ (433)**	**$ (170)**
Fixed Assets					
Depreciation	$ (590)	$ (774)	$ (184)	$ (1,052)	$ (462)
Total Fixed Asset Purchases	327	140	(187)	619	292
Change in Fixed Assets	**$ 263**	**$ 634**	**$ 371**	**$ 433**	**$ 170**
TOTAL BUDGET	$ 272,310	$ 249,235	$ (23,075)	$ 321,525	$ 49,215
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 48,444**	**$ 48,444**	**$ -**	**$ -**
FTEs	0.67	0.50	(0.17)	0.90	0.23

Situation Awareness and Infrastructure Security Program

Situation Awareness and Infrastructure Security Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.08	0.09	0.01
Direct Expenses	$ 19,932	$ 23,058	$ 3,126
Indirect Expenses	$ 1,840	$ 2,621	$ 781
Inc(Dec) in Fixed Assets	$ (2,392)	$ (2,398)	$ (6)
Total Funding Requirement	$ 19,380	$ 23,281	$ 3,901

Program Scope and Functional Description

The FRCC and the other Regional Entities support the ERO's situational awareness, cyber security preparedness and provide independent reliability information to policy makers and regulators. The Reliability Process for the FRCC Bulk Electric System documents the various reliability roles and functions that are coordinated, monitored and established by FRCC to provide situation awareness of the reliability of the FRCC BES. Two of the primary reliability goals of the FRCC are continuous improvement of the situation awareness of the operators within the FRCC and ensuring that adequate physical, operational and cyber security objectives are in place for the Regions' shared communications networks.

The FRCC supports NERC's situation awareness/event analysis coordination conference calls, the Situation Awareness for FERC, NERC and the Regions (SAFNR) Version 2 project and the FRCC satellite phone for situation awareness.

The NERC Rules of Procedure, Section 1000, requires that NERC monitor present conditions on the BES and provide leadership coordination, technical expertise and assistance to the industry in responding to events as necessary.

The Situation Awareness process will be used to support NERC and FERC's efforts for situation awareness of current system conditions.

2015 Key Assumptions

- NERC's Critical Infrastructure Department will have responsibility for the identification and management of the specialized critical infrastructure protection resources needed to support overall ERO CIP goals and objectives, as well as the specialized CIP resources needs of the other program areas (e.g., Standards, Compliance, Situation Awareness)

- NERC will continue to budget and incur costs to operate and maintain the software applications and systems known as Situational Awareness for NERC, FERC and Regions (SAFNR). NERC will also continue to fund the Grid Security Exercise (GridEx) and the Security Readiness Program to help Registered Entities with CIP compliance and security

awareness. The Regional Entities will be expected to provide subject matter experts for support of these activities.

- NERC will continue to fund, operate and maintain the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), with no increased cost to Regional Entities.

- There will be increased need and demand for CIP-related training and workshops. CIP compliance activities are budgeted within compliance. FRCC will continue to support and facilitate the development of NERC's secure portal for the management of alerts and infrastructure security information.

- There will be continued focus on detecting off-normal events to be analyzed by the responsible entity, FRCC or NERC.

2015 Goals and Key Deliverables

- Ensure that FRCC goals and activities support the mission to provide FERC, NERC and the staffs from the eight Regional Entities a visualization tool that enables the appropriate level of situation awareness for the near real-time conditions on the BES. Continue to work with the FRCC Reliability Coordinator to ensure that SAFNR and appropriate hardware and software resources are allocated. Continue to support future development of the situation awareness project capabilities.
- Issue and track security recommendations to protect the Bulk Power System. Share information learned in Situation Awareness with the Events Analysis program to develop relevant lessons learned.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – There is a de minimus (0.01) increase in FTEs. The increase in personnel expense is due to a budgeted annual merit increase.
- **Operating Expenses** –The increase in Operating Expenses is driven by the cost of a security improvement initiative offset by an anticipated decrease in legal fees.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.

Situation Awareness and Infrastructure Security Program

Funding sources and related expenses for the situation awareness and infrastructure security section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
Situation Awareness and Infrastructure Security

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 18,365	$ 18,365	$ -	$ 22,769	$ 4,404
Penalty Sanctions	1,015	1,015	$ -	512	(502)
Total ERO Funding	**$ 19,380**	**$ 19,380**	**$ -**	**$ 23,281**	**$ 3,901**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 19,380**	**$ 19,380**	**$ -**	**$ 23,281**	**$ 3,901**
Expenses					
Personnel Expenses					
Salaries	$ 10,017	$ 7,735	$ (2,282)	$ 12,256	$ 2,239
Payroll Taxes	631	493	(138)	762	131
Benefits	1,387	1,015	(372)	1,463	76
Retirement Costs	1,591	1,270	(321)	1,961	370
Total Personnel Expenses	**$ 13,626**	**$ 10,513**	**$ (3,113)**	**$ 16,442**	**$ 2,816**
Meeting Expenses					
Meetings	$ 13	$ 18	$ 5	$ 34	$ 21
Travel	69	68	(1)	99	30
Conference Calls	8	21	13	9	1
Total Meeting Expenses	**$ 90**	**$ 107**	**$ 17**	**$ 142**	**$ 52**
Operating Expenses					
Consultants & Contracts	$ 209	$ 234	$ 25	$ 401	$ 192
Office Rent	1,068	863	(205)	1,196	128
Office Costs	2,162	1,540	(622)	2,237	75
Professional Services	346	101	(245)	178	(168)
Miscellaneous	-	-	-	-	-
Depreciation	2,431	2,440	9	2,462	31
Total Operating Expenses	**$ 6,216**	**$ 5,178**	**$ (1,038)**	**$ 6,474**	**$ 258**
Total Direct Expenses	**$ 19,932**	**$ 15,798**	**$ (4,134)**	**$ 23,058**	**$ 3,126**
Indirect Expenses	**$ 1,840**	**$ 1,660**	**$ (180)**	**$ 2,621**	**$ 781**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 21,772**	**$ 17,458**	**$ (4,314)**	**$ 25,679**	**$ 3,907**
Change in Assets	**$ (2,392)**	**$ 1,922**	**$ 4,314**	**$ (2,398)**	**$ (6)**
Fixed Assets					
Depreciation	$ (2,431)	$ (2,440)	$ (9)	$ (2,462)	$ (31)
Total Fixed Asset Purchases	39	17	(22)	64	25
Change in Fixed Assets	**$ 2,392**	**$ 2,423**	**$ 31**	**$ 2,398**	**$ 6**
TOTAL BUDGET	$ 19,380	$ 15,035	$ (4,345)	$ 23,281	$ 3,901
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 4,345**	**$ 4,345**	**$ -**	**$ -**
FTEs	0.08	0.06	(0.02)	0.09	0.01

General and Administrative

General and Administrative (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.36	4.04	0.68
Expenses	$ 623,583	$ 782,663	$ 159,080
Inc(Dec) in Fixed Assets	$ (1,643)	$ -	$ 1,643
Total Allocation to Statutory Programs	$ 621,940	$ 782,663	$ 160,723
Working Capital Requirement	$ (849,875)	$ (657,395)	$ 192,480

Program Scope and Functional Description Background

Charges included in General and Administrative are general legal expenses, executive time and expenses, human resources, information technology and accounting and finance. Every effort is made to charge items and time directly to activities and to designate as statutory or non-statutory. Undesignated items are shared costs between the Regional Entity Division and the Member Services Division and are allocated based on actual labor hours charged.

Legal and Regulatory Background

The FRCC General Counsel serves as the chief legal advisor to the President and CEO, Board of Directors, staff and stakeholders on all legal and regulatory matters affecting the FRCC. FRCC may use additional specialized legal resources on an as-needed basis, such as for tax matters, employee benefit plan issues and significant policy or FERC matters.

2015 Goals and Key Deliverables

- Assist the FRCC in carrying out its responsibilities as required by the approved delegation agreement between NERC and FRCC.
- Provide general corporate legal advice, legal training and timely, accurate filings to Regulatory authorities.

2015 Assumptions

In the 2015 Budget, as in the 2014 and 2013 budgets, there are no specific funds for hearings under CMEP Rules.

Information Technology Background

The FRCC maintains a number of tools and other support services for the benefit of its members, Registered Entities, Reliability Coordinator agent(s) and other system operators. These services include the FRCC Load and Resource Database (LRDB), the Compliance Tracking System (CTS), Compliance Issues Tracking System (CITS), Models on Demand (MOD), the FRCC corporate website, as well as other systems for collaboration, communication, data gathering and analysis.

Several years ago, NERC and the eight (8) Regional Entities formed an executive management group (known as the ERO EMG) which has, among other things, concentrated on developing enterprise-wide IT applications; with a goal of improving efficiency and consistency across NERC and the Regional Entities. As enterprise-wide projects are identified and prioritized by the ERO EMG, they are managed through a single Project Management Office (PMO) at NERC. The PMO has developed an ERO Enterprise application roadmap that will identify projects that NERC and the Regional Entities have agreed upon that are necessary to support improved efficiency and consistency across the ERO.

The NERC IT budget does not supplant the FRCC's need for IT expenditures for specific regional projects, but to the extent that agreed –upon ERO Enterprise applications provide greater efficiencies, there is no unnecessary, redundant expenditures contained in the FRCC business plan and budget.

2015 Goals and Key Deliverables

- Maintain IT and telecommunications systems and resources for efficient utilization of FRCC personnel.
- Improve the physical security of the FRCC office with additional access control and logging.
- Implement updated communications tools and technologies.
- Develop and enhance tools to automate and improve FRCC data collection and analysis processes.
- Expand IT support of the FRCC CMEP and provide additional metrics to improve accuracy and tracking within the CMEP processes.
- Continue the process of Document Management conversion in the Operating and Planning and Administrative programs.
- Implement needed changes to improve the FRCC corporate security posture as identified in the security assessment performed in 2014; improve overall security in all programs, enhance access controls with improved authentication mechanisms and increase security awareness and training.
- Improve disaster recovery and business continuity capabilities by implementing new geographically diverse data recovery solutions.

Human Resources Background

The FRCC has assembled an exceptional team of highly qualified employees to carry out the activities of the FRCC. The human resources department, in adherence with applicable federal and state laws, develops plans, and implements human resources policies and procedures, including staffing, compensation, benefits, employee relations, and training and development.

2015 Goals and Key Deliverables

- Recruit successful employees
- Improve human resource policies and procedures

- Provide management and training programs
- Ensure competitive employee compensation and benefits

Finance and Accounting Background

The FRCC will submit its annual budget for statutory and non-statutory activities to the FRCC Board of Directors for approval and then file the approved annual budget for statutory and non-statutory activities to NERC. This includes supporting materials such as a complete business plan and organizational chart, and the proposed expenditure of funds collected in sufficient detail to justify the requested funding collection and budget expenditures.

The Finance and Accounting Department will: direct the overall financial plans and accounting practices of the organization; oversee treasury, accounting, budget preparation and reporting, tax, and audit activities; and oversee financial and accounting system controls and standards.

2015 Goals and Key Deliverables

- Prepare the 2016 statutory and non-statutory budgets
- Report budget variances to the FRCC Corporate Compliance Finance and Audit Committee, the FRCC Board and to NERC on a quarterly basis
- Evaluate and advise on the impact of long-range planning
- Continue to provide on-going training to employees to ensure employees charge their time correctly
- Carry out succession planning and training in anticipation of retirement of key personnel

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase is the result of a succession plan for an anticipated retirement and the training costs associated with that transition. The increase in personnel expense is also due to a budgeted annual merit increase.
- Operating Expenses –The increase in Operating Expenses is driven by the increased contract costs included in Contracts, Consultants and Software for a security improvement initiative.

General and Administrative

Funding sources and related expenses for the general and administrative section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
General and Administrative

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ (849,875)	$ (849,875)	$ -	$ (657,395)	$ 192,480
Penalty Sanctions			-		
Total ERO Funding	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Expenses					
Personnel Expenses					
Salaries	$ 420,733	$ 462,932	$ 42,199	$ 533,458	$ 112,725
Payroll Taxes	26,482	29,533	3,051	33,175	6,693
Benefits	58,253	57,398	(855)	62,568	4,315
Retirement Costs	65,227	74,173	8,946	85,353	20,126
Total Personnel Expenses	**$ 570,695**	**$ 624,036**	**$ 53,341**	**$ 714,554**	**$ 143,859**
Meeting Expenses					
Meetings	$ -	$ -	$ -	$ -	$ -
Travel	-	-	-	-	-
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Operating Expenses					
Consultants & Contracts	$ 2,547	$ 3,202	$ 655	$ 11,301	$ 8,754
Office Rent	44,857	51,666	6,809	52,037	7,180
Office Costs	3,841	1,807	(2,034)	4,771	930
Professional Services	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	1,643	-	(1,643)	-	(1,643)
Total Operating Expenses	**$ 52,888**	**$ 56,675**	**$ 3,787**	**$ 68,109**	**$ 15,221**
Total Direct Expenses	**$ 623,583**	**$ 680,711**	**$ 57,128**	**$ 782,663**	**$ 159,080**
Indirect Expenses	**$ (623,583)**	**$ (680,711)**	**$ (57,128)**	**$ (782,663)**	**$ (159,080)**
Other Non-Operating Expenses	$ -	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Change in Assets	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Fixed Assets					
Depreciation	$ (1,643)	$ -	$ 1,643	$ -	1,643
Total Fixed Asset Purchases	-	-	-	-	-
Change in Fixed Assets	**$ 1,643**	**$ -**	**$ (1,643)**	**$ -**	**$ (1,643)**
TOTAL BUDGET	$ -	$ -	$ 1,643	$ -	$ 1,643
TOTAL CHANGE IN WORKING CAPITAL	**$ (849,875)**	**$ (849,875)**	**$ (1,643)**	**$ (657,395)**	**$ 190,837**
FTEs	3.36	3.57	0.21	4.04	0.68

Section B – Supplemental Financial Information
2015 Business Plan and Budget

Reserve Balance

Table B-1

Working Capital Reserve Analysis 2014-2015		
STATUTORY		
Beginning Working Capital Reserve (Deficit), December 31, 2013		1,966,888
Less: Penalty sanctions being held to be used as offset to 2015 assessments	[1]	**(153,000)**
Plus: 2014 ERO Funding (from LSEs or designees)		5,488,058
Plus: Projected 2014 Other funding sources		139,369
Plus: Penalty Sanctions Applied		343,000
Less: 2014 Projected expenses & capital expenditures		**(6,530,067)**
Projected Working Capital Reserve Surplus/(Deficit), December 31, 2014		**1,254,248**
Desired Working Capital Reserve, December 31, 2015	[2]	596,853
Less: Projected Working Capital Reserve, December 31, 2014		**(1,254,248)**
Increase(decrease) in assessments to achieve desired Working Capital Reserve		**(657,395)**
2015 Assessment for Expenses and Capital Expenditures		7,162,233
Less: Penalty Sanctions	[1]	**(153,000)**
Less: Other Funding Sources		**(114,000)**
Adjustment to achieve desired Working Capital Reserve		**(657,395)**
2015 Assessment		6,237,838

[1] Represents collections prior to June 30, 2014.

[2] On June 26, 2013, the FRCC Board of Directors set a working capital and operating working capital and operating reserve requirement of one (1) month of the total annual budget. The FRCC has a $1.5 million line of credit.

Breakdown by Statement of Activity Sections

The following detailed schedules are in support of the Table on page 13, of the 2015 FRCC Business Plan and Budget. All significant variances have been disclosed by program area in the preceding pages.

Penalty Sanctions

Penalty monies received prior to June 30, 2014 are to be used to offset assessments in the 2015 Budget, as documented in the NERC Policy – ACCOUNTING, FINANCIAL STATEMENT AND BUDGETARY TREATMENT OF PENALTIES IMPOSED AND RECEIVED FOR VIOLATIONS OF RELIABILITY STANDARD. Penalty monies received from July 1, 2014 through June 30, 2015 will be used to offset assessments in the 2016 Budget.

All penalties received prior to June 30, 2014 are detailed below.

Allocation Method: Penalty sanctions received have been allocated to the following statutory programs to reduce assessments: Reliability Standards; Compliance Monitoring & Enforcement and Organization Registration & Certification; Reliability Assessments and Performance Analysis; Training, Education and Operator Certification; and Situation Awareness and Infrastructure Security. Penalty sanctions are allocated based upon the number of FTEs in the Program divided by the aggregate total FTEs in the Programs receiving the allocation.

Table B-2

Penalty Sanctions Received On or Prior to June 30, 2014	Date Received	Amount Received
Penalty #1	10/25/2013	$ 38,000
Penalty #2	11/26/2013	100,000
Penalty #3	12/27/2013	7,000
Penalty #4	1/22/2014	2,000
Penalty #5	1/22/2014	2,000
Penalty #5	3/25/2014	4,000
Total Penalties Received		$ 153,000

Supplemental Funding

Table B-3

Outside Funding Breakdown By Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget
Reliability Standards Development				
Total	$ -	$ -	$ -	$ -
Compliance Monitoring, Enforcement & Org. Registration	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Reliability Assessment and Performance Analysis				
Services & Software Fees	$ 24,000	$ 24,000	$ 24,000	$ -
	-	-	-	-
Total	$ 24,000	$ 24,000	$ 24,000	$ -
Training, Education and Operator Certification				
Workshops	$ 90,000	$ 115,369	$ 90,000	$ -
Total	$ 90,000	$ 115,369	$ 90,000	$ -
Situation Awareness and Infrastructure Security	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
General and Administrative*				
Interest	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Total Outside Funding	$ 114,000	$ 139,369	$ 114,000	$ -

Assumes that no appreciable excess cash will be in the Bank Accounts and due to current low interest rates, no Interst is being budgeted.

Personnel Expenses

Table B-4

Personnel Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Salaries					
Total Salaries	$ 3,806,631	$ 3,630,346	$ 4,082,307	$ 275,676	7.24%
Total Payroll Taxes	$ 239,599	$ 231,599	$ 253,874	$ 14,275	5.96%
Benefits					
Workers Compensation	$ 10,241	$ 10,006	$ 11,179	$ 938	9.16%
Medical, LTD, STD Insurances	483,409	418,850	445,548	(37,861)	-7.83%
Employment Fees	-		-	-	
Education	100,319	88,994	100,676	357	0.36%
Employee Welfare & Contract Labor	18,936	55,671	22,080	3,144	16.60%
Relocation	44,350	35,000		(44,350)	-100.00%
Total Benefits	$ 657,255	$ 608,521	$ 579,483	$ (77,772)	-11.83%
Retirement					
Retirement Costs	$ 602,881	$ 594,403	$ 666,669	$ 63,788	10.58%
		-		-	
Total Retirement	$ 602,881	$ 594,403	$ 666,669	$ 63,788	10.58%
Total Personnel Costs	$ 5,306,366	$ 5,064,869	$ 5,582,333	$ 275,967	5.20%
FTEs	30.40	27.97	30.91	0.5	1.68%
Cost per FTE					
Salaries	$ 125,218	$ 129,794	$ 132,071	6,853	5.47%
Payroll Taxes	7,882	8,280	8,213	332	4.21%
Benefits	21,620	21,756	18,747	(2,873)	-13.29%
Retirement	19,832	21,251	21,568	1,736	8.76%
Total Cost per FTE	**$ 174,552**	**$ 181,082**	**$ 180,600**	**$ 6,048**	**3.46%**

Consultants and Contracts

Table B-5

Contracts & Consultants and Software & Licenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Contracts & Consultants and Software & Licenses					
Reliability Standards Development	$ 4,529	$ 5,222	$ 7,381	$ 2,852	62.97%
Compliance Monitoring & Enforcement and Org Reg	119,235	225,494	214,984	95,749	80.30%
Reliability Assessment and Performance Analysis	192,989	130,637	122,547	(70,442)	-36.50%
Training, Education and Operator Certification	29,259	51,473	37,104	7,845	26.81%
Situation Awareness and Infrastructure Security	209	234	401	192	91.87%
General and Administrative	2,547	3,202	11,301	8,754	343.70%
Total Contracts & Consultants and Software & Licenses	$ 348,768	$ 416,262	$ 393,718	$ 44,950	12.89%

"The amount for Consultants & Contracts in the Compliance Monitoring and Enforcement Program includes $16,000 in the 2014 budget, $25,500 in the projected 2014 and $3,500 in the 2015 budget estimated by SERC as the costs for SERC to perform compliance monitoring and enforcement responsibilities for the FRCC registered functions."

Office Rent

Table B-6

Office Rent	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Office Rent	$ 555,089	$ 554,412	$ 547,586	$ (7,503)	-1.35%
Total Office Rent	**$ 555,089**	**$ 554,412**	**$ 547,586**	**$ (7,503)**	**-1.35%**

Office Costs

Table B-7

Office Costs	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Telephone	$ 50,931	$ 49,865	$ 43,767	$ (7,164)	-14.07%
Internet	2,618	2,566	4,020	$ 1,402	53.55%
Office Supplies	14,172	19,313	17,719	$ 3,547	25.03%
Computer Supplies	4,226	4,191	9,322	$ 5,096	120.59%
Publications, Subscriptions & Dues	9,710	7,445	13,533	$ 3,823	39.37%
Postage	1,558	1,528	1,523	$ (35)	-2.25%
Equipment Maintenance	930	917	6,750	$ 5,820	625.81%
Copying	-			$ -	
Printing	23,166	26,334	21,069	$ (2,097)	-9.05%
Stationary Forms				$ -	
Commerical Insurance	11,032	10,815	14,366	$ 3,334	30.22%
Miscellaneous				$ -	
Total Office Costs	**$ 118,343**	**$ 122,974**	**$ 132,069**	**$ 13,726**	**11.60%**

Professional Services

Table B-8

Professional Services	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Outside Legal	$ 100,000	$ 25,000	$ 35,000	$ (65,000)	-65.00%
Accounting & Auditing Fees	16,642	16,315	16,324	$ (318)	-1.91%
Total Services	**$ 116,642**	**$ 41,315**	**$ 51,324**	**$ (65,318)**	**-56.00%**

Other Non-Operating Expenses

Table B-9

Other Non-Operating Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Interest Expense	$ -	$ -		$ -	
Office Relocation	-	-		$ -	
Total Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	

2015, 2016 and 2017 Projections

Table B-10

Statement of Activities and Capital Expenditures
2015, 2016 and 2017 Projections
Regional Entity

	2014 Budget	2015 Budget	$ Change 2015:2014 Over(Under)	% Chg 2015:2014 Over(Under)	2016 Projection	$ Change 2016:2015 Over(Under)	% Chg 2016:2015 Over(Under)	2017 Projection	$ Change 2017:2016 Over(Under)	% Chg 2017:2016 Over(Under)
Funding										
ERO Funding										
ERO Assessments	$ 5,488,057	$ 6,237,838	$ 749,781	13.66%	$ 7,271,064	$ 1,033,226	16.56%	$ 7,506,418	$ 235,354	3.24%
Penalty Sanctions	343,000	153,000	(190,000)	0.00%	-		-100.00%	-	-	
Total ERO Funding	**$ 5,831,057**	**$ 6,390,838**	**$ 559,781**	9.60%	**$ 7,271,064**	**$ 1,033,226**	13.77%	**$ 7,506,418**	**$ 235,354**	3.24%
Membership Dues	$ -	$ -	$ -		$ -	$ -		$ -	$ -	
Testing Fees	-	-	-		-	-		-	-	
Services & Software	24,000	24,000	-	0.00%	24,000	-	0.00%	24,000	-	0.00%
Workshops	90,000	90,000	-	0.00%	90,000	-	0.00%	90,000	-	0.00%
Interest	-	-	-		-	-		-	-	
Miscellaneous	-	-	-		-	-		-	-	
Total Funding	**$ 5,945,057**	**$ 6,504,838**	**$ 559,781**	9.42%	**$ 7,385,064**	**$ 1,033,226**	13.53%	**$ 7,620,418**	**$ 235,354**	3.19%
Expenses										
Personnel Expenses										
Salaries	$ 3,806,631	$ 4,082,307	$ 275,676	7.24%	$ 4,204,776	$ 122,469	3.00%	$ 4,330,919	$ 126,143	3.00%
Payroll Taxes	239,599	253,874	14,275	5.96%	261,490	7,616	3.00%	269,335	7,845	3.00%
Benefits	657,255	579,483	(77,772)	-11.83%	594,062	14,579	2.52%	609,082	15,020	2.53%
Retirement Costs	602,881	666,669	63,788	10.58%	686,264	19,595	2.94%	706,447	20,183	2.94%
Total Personnel Expenses	**$ 5,306,366**	**$ 5,582,333**	**$ 275,967**	5.20%	**$ 5,746,592**	**$ 164,259**	2.94%	**$ 5,915,783**	**$ 169,191**	2.94%
Meeting Expenses										
Meetings	$ 80,930	$ 69,292	$ (11,638)	-14.38%	$ 69,588	$ 296	0.43%	$ 69,892	$ 304	0.44%
Travel	167,209	191,753	24,544	14.68%	192,612	859	0.45%	193,497	885	0.46%
Conference Calls	18,771	9,482	(9,289)	-49.49%	9,564	82	0.86%	9,648	84	0.88%
Total Meeting Expenses	**$ 266,910**	**$ 270,527**	**$ 3,617**	1.36%	**$ 271,764**	**$ 1,237**	0.46%	**$ 273,037**	**$ 1,273**	0.47%
Operating Expenses										
Consultants & Contracts	$ 348,768	$ 393,718	$ 44,950	12.89%	$ 422,443	$ 28,725	7.30%	$ 448,117	$ 25,674	6.08%
Office Rent	555,089	547,586	(7,503)	-1.35%	559,532	11,946	2.18%	571,837	12,305	2.20%
Office Costs	118,343	132,069	13,726	11.60%	134,291	2,222	1.68%	136,578	2,287	1.70%
Professional Services	116,642	51,324	(65,318)	-56.00%	52,864	1,540	3.00%	54,450	1,586	3.00%
Miscellaneous	-	-	-		-	-		-	-	
Depreciation	110,490	202,287	91,797	83.08%	202,897	610	0.30%	203,525	628	0.31%
Total Operating Expenses	**$ 1,249,332**	**$ 1,326,984**	**$ 77,652**	6.22%	**$ 1,372,027**	**$ 45,043**	3.39%	**$ 1,414,507**	**$ 42,480**	3.10%
Total Direct Expenses	**$ 6,822,608**	**$ 7,179,844**	**$ 357,236**	5.24%	**$ 7,390,383**	**$ 210,539**	2.93%	**$ 7,603,327**	**$ 212,944**	2.88%
Indirect Expenses	**$ (1,643)**	$ 0	$ 1,643		**$ 0**	**$ 1,643**	0.00%	**$ -**	**$ 212,944**	-100.00%
Other Non-Operating Expenses	**$ -**	$ -	$ -		**$ -**	**$ -**		**$ -**	**$ -**	
Total Expenses	**$ 6,820,965**	**$ 7,179,844**	**$ 358,879**	5.26%	**$ 7,390,383**	**$ 212,182**	2.93%	**$ 7,603,327**	**$ 425,889**	2.88%
Change in Assets	**$ (875,908)**	**$ (675,006)**	**$ 200,902**	-22.94%	**$ (5,319)**	**$ 821,044**	-99.21%	**$ 17,091**	**$ (190,534)**	-421.32%
Fixed Assets										
Depreciation	$ (110,490)	$ (202,287)	$ (91,797)	83.08%	$ (202,897)	$ (610)	0.30%	$ (203,525)	$ (628)	0.31%
Total Fixed Asset Purchases	82,814	184,676	101,862	123.00%	197,578	12,902	6.99%	220,616	23,038	11.66%
								-	-	
Change in Fixed Assets	**$ 27,676**	**$ 17,611**	**$ (10,065)**	-36.37%	**$ 5,319**	**$ (12,292)**	-69.80%	**$ (17,091)**	**$ (22,410)**	-421.32%
TOTAL BUDGET	$ 6,793,289	$ 7,162,233	$ 368,944	5.43%	$ 7,385,064	$ 224,474	3.11%	$ 7,620,418	$ 448,299	3.19%
TOTAL CHANGE IN WORKING CAPITAL	**$ (848,232)**	**$ (657,395)**	**$ 190,837**	-22.50%	**$ -**	**$ 808,752**	-100.00%	**$ -**	**$ (212,944)**	
FTEs	30.40	30.91	0.51	1.68%	30.91	-	0.00%	30.91	-	0.00%

Section C – Non-Statutory Activities
2015 Business Plan and Budget

Member Services Activities (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	16.8	18.4	1.5
Direct Expenses	7,454,381	8,422,053	967,672
Indirect Expenses	-	-	-
Inc(Dec) in Fixed Assets	1,614	(30,071)	(31,685)
Total Funding Requirement	7,455,995	8,391,982	935,987

Non-Statutory Functional Scope Background

The Member Services (MS) division of the FRCC provides, coordinates and administers a variety of services relating to the reliable planning and operation of the BES within the FRCC Region. These services are carried out by the FRCC Member Services Planning Committee (PC) and the FRCC Member Services Operating Committee (OC), various subcommittees, task forces and working groups, as well as FRCC Staff.

Member Services Objectives

- Ensure the reliability of the BES in the FRCC region.
- Coordination, planning, operation and maintenance of reliable bulk electricity supply in the FRCC region.

Membership and Governance

The FRCC's Members in the Member Services Division include investor-owned utilities, cooperative utilities, municipal utilities, power marketers and independent power producers. Current membership is 23 FRCC Members in 2014 and is not expected to change in 2015.

The activities of FRCC are directed by its Board of Directors. The Board is comprised of senior level executives from the FRCC membership.

Planning Committee (PC) Functional Scope

The PC promotes the reliability of the BES within the FRCC Region by assessing and encouraging generation and transmission adequacy. The PC assesses generation adequacy by performing a reliability assessment taking into account projected load and resources. The PC, through the FRCC Regional Transmission Planning Process, provides a vehicle for ensuring that transmission planning within the FRCC will provide for the development of a robust transmission network within the FRCC Region. The Regional Transmission Planning Process is a coordinated transmission planning process that evaluates all BES and non-BES transmission facilities. The major goal of this process is to ensure that the planning of transmission facilities

will meet the needs of all market participants in a coordinated, open and transparent transmission planning environment.

The FRCC will continue to develop, on an annual basis, a Regional Transmission Plan following the Regional Transmission Planning Process. The Regional Transmission Planning process will be revised to incorporate the planning principles from FERC Order 1000. The Regional Plan is based on the Ten Year Site Plans that are required to be submitted to the Florida Public Service Commission (FPSC) on April 1st of each year. The FRCC participates in an annual Ten Year Site Plan Workshop held by the FPSC where the results of resource and transmission adequacy assessments are presented.

The FRCC PC relies on the following subordinate groups to achieve its goals: Resource Working Group (RWG), Stability Working Group (SWG), and the Transmission Working Group (TWG).

The PC, supported by FRCC MS staff, has the primary responsibility of the Planning Authority (PA) function including implementation of all applicable PA NERC Reliability Standards.

Resource Working Group
The RWG performs reliability assessments of FRCC resource adequacy for the future 10-year period for peninsular Florida based on individual utility information that was the basis of their respective EIA-411 and Ten Year Site Plan filings with the Florida Public Service Commission. These reliability assessments are based upon the FRCC resource adequacy criteria.

Stability Working Group
The SWG is responsible for assessing the dynamic performance of the FRCC BES under various credible system conditions. In addition, the SWG performs the following assessments and studies: Coordination and performance of Special Protection Systems, the effectiveness of FRCC under-frequency load shedding program and coordination with other protection and control systems, Extreme Event Study and other assessments in support of the FRCC Regional Transmission Planning Process. The SWG annually develops FRCC dynamic models.

Transmission Working Group
The TWG engages in active coordination of transmission planning within the FRCC Region under the direction of the FRCC Planning Committee in support of the FRCC Regional Transmission Planning Process. The TWG annually performs a FRCC Long Range Study, sensitivity studies as directed by the PC, evaluates Transmission Service Requests and evaluates Generator Interconnection Service Requests. In addition, the TWG annually develops a FRCC Transmission Map, FRCC power flow models and FRCC short circuit models.

Operating Committee (OC) Functional Scope

The primary goal of the OC is to promote the reliability of the BES within the FRCC Region. The OC is responsible for the coordination, operations planning, operation and maintenance of the interconnected systems operating in the Region. The OC's primary reliability goals include effective implementation of the Regional Reliability Plan (*Reliability Process for the FRCC Bulk Electric System*), continuous improvement of operator awareness and communications and ensuring that adequate physical, operational and cyber security objectives are in place for the Region's shared communications network. The OC subordinate groups include the Operating

Reliability Subcommittee (ORS), Data Exchange Working Group (DEWG), Fuel Reliability Working Group (FRWG), Operations Planning Working Group (OPWG), Telecommunications Subcommittee (TS), System Protection and Control Subcommittee (SPCS) and the Critical Infrastructure Protection Subcommittee (CIPS). The OC ensures reliable operations are maintained through the implementation and oversight of the FRCC Reliability Coordinator (RC) functions as established in the Regional Reliability Plan.

The FRCC RC responsibilities include the real-time operating function and the next-day operations planning function. The RC tasks are performed by a designated agent of the FRCC with direction and oversight by FRCC committees and support staff. The designated agent performs real-time operations and next-day planning operations. FRCC staff supports Regional reliability by performing the roles of the Operations Planning Coordinator (OPC), and State Capacity Emergency Coordinator (SCEC) as defined in the *Reliability Process for the FRCC Bulk Electric System* document.

The FRCC RC function is accountable to the FRCC OC who has overall responsibility of the administration, development and implementation of operating procedures provided by the ORS for the NERC Operations & Planning (Non-CIP) Standards.

The FRCC continues to improve FRCC PA and RC compliance management programs under the Member Services Division based on the evolving regulatory requirements. The FRCC has improved its oversight of PA and RC functions by creating an independent Member Services Regulatory Department with a dedicated Regulatory Director who reports directly to the FRCC President and CEO and who has direct access to the FRCC Board of Directors. This position is responsible for the implementation, maintenance and oversight of the FRCC Internal Compliance Program (ICP) including all compliance activities for the FRCC registered entity functions and is the primary interface for all regulatory activities associated with the FRCC Member Services committees and is the FRCC liaison between external Compliance Enforcement Authorities.

Operating Reliability Subcommittee (ORS)

The ORS provides overall administration for the development and implementation of operating procedures and other reliability matters including the oversight of the FRCC RC function for Operating and Planning (non-CIP) NERC Standards. The ORS reviews and assesses regional import and export limits, scheduled transmission outages, real-time system reliability, events analysis, information and data exchange and other reliability issues. The ORS provides formal oversight and implementation of the Reliability Process for the FRCC Bulk Electric System which establishes the reliability responsibilities of the various entities within the Region and specifically monitors the agent responsible for performing the RC functions.

Data Exchange Working Group (DEWG)

The DEWG, subordinate to the ORS, supports the real-time data needs of the FRCC Reliability Coordinator and other operating entities. It is also responsible for developing methodologies to facilitate the exchange of real-time, modeling and other operational data to help ensure reliable electric power system operations. Accurate modeling of the FRCC BES is essential to maintaining situation awareness and ensuring reliability. Within the FRCC, operating entities provide system data via the FRCC Reliability Data Link (RDL). The FRCC RDL receives electric system reliability data from the operating entities on a real-time basis and allows the data to be made available.

Fuel Reliability Working Group (FRWG)
The FRWG, also subordinate to the ORS, has been established to deal with matters relating to fuel and impacts to BES reliability. Specifically, the FRWG provides the administrative oversight of a Regional fuel reliability forum that studies the interdependencies of fuel availability and electric reliability and supports coordinated Regional responses to fuel issues and fuel emergencies.

Operations Planning Working Group (OPWG)
The OPWG, as a part of the ORS, has been established to provide oversight, guidelines and procedures to the FRCC Operations Planning Coordinator (OPC) in accordance with the Reliability Process for the FRCC BES document. The OPWG focuses on BES reliability and developing processes and documentation that support regional reliability and adherence to the NERC Reliability Standards as they relate to the OPC function.

FRCC Telecommunications Subcommittee (TS)
The TS provides oversight for the TS budget which is included in the OC budget. The primary purpose of the TS is to ensure that adequate and redundant communications facilities are made available to the operating entities within the FRCC, including the FRCC Reliability Coordinator. The TS administers the FRCC Hotline program, Satellite phone program, and also ensures that reliable and redundant communications are maintained by the Eastern Interconnect Data Sharing Network, Inc. (EIDSN). All TS programs are non-statutory and support the Reliability Coordinator functions; with the exception of the FRCC satellite phone (located at the FRCC office) which is a tool that can be used by the Regional Entity to perform situation awareness and thus is budgeted as statutory.

FRCC System Protection and Control Subcommittee (SPCS)
The FRCC System Protection and Control Subcommittee (SPCS) has primary responsibility for the coordination of protection and control systems within the FRCC region, including regional disturbance monitoring equipment, review of protective mis-operations, protection related disturbance analysis and implementation of specific regional programs and procedures including the assessments of the FRCC Under-Frequency Load Shedding Program. The SPCS also reviews and coordinates system protection and control equipment installations, settings, protection philosophies and testing criteria within the region, when installations impact multiple entities. The SPCS serves as an important forum for sharing subject matter expert guidance and lessons learned / best practices for equipment issues and protection coordination.

FRCC Critical Infrastructure Protection Subcommittee (CIPS)
The purpose of the FRCC CIPS is to enhance the physical and cyber security of the critical BES infrastructure in the FRCC Region, with an emphasis on protecting, preventing, limiting and recovering from malicious activities directed at the FRCC critical energy infrastructure. The CIPS provides guidance to the OC on matters of critical energy infrastructure security, including cyber and physical security. The CIPS provides advice to the OC including implementation of all applicable FRCC RC CIP-002 through CIP-009 Reliability Standards.

Major 2015 Cost Impacts

The FRCC's proposed 2015 Members Services budgeted expenses and net fixed assets are $8,391,982, which is a $935,987 or 12.6% increase over the 2014 budgeted expenses. The cost impacts by function of this increase are:

Planning Committee (PC)
The Member Services Planning Committee (PC) expenses for 2015 are made up of the PC Committee budget, as well as the administrative costs to provide support personnel for implementation of the FRCC Planning Authority (PA) functions and all other Member Services PC activities. In 2015, staff will spend additional time enhancing FRCC steady state planning studies and has budgeted $150,000 for additional stability studies to prepare to meet the requirements of the new NERC Transmission Planning (TPL) Standard. In addition, staff is expected to add one FTE in 2015 to support the implementation of FERC Order 1000 as recommended by the PC.

The 2015 PC budget is developed based on the activities of the Resource Working Group (RWG), the Stability Working Group (SWG) and the Transmission Working Group (TWG). These budgets are primarily for the labor involved in coordination activities performed by member representatives, software and meeting costs.

Operating Committee (OC)
The Member Services Operating Committee (OC) expenses for 2015 are made up of a 2015 OC budget as well as the administrative costs to provide support personnel for implementation of the FRCC Reliability Coordinator (RC) functions and other Member Services OC activities. In 2015, staff will spend additional time coordinating activities with member companies to ensure continued reliability and compliance with changing NERC Reliability Standards.

The 2015 OC budget is developed based primarily on the activities of the Operating Reliability Subcommittee (ORS), the Telecommunications Subcommittee (TS), the Fuel Reliability Working Group (FRWG) and the Critical Infrastructure Protection Subcommittee (CIPS). These budgets are related to, or in support of both the FRCC Reliability Coordinator (RC) and Member Services entity's reliability functions and includes consulting costs, contract costs, computer software purchases and expenses to support the associated activities. These budgets do not include FRCC staff salaries or associated personnel costs.

The administrative costs associated with the FRCC OC support personnel include FRCC staff that support implementation of the FRCC RC functions and staff that support overall OC activities. The staff includes dedicated employees as well as shared employees.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs is attributed to an additional employee in the planning area to support new long range planning activities, the effect of a complete year for the 2014 addition to staff to support the Reliability Coordinator function that was budgeted to be filled in mid-2014 and the result of the implementation of a succession plan for a key accounting position.
- **Operating Expenses** – The increase in Operating Expenses is attributed to increases in consultant and contractor costs for the RC and PA functions.

2014 Member Services Budget and Projection and 2015 Budget Comparisons

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
NON-STATUTORY MEMBER SERVICES

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -	$ -	$ -
Penalty Sanctions	-	-	-	-	-
Total ERO Funding	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Membership Dues	$ 6,916,762	$ 6,916,762	$ -	8,240,106	1,323,344
Testing Fees	-	-	-	-	-
Services & Software	277,419	312,531	35,112	254,459	(22,960)
Workshops	-	-	-	20,000	20,000
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 7,194,181**	**$ 7,229,293**	**$ 35,112**	**$ 8,514,565**	**$ 1,320,384**
Expenses					
Personnel Expenses					
Salaries	$ 2,108,824	$ 2,134,834	$ 26,010	$ 2,423,514	$ 314,690
Payroll Taxes	132,734	136,193	3,459	150,716	17,982
Benefits	350,795	320,232	(30,563)	351,746	951
Retirement Costs	328,267	343,386	15,119	387,762	59,495
Total Personnel Expenses	**$ 2,920,620**	**$ 2,934,645**	**$ 14,025**	**$ 3,313,738**	**$ 393,118**
Meeting Expenses					
Meetings	$ 37,515	$ 39,955	$ 2,440	$ 26,582	$ (10,933)
Travel	63,716	55,451	(8,265)	60,205	(3,511)
Conference Calls	27,108	30,959	3,851	45,286	18,178
Total Meeting Expenses	**$ 128,339**	**$ 126,365**	**$ (1,974)**	**$ 132,073**	**$ 3,734**
Operating Expenses					
Consultants & Contracts	$ 3,657,668	$ 3,843,855	$ 186,187	$ 4,260,160	$ 602,492
Office Rent	224,835	238,262	13,427	236,403	11,568
Office Costs	419,112	472,831	53,719	375,314	(43,798)
Professional Services	79,910	35,385	(44,525)	45,476	(34,434)
Miscellaneous	-	75,000	75,000	-	-
Depreciation	23,897	45,496	21,599	58,889	34,992
Total Operating Expenses	**$ 4,405,422**	**$ 4,710,829**	**$ 305,407**	**$ 4,976,242**	**$ 570,820**
Total Direct Expenses	**$ 7,454,381**	**$ 7,771,839**	**$ 317,458**	**$ 8,422,053**	**$ 967,672**
Indirect Expenses	$ -	$ -	**$ -**	**$ -**	**$ -**
Other Non-Operating Expenses	$ -	$ -	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 7,454,381**	**$ 7,771,839**	**$ 317,458**	**$ 8,422,053**	**$ 967,672**
Change in Assets	**$ (260,200)**	**$ (542,546)**	**$ (282,346)**	**$ 92,512**	**$ (352,712)**
Fixed Assets					
Depreciation	$ (23,897)	$ (45,496)	$ (21,599)	$ (58,889)	$ (34,992)
Total Fixed Asset Purchases	25,511	78,929	53,418	28,818	3,307
	-	-			
Change in Fixed Assets	**$ (1,614)**	**$ (33,433)**	**$ (31,819)**	**$ 30,071**	**$ 31,685**
TOTAL BUDGET	$ 7,455,995	$ 7,805,272	$ 349,277	$ 8,391,982	$ 935,987
TOTAL CHANGE IN WORKING CAPITAL	**$ (261,814)**	**$ (575,979)**	**$ (314,165)**	**$ 122,583**	**$ 384,397**
FTEs	16.84	15.73	(1.11)	18.35	1.51

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
NON-STATUTORY						
Operational Programs						
Operations Committee	10.48	9.94		10.27	10.27	-0.21
Planning Committee	3.27	3.52		4.57	4.57	1.30
Total FTEs Operational Programs	**13.75**	**13.46**	**0.00**	**14.84**	**14.84**	**1.09**
Administrative Programs						
General & Administrative	3.09	2.99		3.51	3.51	0.42
Total FTEs Administrative Programs	**3.09**	**2.99**	**0.00**	**3.51**	**3.51**	**0.42**
Total FTEs	**16.84**	**16.45**	**0.00**	**18.35**	**18.35**	**1.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

Member Services Reserve Analysis — 2014 – 2015

Working Capital Reserve Analysis 2014-2015 NON-STATUTORY MEMBER SERVICES		
Beginning Working Capital Reserve (Deficit), December 31, 2013		587,073
Change in Post Retirement Benefit Obligation - Noncash Item		565,655
2014 Funding (from members)		6,916,762
2014 Projected Other funding sources		312,531
Total Cash Available 2014		8,382,021
Less: '2014 Projected expenses & capital expenditures		**(7,805,272)**
Projected Working Capital Reserve Surplus/(Deficit), December 31, 2014		**576,749**
Desired Working Capital Reserve, December 31, 2015	[1]	699,332
Less: Projected Working Capital Reserve, December 31, 2014		**(576,749)**
Increase(decrease) in assessments to achieve desired Working Capital Reserve		**122,583**
2015 Funding for Expenses and Capital Expenditures		8,391,982
Less: Other Funding Sources		**(274,459)**
Adjustment to achieve desired Working Capital Reserve		**122,583**
2015 Funding (reserve adjustment)		8,240,106

[1] On June 26, 2013, the FRCC Board of Directors set a working capital and operating working capital and operating reserve requirement of one (1) month of the total annual budget. The FRCC has a $1.5 million line of credit.

Section D – Additional Consolidated Financial Statements

2015 Business Plan and Budget

Section D — 2015 Additional Consolidated Financial Information

		Functions in Delegation Agreement							Non-Statutory Functions		
Statement of Activities and Capital Expenditures by Program 2014 Budget	Total	Statutory Total	Reliability Standards Development (Section 300)	Compliance Monitoring and Org Reg % Cert(Section 400 & 500)	Reliability Assessment and Performance Analysis (Section 800)	Training and Education (Section 900)	Situation Awareness and Infrastructure Security (Section 1000)	General and Administrative	Non-Statutory Total	Operating Committee	Planning Committee
Funding											
ERO Funding											
ERO Assessments	$ 6,237,838	$ 6,237,838	$ 413,407	$ 5,099,302	$ 1,133,412	$ 226,344	$ 22,769	$ (657,395)	$ -	$ -	$ -
Penalty Sanctions	153,000	153,000	9,737	112,572	24,997	5,182	512		-	-	-
Total ERO Funding	**6,390,838**	**6,390,838**	**423,143**	**5,211,874**	**1,158,409**	**231,525**	**23,281**	**(657,395)**	**-**	**-**	**-**
Membership Dues	$ 8,240,106	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 8,240,106	$ 6,792,087	$ 1,448,019
Testing Fees	-	-							-		
Services & Software	278,459	24,000			24,000				254,459	254,459	
Workshops	110,000	90,000				90,000			20,000	20,000	
Interest	-	-							-		
Miscellaneous	-	-							-		
Total Funding	**$ 15,019,403**	**$ 6,504,838**	**$ 423,143**	**$ 5,211,874**	**$ 1,182,409**	**$ 321,525**	**$ 23,281**	**$ (657,395)**	**$ 8,514,565**	**$ 7,066,546**	**$ 1,448,019**
Expenses											
Personnel Expenses											
Salaries	$ 6,505,821	$ 4,082,307	$ 225,465	$ 2,611,174	$ 580,711	$ 119,243	$ 12,256	$ 533,458	$ 2,423,514	$ 1,676,219	$ 747,295
Payroll Taxes	404,590	253,874	14,021	162,386	36,114	7,416	762	33,175	150,716	104,243	46,473
Benefits	931,229	579,483	32,602	385,976	82,646	14,228	1,463	62,568	351,746	235,709	116,037
Retirement Costs	1,054,431	666,669	36,074	431,288	92,914	19,079	1,961	85,353	387,762	268,195	119,567
Total Personnel Expenses	$ 8,896,071	$ 5,582,333	**$ 308,162**	**$ 3,590,824**	**$ 792,385**	**$ 159,966**	**$ 16,442**	**$ 714,554**	$ 3,313,738	$ 2,284,366	$ 1,029,372
Meeting Expenses											
Meetings	$ 95,874	$ 69,292	$ 2,606	$ 12,729	$ 1,612	$ 52,311	$ 34		$ 26,582	$ 18,286	$ 8,296
Travel	251,958	191,753	17,469	122,194	47,375	4,616	99		60,205	53,700	6,505
Conference Calls	54,768	9,482	203	4,390	447	4,433	9		45,286	30,491	14,795
Total Meeting Expenses	$ 402,600	$ 270,527	**$ 20,278**	**$ 139,313**	**$ 49,434**	**$ 61,360**	**$ 142**	**$ -**	$ 132,073	$ 102,477	$ 29,596
Operating Expenses											
Consultants & Contracts	$ 4,653,878	$ 393,718	$ 7,381	$ 214,984	$ 122,547	$ 37,104	$ 401	$ 11,301	$ 4,260,160	$ 4,036,905	$ 223,255
Office Rent	783,989	547,586	21,993	404,082	56,646	11,632	1,196	52,037	236,403	163,508	72,895
Office Costs	507,383	132,069	7,681	80,150	14,617	22,613	2,237	4,771	375,314	351,537	23,777
Professional Services	96,800	51,324	3,261	37,762	8,398	1,725	178		45,476	31,435	14,041
Miscellaneous	-	-							-		
Depreciation	261,176	202,287	1,633	191,775	5,365	1,052	2,462		58,889	50,230	8,659
Total Operating Expenses	$ 6,303,226	$ 1,326,984	**$ 41,949**	**$ 928,753**	**$ 207,573**	**$ 74,126**	**$ 6,474**	**$ 68,109**	$ 4,976,242	$ 4,633,615	$ 342,627
Total Direct Expenses	**$ 15,601,897**	**$ 7,179,844**	**$ 370,389**	**$ 4,658,890**	**$ 1,049,392**	**$ 295,452**	**$ 23,058**	**$ 782,663**	**$ 8,422,053**	**$ 7,020,458**	**$ 1,401,595**
Indirect Expenses	-	-	**49,808**	**575,856**	**127,871**	**26,506**	**2,621**	**(782,663)**			
Other Non-Operating Expenses	-	-	-	-	-	-	-	-	-	-	-
Total Expenses	**$ 15,601,897**	**$ 7,179,844**	**$ 420,197**	**$ 5,234,746**	**$ 1,177,263**	**$ 321,958**	**$ 25,679**	**$ -**	**$ 8,422,053**	**$ 7,020,458**	**$ 1,401,595**
Change in Assets	**$ (582,494)**	**$ (675,006)**	**$ 2,946**	**$ (22,872)**	**$ 5,146**	**$ (433)**	**$ (2,398)**	**$ (657,395)**	**$ 92,512**	**$ 46,088**	**$ 46,424**
Fixed Assets											
Depreciation	$ (261,176)	$ (202,287)	$ (1,633)	$ (191,775)	$ (5,365)	$ (1,052)	$ (2,462)	$ -	$ (58,889)	$ (50,230)	$ (8,659)
Total Fixed Asset Purchases	213,494	184,676	4579	168,903	10,511	619	64		28,818	11,545	17,273
Change in Fixed Assets	**$ 47,682**	**$ 17,611**	**$ (2,946)**	**$ 22,872**	**$ (5,146)**	**$ 433**	**$ 2,398**	**$ -**	**$ 30,071**	**$ 38,685**	**$ (8,614)**
TOTAL CHANGE IN WORKING CAPITAL	**$ (534,812)**	**$ (657,395)**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ (657,395)**	**$ 122,583**	**$ 84,773**	**$ 37,810**

Statement of Financial Position

Statement of Financial Position
2013 Audited, 2014 Projection, 2015 Budget and 2016 Projected

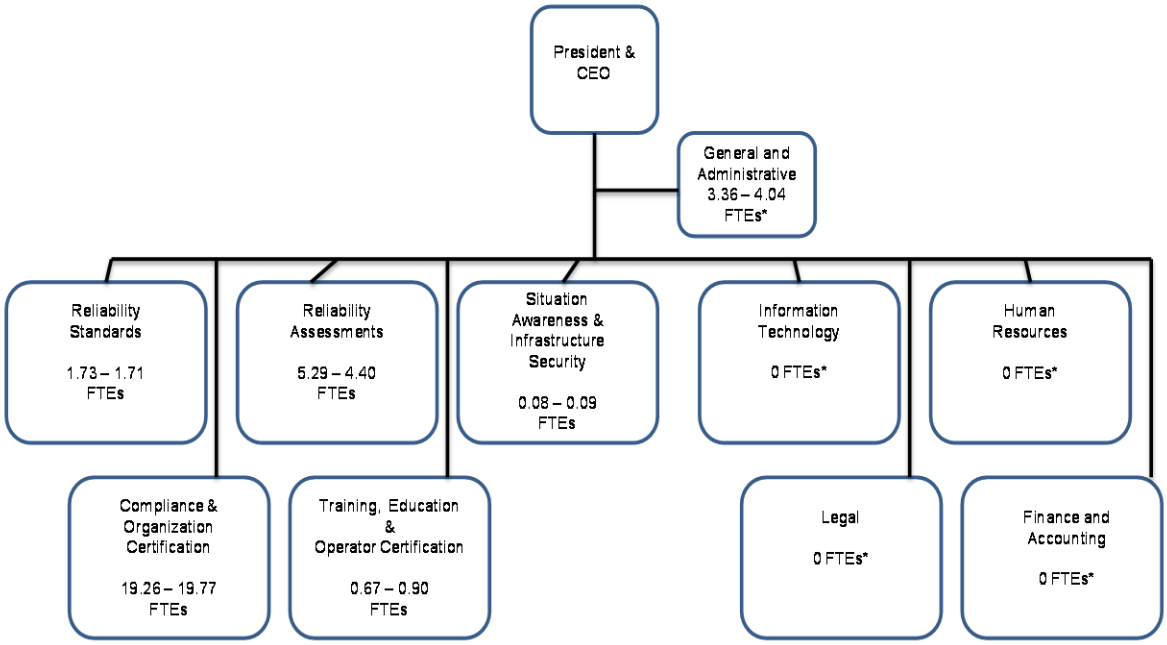
STATUTORY and NON-STATUTORY

	(Per Audit) 12/31/2013	Projected 12/31/2014	Budget 12/31/2015	Projected 12/31/2016
ASSETS				
Cash	6,558,632	4,763,059	3,577,263	3,665,908
Accounts receivable	2,855,070	2,955,070	3,155,070	3,355,070
Other receivables	-	-	-	-
Prepaid expenses and other current assets	18,526	15,000	15,000	15,000
Other Assets	259,175	150,000	150,000	150,000
Property and equipment (net of depreciation)	418,454	300,000	300,000	300,000
Total Assets	**10,109,857**	**8,183,129**	**7,197,333**	**7,485,978**
LIABILITIES AND NET ASSETS				
Liabilities				
Accounts payable and accrued expenses	2,556,119	2,540,000	1,800,000	1,900,000
Deferred income	3,111,955	3,657,736	3,846,312	3,957,406
Compliance Penalty Assessment	481,000	-	-	-
Accrued postretirement benefits obligation	1,406,822	1,477,163	1,551,021	1,628,572
Total Liabilities	**7,555,896**	**7,674,899**	**7,197,333**	**7,485,978**
Net Assets - unrestricted	2,553,961	508,230	-	-
Total Liabilities and Net Assets	**10,109,857**	**8,183,129**	**7,197,333**	**7,485,978**

Statutory Organizational Chart

Florida Reliability Coordinating Council, Inc.
Statutory Organization Chart

2014 Budgeted FTEs 30.40
2015 Budgeted FTEs 30.91



*All FTEs for Information Technology, Legal, Finance, and Human Resources, are recorded within General and Administrative

FRCC
Florida Reliability Coordinating Council, Inc.

FRCC 2015 Business Plan & Budget

(As Submitted to NERC and Posted for Comments on 5/16/2014)

(Not Approved by the FRCC Board of Directors)

NERC and Regional Entity Meeting with the NERC FAC

May 21, 2014

Reva R. Maskewitz - Controller

2015 Regional Entity Division Personnel Comparison

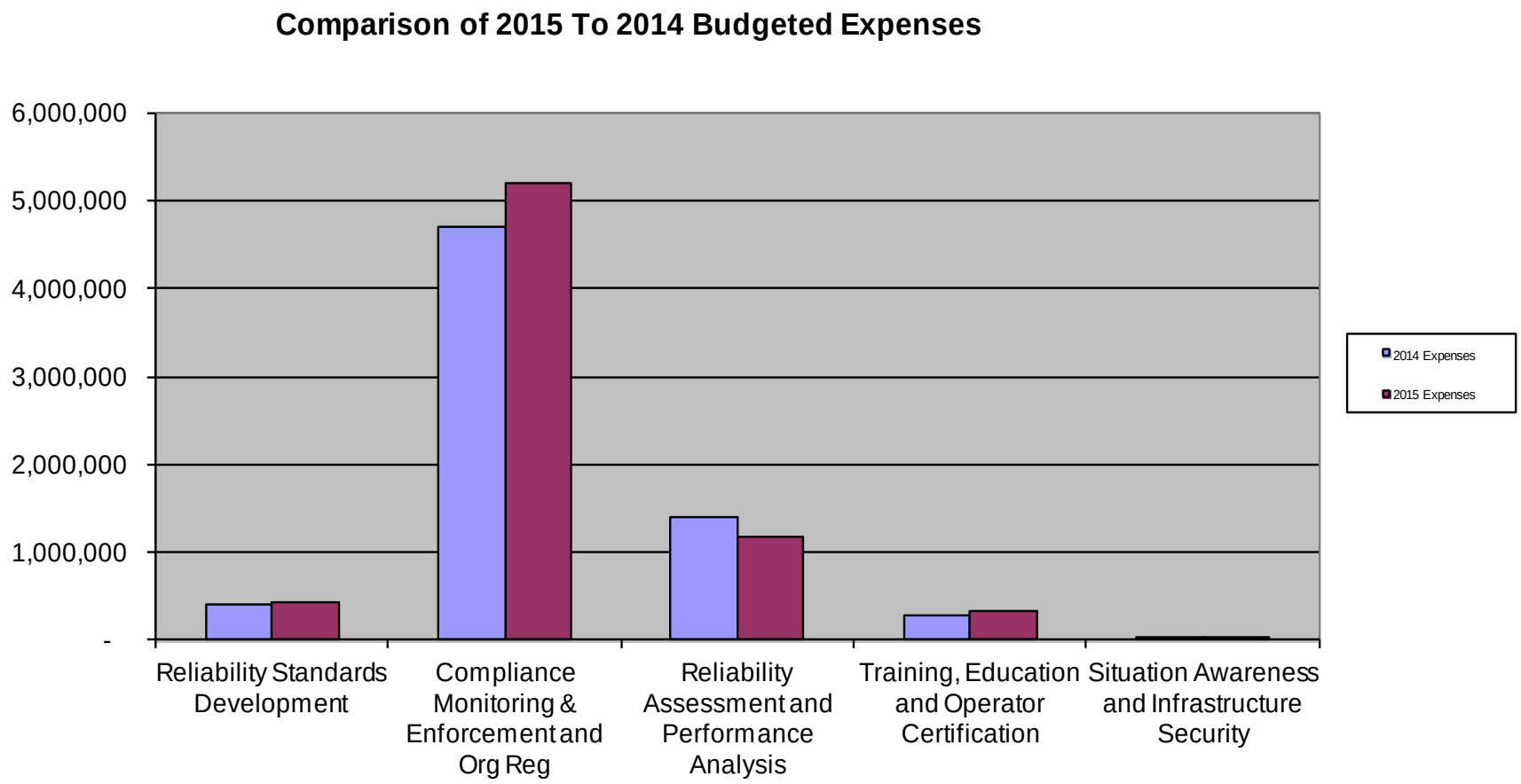
Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
STATUTORY						
Operational Programs						
Reliability Standards Development	1.74	1.33	1.71		1.71	-0.03
Compliance Monitoring & Enforcement and Org Reg	19.26	18.25	19.77		19.77	0.51
Reliability Assessment and Performance Analysis	5.29	4.26		4.40	4.40	-0.89
Training, Education and Operator Certification	0.67	0.50		0.90	0.90	0.23
Situation Awareness and Infrastructure Security	0.08	0.06		0.09	0.09	0.01
Total FTEs Operational Programs	**27.04**	**24.40**	**21.48**	**5.39**	**26.87**	**-0.17**
Administrative Programs						
General & Administrative	3.36	3.57		4.04	4.04	0.68
Total FTEs Administrative Programs	**3.36**	**3.57**	**0.00**	**4.04**	**4.04**	**0.68**
Total FTEs	**30.40**	**27.97**	**21.48**	**9.43**	**30.91**	**0.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

2015 RE Division Total Funding by Program Area

	2014	2015	% Change 2015:2014	$ Change 2015:2014
Reliability Standards Development	409,591	423,143	3.3%	13,552
Compliance Monitoring and Enforcement	4,700,708	5,211,874	10.9%	511,166
Reliability Assessment & Performance Analysis	1,391,299	1,182,409	-15.0%	(208,890)
Training, Education and Operator Certification	272,310	321,525	18.1%	49,215
Situational Awareness & Infrastructure Security	19,380	23,281	20.1%	3,901
Total Statutory Expenses & Net Fixed Assets	6,793,288	7,162,232	5.4%	368,944
Funding:				
Total Statutory Funding Assessment	5,488,056	6,237,837	13.7%	749,781
Pass ThruTraining & Education	90,000	90,000	0.0%	-
Pass Thru Software Maintenance	24,000	24,000	0.0%	-
Cash Reserve Refund (Requirement)	848,232	657,395	-22.5%	(190,837)
Penalty Assessment Allocation	343,000	153,000	-55.4%	(190,000)
Total Statutory Funding (Equals Total Expenses)	6,793,288	7,162,232	5.4%	368,944

2015 to 2014 RE Division Comparative Budgeted Funding



2015 RE Division Overview

- The FRCC will continue to evaluate the adequacy of its resources and to evaluate efficiencies in its processes in order to continue to carry out its delegated responsibilities.

- The FRCC will continue to align itself and support the ERO Strategic Plan for goals, activities and major activities which include:
  - Support of the RAI with training and implementation for compliance and enforcement staff.
  - Support NERC's plan to develop RSAW's concurrent with Reliability Standards.
  - Work with NERC and the other RE's to provide guidance to registered entities on CIP V5.
  - Work to refine and revise procedures and processes to eliminate duplication, increase operating efficiencies, enhance ERO-wide consistency and to achieve measurable reliability outcomes.

2015 RE Division Risks

- Roll out of RAI may require significantly more staff time than budgeted
- Compliance Software costs may be higher than budgeted due to RAI or unplanned NERC projects
- Additional costs may be incurred to implement recommendations from the FRCC Security Assessment Initiative
- As always, there could be a Compliance Hearing

2015 Proposed RE Division Working Capital Policy

- Working Capital and operating reserve requirements shall be one (1) month of the total annual budget
- A 1.5 million line of credit is available for short term and other risks that may be needed to bridge budget cycles and approved assessments.
- Working Capital shall be utilized to satisfy projected annual cash flow and cash balance requirements.
- Operating reserves shall be utilized to satisfy known contingencies where the specific timing and amount is uncertain.

FRCC Proposed 2015 Total Budget Compared to 2014

	2015 Budget	2014 Budget	$ Change	% Change
Regional Entity Division Expenses W/Fixed Assets	$ 7,162,233	$ 6,793,289	$368,944	5.4%
Member Services Division Expenses W/Fixed Assets	8,391,982	7,455,995	935,987	12.6%
Total Expenses	$15,554,214	$14,249,283	$1,304,931	9.2%
Other Funding – Workshops & Fees	388,459	391,419	2,960	(0.8%)
Cash Reserve (Requirement)/(Surplus)	534,812	1,110,046	575,234	(51.8%)
Penalty Sanctions	153,000	343,000	190,000	(55.4%)
Total FRCC Funding Assessment	$14,477,943	$12,404,818	$2,073,125	16.7%

2015 BP&B Summary

- **Regional Entity**
  - Budget increase of 5.4%
  - 0 new Staff
  - 0.5 increased FTEs

- **Member Services**
  - Budget increase of 12.6%
  - 1 new Staff
  - 1.5 increased FTEs

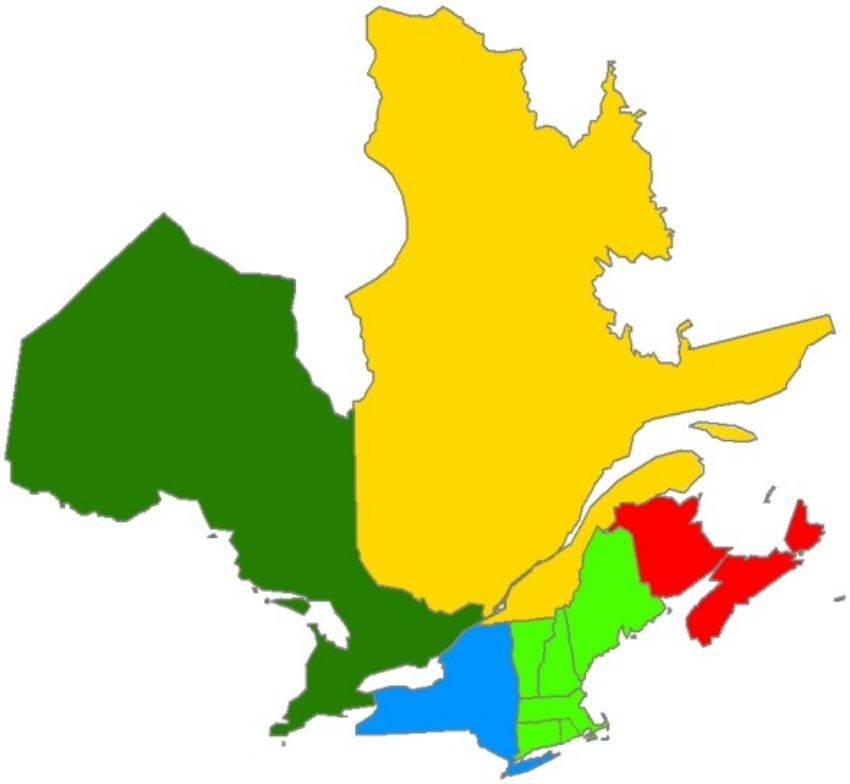
FRCC

QUESTIONS?

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

Northeast Power Coordinating Council, Inc. (NPCC)

Preliminary Draft 2015 Business Plan and Budget



Draft 1
Submitted to NERC
May 14, 2014

Table of Contents

Introduction 3
Personnel Analysis 12
Section A — 2015 Business Plan 15
Reliability Standards Program 15
Compliance Monitoring and Enforcement and Organization Registration and Certification Program 26
Reliability Assessment and Performance Analysis Program 36
Training, Education, and Operator Certification Program 51
Situation Awareness and Infrastructure Security Program 56
Administrative Services 63
Technical Committees and Member Forums 65
General and Administrative 67
Legal and Regulatory 68
Information Technology 69
Human Resources 71
Finance and Accounting 72
Regional Entity Assessment Analysis 74
Section B — Supplemental Financial Information 78
Reserve Balance 78
Breakdown by Statement of Activity Sections 79
Section C —2015 Criteria Services Division Business Plan and Budget 89
Personnel Analysis 96
Reserve Analysis 2014 - 2015 97
Section D 99
Statement of Financial Position 99

Introduction

Total NPCC Resources (in whole dollars)	2015 Budget	U.S.	Canada	Mexico
Regional Entity Division FTEs	36.86			
Criteria Services Division FTEs	2.14			
Total FTEs	**39.0**			
Regional Entity Division Expenses	$14,758,558			
Criteria Services Division Expenses	$1,139,452			
Total Expenses	**$15,898,011**			
Regional Entity Division Inc(Dec) in Fixed Assets	**$19,981**			
Criteria Services Division Inc(Dec) in Fixed Assets	**($10,011)**			
Total Inc(Dec) in Fixed Assets	**$9,970**			
Regional Entity Division Working Capital Requirement**	**($355,161)**			
Criteria Services Division Working Capital Requirement***	**($94,220)**			
Total Working Capital Requirement	**($449,381)**			
Total Regional Entity Division Funding Requirement	$14,423,378			
Total Criteria Services Division Funding Requirement	$1,035,221			
Total Funding Requirement	**$15,458,599**			
Regional Entity Division Assessments	**$14,078,378**	$XXX,XXX	$XXX,XXX	
Regional Entity Division Assessments Percentage	**100.0%**	XX.X%	XX.X%	
Criteria Services Division Membership Fees	**$760,033**	$XXX,XXX	$XXX,XXX	
Total NPCC Assessments & Membership Fees	**$15,113,599**	$XXX,XXX	$XXX,XXX	
NEL	XX	XX	XX	
NEL %	100%	XX.XX%	XX.XX%	

** Refer to Table B-1 on page 78 in Section B.
*** Refer to the Reserve Analysis on page 97 in Section C.

2015 Overview of Total NPCC Resource Requirements

Due to the international nature of NPCC, the total resource requirements including both Regional Entity division and Criteria Services division are identified above. The individual divisional explanations are contained in subsequent sections.

NPCC proposes to increase its total funding requirement from $14,818,588 to $15,458,599 in 2015, an increase of $640,011 or 4.3%. The proposed 2015 funding requirements will be satisfied by a Regional Entity division assessment of $14,078,378 and Criteria Services division fees of $1,035,221, an overall increase of 3.5% compared to the 2014 total assessments and fees of $14,601,588. NPCC believes that the Region remains an effective provider of Regional Entity and Criteria Services division functions. NPCC's corporate culture centers on consistent delivery of excellent results at a cost that is considerate of the longstanding tradition in the Northeast of affordable and reliable electricity.

Organizational Overview

Northeast Power Coordinating Council, Inc. (NPCC) is a 501(c)(6) not-for-profit corporation in the state of New York responsible for promoting and improving the reliability of the international, interconnected bulk power systems in Northeastern North America through (i) 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 (collectively, Regional Entity activities), and (ii) the establishment of Regionally-specific criteria, and monitoring and enforcement of compliance

with such criteria (collectively, criteria services activities). NPCC provides the functions and services for Northeastern North America of a cross-border Regional Entity through a Regional Entity division, as well as Regionally-specific criteria services for Northeastern North America through a criteria services division. NPCC's website is www.npcc.org.

The NPCC Region covers nearly 1.2 million square miles and is populated by more than 56 million people. NPCC U.S. includes the six New England states and the state of New York. NPCC Canada includes the provinces of Ontario, Québec and the Maritime provinces of New Brunswick and Nova Scotia. In total, from a net energy for load perspective, NPCC is approximately 45% U.S. and 55% Canadian. With regard to Canada, approximately 70% of Canadian net energy for load is within the NPCC Region.

Effective January 1, 2012, NPCC executed an Amended and Restated Regional Delegation Agreement with the North American Electric Reliability Corporation (NERC) that delegates to NPCC certain responsibilities and authorities of a cross-border Regional Entity as defined by *Section 215* of the Federal Power Act in the U.S. In addition, NPCC has executed Memoranda of Understanding or Agreements with Canadian provincial regulatory and/or governmental authorities in Ontario, Québec, New Brunswick and Nova Scotia.

In this 2015 business plan, NPCC has included activities consistent with NERC initiatives including the implementation of the revised BES definition, risk-based registration, the Reliability Assurance Initiative, and expanded training for compliance auditing.

It is imperative that NPCC maintain its ability to carry out delegated authorities and responsibilities. NPCC has a flat 2015 targeted staffing level of 39 power industry professionals and support personnel. Details of the 2015 business plans and budget for each program area are included in Section A for the Regional Entity division. The 2015 Regional Entity division schedules are shown in Section B. Section C details the 2015 criteria services division business plan and budget.

Membership and Governance

NPCC monitors approximately 300 registered entities and some 602 functions in the Region for compliance with mandatory Reliability Standards. NPCC currently has approximately 78 members. There are two categories of membership, General and Full. The two categories distinguish between Regional Entity delegated services that are provided in support of the U.S. FERC and Canadian provincial MOUs or Agreements with regulatory and/or governmental authorities, and Criteria Services which FERC references as U.S. non-delegated activities.

General Membership is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the Electric Reliability Organization (ERO) that has an interest in the reliable operation of the Northeastern North American bulk power system. General Members which are also registered entities within the NPCC Region are subject to compliance with Reliability Standards, consistent with their registration, and also receive additional services from the Regional Entity division of NPCC.

Full Membership is available to Members which are already General Members and participate in electricity markets in the Northeast. Independent system operators (ISOs), Regional transmission organizations (RTOs), Transcos and other organizations or entities that perform the Balancing Authority function operating in Northeastern North America are expected to be Full Members of NPCC. The New York State Reliability Council and any other sub-regional

reliability councils which may be formed are also expected to be Full Members. Full Members are subject to compliance with Regionally-specific more stringent reliability criteria for their generation and transmission facilities on which faults or disturbances can have a significant adverse impact outside of the local area and which are identified utilizing a reliability impact-based methodology, in addition to Reliability Standards, and receive additional services from the Criteria Services division of NPCC, which is not funded through the ERO.

Since January 1, 2012 NPCC is governed by a Board of Directors consisting of seven stakeholder voting sectors consisting of a maximum of two directors per sector, an independent sector consisting of two independent directors, an independent Board Chair with voting rights to preclude board deadlocks, and the President and CEO. Within NPCC, no two sectors can control and no one sector can block action. The voting sectors on the NPCC Board of Directors include:

Sector 1) Transmission Owners
Sector 2) Reliability Coordinators
Sector 3) Transmission Dependent Utilities, Distribution Companies, Load Serving Entities
Sector 4) Generator Owners
Sector 5) Marketers, Brokers and Aggregators
Sector 6) Regulators
Sector 7) Sub-Regional Reliability Councils, Customers, other Regional Entities and Interested Entities
Sector 8) Independent

A Finance and Audit Committee (FAC), a Pension Committee (PC), a Corporate Governance and Nominating Committee (CGNC), and a Management Development and Compensation Committee (MDCC) advise the Board on finance, governance, compensation and human resource matters. The Board endorses a non-employee, Certified Public Accountant for election by the NPCC Members as Treasurer of the corporation. The Treasurer chairs the FAC and works with the Chief Operating Officer who provides oversight of the finances of the corporation. The Treasurer reports to the Board on the corporation's financial position, on FAC activities, on tax code requirements, and on independent annual audit results and accounting practices.

The Regional Standards Committee (RSC), the Compliance Committee (CC), the Reliability Coordinating Committee (RCC), and the Public Information Committee, consistent with their approved scopes, are responsible for various reliability issues. The RSC, CC and RCC also provide technical policy recommendations to the Board. All General and Full Members are eligible for representation on the technical committees.

Industry technical experts from within the membership provide valuable input to the Board through various working groups and task forces as well as the committees. The *Amended and Restated Bylaws* establishes NPCC's independence from users, owners and operators of the bulk power system through the enhanced governance structure while providing fair stakeholder representation in the election of the Board of Directors and officers. The members, from each of the seven stakeholder voting sectors, vote to elect directors in their respective sector. The *Amended and Restated Bylaws* establish criteria for board service for both stakeholder and independent directors. Independent Directors are drawn from diverse backgrounds and possess a broad range of industry expertise, perspectives, experiences, skill sets and knowledge to contribute to the effective functioning of a hybrid board structure.

Compliance and enforcement activities are carried out by the NPCC compliance staff and are independent of all users, owners and operators of the international bulk electric system. Compliance activities are governed in the United States by the *Amended and Restated Regional Delegation Agreement* between NERC and NPCC, delegating portions of NERC's authority as the ERO to NPCC. NPCC compliance activities in Canada are governed by an individual provincial Memorandum of Understanding (MOU) or Agreements with each province providing the unique parameters for compliance and enforcement activities for each of the provinces. A MOU between the Independent Electricity System Operator in Ontario (IESO), NERC and NPCC establishes roles and responsibilities with regard to that province. NPCC, NERC and the New Brunswick Energy and Utilities Board are parties to a MOU that sets forth reliability activities for New Brunswick. The Régie de l'énergie, NERC and NPCC executed an Agreement regarding the development of electric power transmission Reliability Standards and a program for the monitoring of the application of these standards for Québec. NPCC, NERC and Nova Scotia executed a MOU that sets forth the mutual understanding of the parties in relation to the approval and implementation of NERC Reliability Standards and NPCC Regional reliability criteria for the province of Nova Scotia.

International Foundation

The Regional Entity functions and services differ according to particular regulatory backstop:

a) U.S. Foundation

The Federal Energy Regulatory Commission (FERC) certified NERC as the Electric Reliability Organization (ERO) on July 20, 2006. The ERO is responsible for developing and enforcing reliability standards within the United States. In executing part of its responsibilities, NERC delegates authority to the Regional Entities to perform certain functions through delegation agreements. Ensuring the reliability of the bulk power system in the state of New York and the six New England States was delegated from NERC to NPCC through the Amended and Restated Regional Delegation Agreement.

b) Ontario

On February 5, 2010, NERC, NPCC and the IESO amended and restated their earlier MOU, dated November 29, 2006, setting forth their mutual understanding as regards NERC's and NPCC's status in Ontario with respect to standard and criteria development, compliance enforcement, and other related matters. The IESO, whose statutory responsibilities include making and enforcing reliability standards, and making and enforcing Ontario market rules that govern the IESO-controlled grid and the wholesale electricity market, was established April 1, 1999 as the Independent Electricity Market Operator in Ontario under the *Electricity Act, 1998* (Ontario). The IESO is subject to the regulatory oversight of the Ontario Energy Board (OEB).

Among other things, the MOU recognizes that NERC and NPCC are standards authorities under the *Electricity Act, 1998* (Ontario). Additionally, under the authority of that same legislation, and as memorialized in the MOU, the NERC reliability standards and NPCC reliability criteria have effect in Ontario. However a 2008 amendment to the Electricity Act, 1998 (Ontario) allows the OEB to review these standards and criteria and issue orders preventing their implementation and remanding them back to NERC and NPCC.

The IESO is subject to compliance monitoring and enforcement by NPCC. The IESO is also subject to compliance monitoring and enforcement of the Ontario market rules by the IESO's Market Assessment and Compliance Division (MACD) that operates at arm's length from the IESO's business units. The MOU notes that where MACD, NERC, and NPCC engage in

investigations pursuant to their respective mandates regarding compliance, MACD can request to take the lead. Moreover, of the three, MACD is the only entity that can assess financial penalties for any Ontario market participant's or the IESO's non-compliance with Ontario market rules, which includes non-compliance with NERC standards and NPCC criteria.

The MOU provides for a peer review process to promote the common compliance and enforcement objectives of NERC/NPCC and MACD. From the perspective of NPCC and NERC, this process, in part, is meant to assure registered entities outside of Ontario that the MACD program is rigorous, thorough and reliable.

The IESO is subject to NPCC assessments of compliance, including audits, as well as NPCC remedial action directives to correct non-compliance. In the event that the IESO disagrees with NPCC's finding of a violation or associated assessment of sanctions in connection with standards and criteria, the IESO has a right to a compliance hearing with NPCC.

c) Québec

The Régie de l'énergie, NERC and NPCC are parties to the May 8, 2009 *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* (the Agreement). Under the terms of the Agreement, the Régie de l'énergie , which is charged with ensuring the reliability of the electric transmission in Québec, retained NPCC and NERC as experts to develop reliability standards and monitoring program procedures for the Province.

The Régie de l'énergie is a public body established by the *Act respecting the Régie de l'énergie* (the Act). Pursuant to its authority under the Act, the Régie de l'énergie, through a series of decisions in 2007, designated Hydro-Québec TransÉnergie (HQTE) as the Reliability Coordinator for Québec. In accordance with its mandate and as recognized in the Agreement, it is this entity that is responsible for the filing with the Régie de l'énergie for approval of reliability standards in Québec. HQTE has filed for the approval of certain reliability standards and the Régie de l'énergie has begun the proceedings required to make such reliability standards mandatory in Québec.

The Agreement contemplates the execution of a second agreement that will detail the mandates granted by the Régie de l'énergie to NPCC and NERC with respect to the implementation of the 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. The second agreement is currently being negotiated by the Régie de l'énergie, NPCC and NERC. The intent, once all the appropriate authorizations are in place, is that NPCC and NERC will act as the Régie's agents in all compliance monitoring and enforcement activities through the implementation of a Québec specific compliance monitoring and enforcement program.

Currently, as there are only a limited number of mandatory standards that have come into effect, and as the second agreement and all the appropriate authorizations covering compliance monitoring and enforcement arrangements are not in place, there has been limited mandatory compliance activity under the formal Québec regime. However, the Hydro-Québec companies, including Hydro-Québec TransÉnergie and Hydro-Québec Production have been subject to voluntarily compliance monitoring, including comprehensive audits by NPCC. Additionally, NPCC has and continues to proceed with its reliability assurance activities within Québec,

including but not limited to events analysis, Reliability Assessment and Performance Analysis and compliance investigations, consistent with the NPCC *Amended and Restated Bylaws*.

d) New Brunswick

The New Brunswick Energy and Utilities Board ("EUB") and NPCC entered into an Agreement dated October 1, 2013, whereby NPCC provides services for the EUB. The EUB is a not-for-profit corporation which was established on October 1, 2004 under the Electricity Act (NB) and charged with developing and administering the wholesale electricity market and maintaining reliability of the integrated power system in New Brunswick.

Effective October 1, 2013, the Electricity Act (NB) and implementing regulations (together, "NB Electricity Act") amended how Reliability Standards are approved, monitored, and enforced in the province of New Brunswick. The NB Electricity Act designates NPCC as a compliance body and NERC as a standards body within the meaning of the NB Electricity Act. The October 1, 2013 Agreement between NPCC and the EUB is intended to be the preliminary step with respect to the implementation of the NB Electricity Act.

With respect to the approval of reliability standards, the NB Electricity Act provides that all of the NERC Reliability Standards that were effective in New Brunswick prior to October 1, 2013 continue to be effective in New Brunswick after October 1, 2013. Additionally, the New Brunswick Power Corporation (formed from several amalgamating corporations) ("NBPC") is required to file for approval, modification, or retirement of NERC Reliability Standards 60 days after a NERC Reliability Standard is approved, modified, or retired by the Federal Energy Regulatory Commission ("FERC"). The EUB rules on the filed Reliability Standard after considering (a) the potential impact on the reliability of the bulk power system, (b) the potential cost and benefits (c) the public interest, and (d) any other factors that the NBUEB considers relevant. The Electricity Act requires the NBEUB to notify NPCC and NERC of an application by the NBPC with respect to reliability standards and provide for a 60 day comment period. The NBEUB is required to approve the reliability standards if there are not substantive modifications proposed from the FERC approved NERC Reliability Standard and there were no substantive comments filed. Amendments to the reliability standard to make them compatible with New Brunswick or Canadian law are considered non-substantive. The approval of reliability standards may be subject to a hearing for several reasons, including substantive comments from NPCC or NERC.

With respect to the monitoring and enforcement of the Reliability Standards in New Brunswick, the NB Electricity Act requires NPCC to identify entities that must register with the EUB in the New Brunswick specific registry. Additionally, NPCC is required to carry out the compliance monitoring and assessment for the EUB and assist and advise the enforcement for the EUB, including financial penalties. NPCC is also permitted to carry out or exercise any power in the implementing regulations that is specific to the EUB. Additionally, NPCC has the powers of an inspector, which permits NPCC to audit and spot check entities within New Brunswick.

e) Nova Scotia

Nova Scotia Power Incorporated (NSPI), NPCC and NERC are parties to a May 11, 2010 Memorandum of Understanding regarding the approval and implementation of mandatory NERC reliability standards and NPCC Regional reliability criteria. Pursuant to the MOU's terms, NERC and NPCC filed standards and criteria with the Nova Scotia Utility and Review Board (NSUARB) for approval on June 30, 2010 and June 29, 2010, respectively. A decision from the NSUARB on both NERC and NPCC filings was rendered on July 20, 2011. Hence, the

standards and criteria are mandatory in Nova Scotia and NSPI will be subject to the NERC compliance monitoring and enforcement program, as implemented by NPCC.

NPCC will conduct compliance activities with respect to the standards and then forward any non-compliance information and recommendations to the NSUARB for use in enforcement proceedings. Enforcement will be administered by the NSUARB which will, among other things, determine whether a violation has occurred and, if so, what remedial measures or non-monetary penalties should be imposed.

Regional Entity Division Functional Scope

NPCC's Regional Entity division functions in support of the ERO include:

- Active participation in the development of North American Reliability Standards for the bulk electric system, and as needed development of Reliability Standards applicable within the NPCC cross-border Regional Entity
- Monitoring and enforcement of approved Reliability Standards, including the registration of responsible entities, and as needed certification of such entities
- Assessment of the present and future reliability of the bulk power system
- Operational coordination and situation awareness support
- Event analysis and identifying lessons learned to improve reliability
- Effective training and education of reliability personnel
- Promoting the protection of critical electric infrastructure

In recognition of the delegated compliance role of Regional Entities as an important means to enhancing reliability, NPCC has designated a significant percentage of its staff resources to compliance monitoring and enforcement. NPCC has also developed and deployed a robust set of online tools for gathering data, analysis, and tracking of compliance information to support its ability to carry out its responsibilities in a cost effective manner.

NPCC has organized the remaining staff into program areas consistent with EPAct 2005 to address the other functions listed above. These experts in operations, planning and reliability analysis assist registered entities in assessing and improving reliability. It is in support of these areas that NPCC engages the majority of industry experts on its technical committees.

2015 Key Assumptions and 2015 Goals and Key Deliverables

NERC and the eight Regional Entities collaborated in the development of a common operating model with complementary roles and responsibilities, an ERO Enterprise Strategic Plan, and a set of business planning assumptions, goals, metrics and key deliverables for the 2014 through 2017 period. The results from that collaboration are included as a set of Shared Business Plan and Budget Assumptions that will be contained in Exhibit A to the NERC 2015 Business Plan and Budget and may be referenced by the users of this document. In each of the following program area sections footnotes are used to reference the specific ERO Enterprise Goals that NPCC's activities support.

2015 Overview of Regional Entity Division Cost Impacts

NPCC proposes to increase its Regional Entity division funding requirement from $13,828,880 to $14,423,378 in 2015, an increase of $594,498 or 4.3%. The proposed Regional Entity division assessment of $14,078,378 to support the budget is an increase of 3.4% compared to the 2014 assessment of $13,611,880.

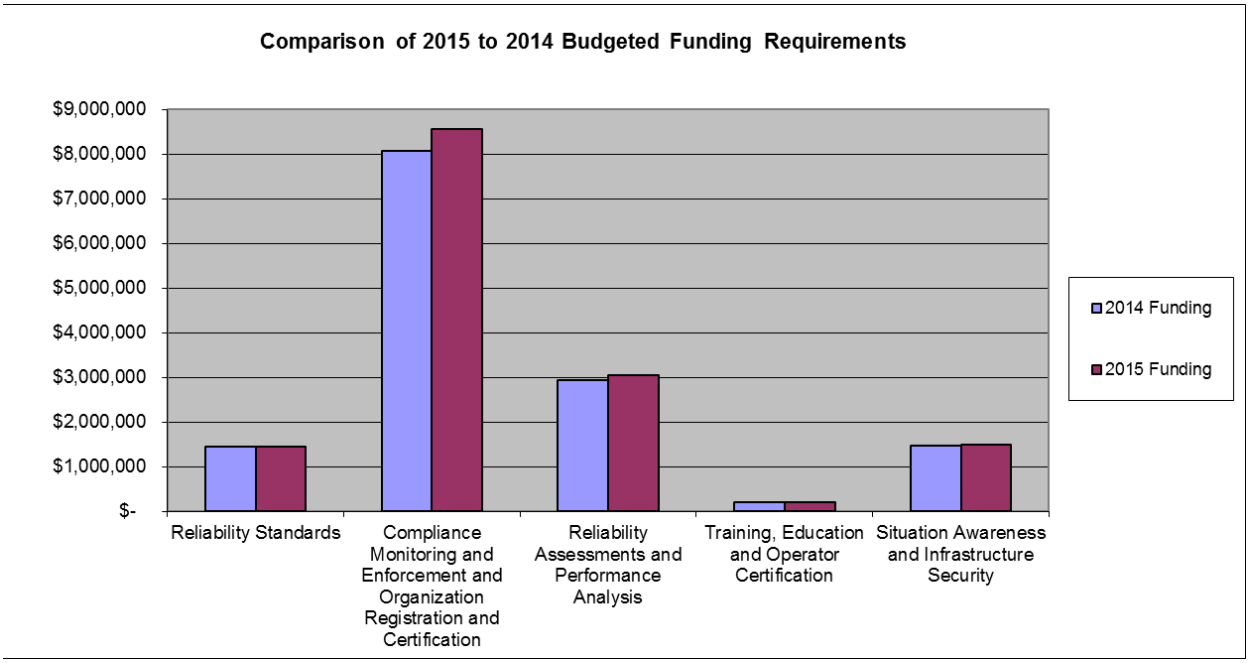
2014 Projections

Current year projections are taken into consideration in development of the budget. Expenses are currently projected to be on budget or slightly under budget in all areas. 2014 Projections reflect expectations based on the first quarter statement of activities. It is anticipated that projections could change throughout 2014 and would be reflected in each subsequent quarter's statement of activities.

Summary by Program

Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards	$ 1,447,330	$ 1,447,330	$ 1,456,129	$ 8,799	0.6%
Compliance Monitoring and Enforcement and Organization Registration and Certification	$ 8,079,371	$ 8,079,371	$ 8,568,145	$ 488,774	6.0%
Reliability Assessments and Performance Analysis	$ 2,942,339	$ 2,942,339	$ 3,053,923	$ 111,585	3.8%
Training, Education and Operator Certification	$ 195,855	$ 195,855	$ 199,010	$ 3,154	1.6%
Situation Awareness and Infrastructure Security	$ 1,464,111	$ 1,464,111	$ 1,501,332	$ 37,221	2.5%
Total	$ 14,129,006	$ 14,129,006	$ 14,778,539	$ 649,533	4.6%

This chart does not include allocation of working capital requirements among the Program Areas.



This chart does not include allocation of working capital requirements among the Program Areas.

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
REGIONAL ENTITY DIVISION						
Operational Programs						
Reliability Standards	2.93	2.93	2.00	0.93	2.93	0.00
Compliance Monitoring and Enforcement and Organization Registration and Certification	16.00	16.00	16.00	0.00	16.00	0.00
Training, Education, and Operator Certification	0.10	0.10	0.10	0.00	0.10	0.00
Reliability Assessment and Performance Analysis	5.83	5.83	4.90	0.93	5.83	0.00
Situation Awareness and Infrastructure Security	3.00	3.00	3.00	0.00	3.00	0.00
Total FTEs Operational Programs	**27.86**	**27.86**	**26.00**	**1.86**	**27.86**	**0.00**
Administrative Programs						
Technical Committees and Member Forums	0.50	0.50	0.50	0.00	0.50	0.00
General and Administrative	2.50	2.50	2.50	0.00	2.50	0.00
Information Technology	3.00	3.00	3.00	0.00	3.00	0.00
Legal and Regulatory	1.00	1.00	1.00	0.00	1.00	0.00
Human Resources	1.00	1.00	1.00	0.00	1.00	0.00
Accounting and Finance	1.00	1.00	1.00	0.00	1.00	0.00
Total FTEs Administrative Programs	**9.00**	**9.00**	**9.00**	**0.00**	**9.00**	**0.00**
Total FTEs	**36.86**	**36.86**	**35.00**	**1.86**	**36.86**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

2014 Budget and Projection and 2015 Budget Comparisons

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget

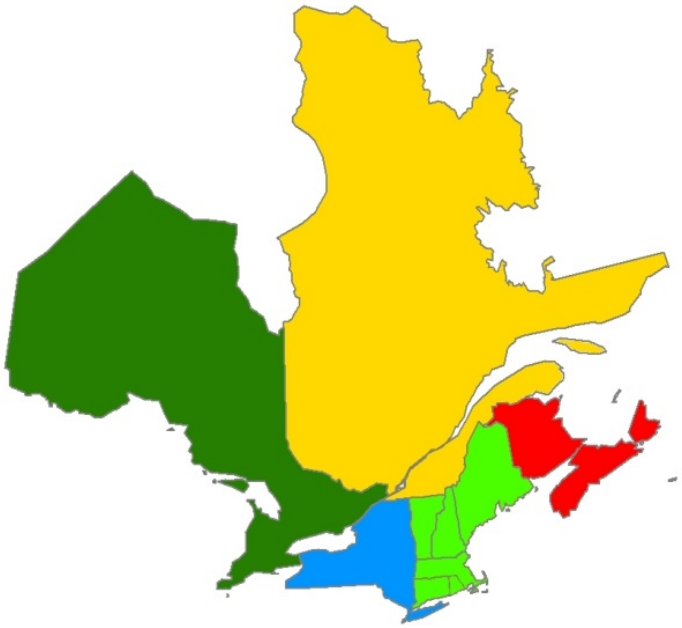
REGIONAL ENTITY DIVISION

		2014 Budget	2014 Projection	Variance[2] 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 13,611,880	$ 13,611,880	$ -	$ 14,078,378	$ 466,498
	Penalty Sanctions[1]	153,000	153,000	-	281,000	128,000
Total ERO Funding		**$ 13,764,880**	**$ 13,764,880**	**$ -**	**$ 14,359,378**	**$ 594,498**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	64,000	64,000	-	64,000	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 13,828,880**	**$ 13,828,880**	**$ -**	**$ 14,423,378**	**$ 594,498**
Expenses						
Personnel Expenses						
	Salaries	$ 5,911,227	$ 5,911,227	$ -	$ 6,195,425	$ 284,198
	Payroll Taxes	384,311	384,311	-	387,209	2,898
	Benefits	1,430,261	1,430,261	-	1,256,595	(173,666)
	Retirement Costs	1,124,361	1,124,361	-	1,090,013	(34,348)
Total Personnel Expenses		**$ 8,850,160**	**$ 8,850,160**	**$ -**	**$ 8,929,241**	**$ 79,081**
Meeting Expenses						
	Meetings	$ 365,000	$ 365,000	$ -	$ 365,000	$ -
	Travel	890,000	890,000	-	890,000	-
	Conference Calls	77,000	77,000	-	45,000	(32,000)
Total Meeting Expenses		**$ 1,332,000**	**$ 1,332,000**	**$ -**	**$ 1,300,000**	**$ (32,000)**
Operating Expenses						
	Consultants & Contracts	$ 1,924,433	$ 1,924,433	$ -	$ 2,342,000	$ 417,567
	Office Rent	737,272	737,272	-	751,500	14,228
	Office Costs	536,500	536,500	-	578,700	42,200
	Professional Services	966,500	966,500	-	1,025,000	58,500
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	80,000	80,000	-	40,000	(40,000)
	Depreciation	250,000	250,000	-	202,019	(47,981)
Total Operating Expenses		**$ 4,494,705**	**$ 4,494,705**	**$ -**	**$ 4,939,219**	**$ 444,514**
	Total Direct Expenses	**$ 14,676,865**	**$ 14,676,865**	**$ -**	**$ 15,168,460**	**$ 491,595**
Indirect Expenses		**$ (405,859)**	**$ (405,859)**	**$ -**	**$ (409,902)**	**$ (4,043)**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 14,271,006**	**$ 14,271,006**	**$ -**	**$ 14,758,558**	**$ 487,552**
Change in Assets		**$ (442,126)**	**$ (442,126)**	**$ -**	**$ (335,180)**	**$ 106,946**
Fixed Assets						
	Depreciation	$ (250,000)	$ (250,000)	$ -	$ (202,019)	$ 47,981
	Computer & Software CapEx	108,000	108,000	-	222,000	114,000
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(0)	(0)	-	(0)	-
Inc(Dec) in Fixed Assets (C)		**(142,000)**	**(142,000)**	**-**	**19,981**	**161,981**
TOTAL BUDGET (=B+C)		**$ 14,129,006**	**$ 14,129,006**	**$ -**	**$ 14,778,539**	**$ 649,533**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**

[1] $281,000 of penalty sanctions collected to date and prior to June 30, 2014.

[2] 2014 Projections reflect expectations based on the 1st quarter statement of activities. It is anticipated that projections could change throughout 2014 and would be reflected in each subsequent quarter's statement of activities.

Section A – Regional Entity Division
2015 Business Plan and Budget



Section A — 2015 Business Plan

Reliability Standards Program

Reliability Standards Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.93	2.93	0.00
Direct Expenses	$917,936	$905,638	($12,299)
Indirect Expenses	$555,686	$561,221	$5,535
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($26,292)	($10,729)	$15,563
Total Funding Requirement	$1,447,330	$1,456,129	$8,799

Program Scope and Functional Description

The NPCC Reliability Standards program operates in accordance with NPCC's filed and approved Delegation Agreement "Exhibit C", and NERC Rules of Procedure Section 300. The program supports the ERO standards program area roles and responsibilities by providing supporting activities for the development of clear, concise, sustainable, high quality and technically sound mandatory "results based" reliability standards which provide for an adequate level of reliability in a timely and efficient manner. The primary objective of NPCC's program area is to support the development of ERO standards which establish threshold requirements for ensuring the bulk electric system is planned, operated, and maintained in a manner that minimizes risks of cascading failures, avoids damage to major equipment, is responsive to risks, or limits interruptions of bulk power supply. At a Regional level, the program develops Regional Reliability Standards and ensures that Regional reliability criteria, contained in the form of Directories, are not inconsistent with any applicable NERC and Regional Reliability Standards. The NPCC Reliability Standards program also supports and participates in the development, revision, and maintenance of NERC Reliability Standards, initiates new regional or continent wide reliability standards when necessary, and provides a forum for the comprehensive review and improvement of existing and developing standards.

The NPCC Reliability Standards Program Area supports the reliability of the bulk electric system by:

- Facilitating active participation of NPCC Regional industry stakeholders in all NERC Reliability Standards activities to promote the development of results based, cost effective quality standards in a timely and efficient manner.
- Promote awareness by holding workshops and conducting Regional Standards Committee meetings to inform and educate stakeholders.
- Internally and informally training staff for the new and developing standards through meetings.
- Regional coordination activities with Standards Program Areas from other Regions.

- Development and maintenance of Regional Standards as necessary to address Regional reliability related issues or risks and ensure those standards are not inconsistent with the NERC continent wide standards. These Regional standards contain requirements that are more stringent, add specificity to or augment the NERC Continent-wide standards.
- NPCC maintains and abides by the NPCC Regional Standards Processes Manual assuring compliance with all FERC filed documents with respect to standards development.

Funding Drivers and Reliability Benefits

- Expanded Scope of Standards activities
    - Utilize NPCC RSC, Task Forces and Working Groups to comment on developing NERC Standards to ensure they are results based and directionally consistent with the Independent Experts Review Panel Report (IERP)[1]
    - Develop process for ensuring lessons learned from Event Analysis are evaluated for any gaps in standards or criteria[2]
    - Responding to increasing amount of FERC Rulings, NOPRs, preliminary staff assessments, and FERC issued Directives[3]
    - Providing support for increased standard development activities as outlined in the NERC 2014-2016 Reliability Standards Development Plan and assuming an active role in the newly formed NERC Project Management Oversight Subcommittee ("PMOS")
    - Participating in informal activities of standards development to promote consensus early in project development and provide technical guidance
    - Providing a forum for all NPCC representatives on the NERC drafting teams
    - Actively coordinating and reviewing Reliability Standards Audit Worksheets (RSAW) for correctness
    - Provide NPCC Regional point of contact for the new Reliability Issues Steering Committee ("RISC") to provide emerging and existing BES reliability related risks and potential gaps in the existing NERC standards
- Increased Number of Standards Projects
    - Active NERC Projects in the standards area are also expected to increase to address FERC outstanding directives.
    - The concept of informal development was introduced in 2013 and will be expanded to include more standards development projects in 2015 requiring more technical support, participation, and facilitation.
    - NERC has developed procedures and processes to allow it to revise standards in a more expeditious manner that may need clarification or address some deficiency.
    - NPCC is assisting with the Project Management Oversight Subcommittee (PMOS) which is responsible for managing the development of NERC standards projects and tracking Paragraph 81 Phase 2 retirement candidates

[1] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[2] In support of ERO Goal 1aDevelop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[3] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

  - Promote and assist with the Cost Effective Analysis Process ("CEAP") to ensure standards have the most cost effective requirements which meet the reliability objectives of standards under development[4]

- Further resources required to evaluate the standards from a "cost benefit" and also a "cost effectiveness" perspective will be required.
- NERC Reliability Standards will continue to require Violation Risk Factors (VRFs) to be developed and NERC is reviewing additional levels of VRF and development of a Sanction Matrix which is envisioned to replace the Violation Severity Levels (VSLs).
- Expanded efforts to educate and inform stakeholders in the areas of NERC and NPCC Regional Standards through NPCC Workshops and with anticipated additional forums such as increases in the amount of Internet based meetings and technical conferences. [5]

2015 Key Assumptions

- Facilitate stakeholder review, comment on, and develop ballot recommendations or list of Regional issues, for all NERC Reliability Standards Projects under informal or formal development or revision prior to the end of ballots
  - NERC and NPCC benefit from NPCC's Regional coordination consisting of a broad stakeholder review process and development of consensus recommendations to assure proposed standards will support international reliability and provide appropriate reliability objectives for the Continent-wide standards
  - Coordinate a comprehensive review of the results based standards initiative processes and standards being implemented
  - Conduct and obtain training for performing Quality Reviews of standards at both the Regional level and to assist the ERO with analysis of the continent wide standards
  - Coordinate the review of all Reliability Standards Audit Worksheets during their postings for comment for potential expansion of their associated standard's requirements
  - Refine the NPCC triage process to assess posted standards and related material to ensure it is properly routed to and addressed by the appropriate NPCC technical or process resources.
- Participate in the stakeholder efforts to develop Standards Authorization Requests (SARs) and Regional SARs to further improve standards in response to any potential inadequacies in reliability or to improve standards
- Monitor and participate in the drafting of key NERC Reliability Standards-CIP, Protections Systems, Balancing Control Performance, and Frequency Response, etc.
  - The NPCC monitoring of the development of standards helps to ensure reliability requirements that are clear, measureable, and enforceable and support international reliability in the Northeast
- Continue with the development and maintenance of a set of NPCC Phase II Directories not inconsistent with the NERC Reliability Standards which clearly delineate the more stringent NPCC criteria requirements

[4] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[5] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

  - The combination of North American and Regional Reliability Standards with the more-stringent NPCC Regional criteria provides for consistency and operational clarity while providing robust defense in–depth, results based, standards to ensure BES reliability
  - Ensure no redundancies exist between the criteria found in the NPCC Directories and the ERO standards
  - Retire Directories that have been overtaken by improved NERC standards
  - Continually file the more stringent requirements with the New York State Department of Public Service and Canadian Provinces as applicable
- Review reliability requirements of ERO and NPCC Regional Standards, NPCC Criteria and ensure consistency, remove redundancies, adopt Functional Model language and ensure requirements are "results based"
  - The unambiguous assignment of reliability requirements to specific functional entities benefits international reliability
  - Participate in the continuing refinement of the Functional Model to capture evolving issues essential to reliability and new objectives in the industry, i.e. demand resource operator, planning functions, new activities yet to be identified such as those associated with Smart Grid, "Synchro-Phasor" technology, etc.
  - Participate in the continual improvement of the NERC standards development processes and initiatives such as the CEAP, PMOS and Single Portal Project.
  - Contribute to the improvement of process related to NERC providing interpretations.
- Review all FERC orders and Provincial regulations as they relate to the standards, their revision and adoption
  - Northeast reliability benefits from careful analyses of governmental orders or actions adopting standards to assure consistency in interpretation
  - Review rulings that are issued and all FERC Directives for potential reliability related issues
  - Conduct and support Regulatory/Governmental Provincial filings on a periodic basis based on individual Provincial Laws and requirements outlined in the Memorandum of Understandings for each Province.
- Enhance NPCC standards website pages to provide uniform and clear information to the stakeholders while also providing the historical and archived information to support NERC and FERC approvals and expanding requirements

2015 Goals and Key Deliverables

The Reliability Standards program goals and objectives for 2015 are grouped into seven categories:

1) Participate in the ERO Results-Based Standards Development

- Participate in the development and revision of the NERC three year work plan through review, commenting and drafting activities
- Participate in the Standards Committee Strategic initiatives to develop results based standards that will provide a defense in depth, complete the standards due for 5 year review, and address all existing and outstanding FERC Directives.
- Support the implementation of the NERC Board of Trustees ("BOT") resolutions specifically supporting the timeliness, cost effectiveness, timely development, and quality of new standards

- Coordinate the development of ERO Reliability Standards within NERC's three-year standards work plan with the emphasis placed on reducing the amount of new FERC Directives issues by closer coordination with the Commission staff
- Conduct thorough reviews of all NERC standards being developed or revised and coordinate comments for Northeastern North America driving consensus to the extent possible
- Facilitate and enhance the NERC Cost Effective Analysis Procedure both within NPCC throughout the industry
- Conduct thorough reviews of all Industry requested NERC Formal Interpretations of standards and develop and promote the NERC Informal Guidance Process, a comprehensive process to deal with all standards related questions, e.g. Single Portal
- NPCC staff along with NPCC solicited Regional drafting team volunteers, will participate in the drafting of all ERO standards affecting or potentially affecting reliability in the Eastern Interconnection and provide support for review and development of comments and propose improvements with specific emphasis on CIP
- NPCC and its members will review and coordinate potential comment on FERC preliminary staff assessments as appropriate
- Participate in ballots for ERO standards and provide consensus recommendations to the NPCC Members of the NERC Registered Ballot Body or provide a list of issues to allow the Members to cast a ballot based on Regional concerns prior to the end of the ballots
- Review and develop issues on FERC Notice of Proposed Rulemakings for any and all standards related issues as appropriate
- Coordinate and evaluate proposed standards utilizing NPCC's Regional technical task forces, working groups and committees
- Educate and notify stakeholders and regulators about issues related to standards development through various means such as webinars and workshops
- Provide outreach to industry trade groups to educate and drive consensus such as the North American Generator Forum and North American Transmission Forum
- Provide a forum for NPCC review of proposed and posted documents from the NERC Critical Infrastructure Protection Committee (CIPC) and NPCC Task Force on Infrastructure Security and Technology (TFIST)
- Provide support to NERC's strategy in the prioritization, identification, scheduling and development of NERC directed Regional Reliability Standards
- Participate in NERC's Standards Committee standards prioritization process, to identify immediate standards needs and prioritization based on need
- Participate in the NERC RISC by providing a Regional point of contact for all potential reliability related risks and gaps within the Northeast or as noted by NPCC stakeholders
- Participate in and provide support to critical standards, such as UVLS, Voltage and Reactive Control, Real Time Tools, Frequency Response, etc.
- Identify and initiate Regional Variances to the NERC Reliability Standards as soon as possible, allowing incorporation into the continent wide standard at its inception
- Identify potential drivers for standards revisions based on revisions to the BES to a bright line criteria and any document revisions required as a result of consideration of the "Exception Process".
- Support additional standards workload from further economic stimulus, i.e. standards on integrating variable generation resources or EHV backbone, Smart Grid, Electric Vehicles or "Synchro-Phasor" projects as necessary

- Provide continued input and leadership to NERC, based on NPCC experiences, regarding strategy for developing cost effectiveness analysis for standards and support activities to enhance this to identify "benefits" for the draft standards.
- Provide support and assistance to the ERO for conducting Quality Review activities on NERC continent-wide standards as possible
- Continually file the NPCC Directories with the Canadian Provincial Regulatory Authorities within the NPCC "footprint", on an as needed basis, as the directories are developed and revised and as the Provinces establish procedures and agreements with NPCC.
- Continue to develop new and innovative processes to better utilize the limited internal and external resources in the Region to enable sufficient technical review of posted standards and related materials
- Support the ERO and the relationships with FERC and the provincial governmental authorities for standards development activities as necessary to accomplish the ERO goals and objectives
- Support the development of system protection and control, communication, transmission operation standards and other critical standards efforts.

2) Regional Standards Development

- NPCC does not anticipate developing further Regional Standards but reserves the right to do so if a reliability issue exists that is not appropriate for Continent-wide development and also will perform clarifications as needed to existing approved Regional Standards.
- Draft any additional standard NERC directs NPCC to develop to meet an urgent reliability related needs, i.e. Geomagnetic disturbance system hardening
- Accomplish all directives of ERO and governmental and/or regulatory authorities with regard to Regional Standards development and procedures
- Adhere to and surpass, where practical, the 2014-2016 NERC Work plan milestones as they pertain to targets for the Regional Standards
- Respond to any FERC Directives that may arise as a result of the filing of NPCC's Regional Standards with the FERC or any Provincial "directives" that may be issued by the Canadian Regulatory Authorities

3) Standards Improvement

- Achieve NPCC reliability goals and objectives by initiating, participating in, and efficiently completing standards related activities
- Leverage internet and web based tools functionality to ensure inter-Regional consistency and quality of Regional Reliability Standards
- Establish long-term strategy for standards improvement and initiate implementation
- Continually identify additional future Regional Standard opportunities if Continent-wide standards are not an appropriate solution
- Ensure the topics addressed by the Reliability Standards parallel changing industry needs
- Participate in reliability metrics activities to identify potential measures for benchmarking of reliability to determine if an adequate level of reliability is being achieved
- Support and develop cost-benefit analysis activities to determine if any potential incremental increases in costs of implementing a standard have sufficient enough reliability benefit to implement that standard

4) Coordination of review of RSAWs

- Develop a process to review the RSAWs consisting of subject matter experts to determine if the RSAWs are technically representative of the standard's requirements and also to review the evidence suggested in the RSAW for satisfactory compliance assessment
- The Regional Standards Committee ("RSC") will oversee and provide the results of the coordination to the appropriate NERC SDT charged with development of the RSAW

5) Business Practices Interface

- Coordinate the review of standards through NPCC RSC, staff, and other members participating in activities of the North American Electric Standards Review Board (NAESB)
- Identify potential market related issues for Regional Standards through NPCC RSC coordination and reviews

6) Opportunities for Process Improvement

- Identify efficiencies for a coordinated NERC standards development process and NPCC Regional Standards Development Procedure and recommend revisions as applicable to either process
- Refine the NERC and NPCC CEAP s to evaluate the costs and effectiveness of proposed new and revised reliability standards to achieve an adequate level of reliability and a steady state set of standards
- Participate in any potential revision and redrafting of the NERC Standards Development Process to consider expedited standards development and cost effectiveness analysis and maintaining the ANSI Accreditation for standards development
- Participate in the enhancement of the Single Portal on the NERC website to provide one stop shopping for stakeholders seeking answers to questions.
- Identify potential future processes to obtain expedited interpretations
- Identify expedited processes for adjusting NERC glossary terms
- Identify refinements for credentialing standard drafting team members to ensure the correct subject matter experts are developing the standards at both the Regional level and the ERO level.
- Establish targets for NERC and NPCC standards procedure improvement and support initiation of implementation of the strategy
- Streamline and improve the Regional Standards program tools and IT based solutions
- Refine the records retention programs to ensure sufficient documentation exists for regulatory approvals
- Develop document management systems to allow the efficient and effective revisions of documents, control of authorship and security of documents
- Identify improvements in process for feedback loops to ensure that event analysis and investigation lessons learned and compliance issues involving violations are fed into the standards program area, as appropriate for review and potential consideration when revising standards
- Support the creation of an ERO standards database, available to industry and online, to identify and review issues related to all approved and developing standards
- Participate in the Functional Model Working Group activities to refine functions, tasks and responsibilities of applicable entities
- Solicit and provide outreach to FERC in the Regional Standards Development Processes

7) Communications

- Improve automated notifications process to assure awareness of dates and proceedings of all standard development activities
- Strengthen the relationship with the industry's technical committees to ensure adequate input to standards development, such as the North American Generator Forum.
- Participate in NPCC and NERC workshops as necessary, to promote awareness and educate the industry
- Develop and institute a consensus building and notification process(es) for engaging stakeholders and providing immediate notification for the need to review standards. Provide the associated coordination for this review utilizing subject matter experts, both internal and external to the Regional Entity staff
- Promote the reliability objectives of the NERC standards as appropriate to the NPCC members of the NERC Registered Ballot Body in order to achieve consensus and support of beneficial standards and to promote the "One-Enterprise" model.

Technically excellent, results based standards that enhance reliability and are developed in a timely and efficient fashion, require the full participation of the right industry experts from all Regional Entities when developing Reliability Standards. The NPCC RSC promotes the drafting team process and solicits drafting team members from appropriate NPCC technical bodies and others in the industry and adjoining Regional Entities. In addition the NPCC RSC works with the individual NERC standards developers to participate in Regional outreach and coordination of issues at each NPCC RSC meeting.

NPCC RSC will also assist in providing notifications and announcements to NPCC participants in the Northeastern North America NERC Registered Ballot Body of important applicable deadlines for ballot pool registration and for casting ballots thereby enhancing participation, promulgation of important information and increasing awareness. In the fourth quarter of 2014 NERC will "roll out" a new Standards Balloting System (SBS). This new system will require training and an implementation communication plan. NERC will develop the training and NPCC will assist in providing it throughout the Northeast. The SBS will require all users to reregister to cast ballots as well as submit comments. This support will enhance efficiency of the NERC procedure and help to ensure the necessary quorums are present at ballot and help to clean up the registered ballot body list. NPCC will also, when practical, promote important standards and the requirements of those standards through various communications.

NPCC will also participate in the development and revision of standards as directed by FERC, Canadian provincial and other regulatory and/or governmental authorities. FERC to date has identified numerous NERC Reliability Standards needing further work and has issued numerous Directives appearing in FERC Orders. In 2013 FERC also issued remanded interpretations and standards which require NERC to address commissions concerns as outlined in the associated Orders. These remands have created a need for NERC to review existing processes and determine approaches going forward. NPCC will support these efforts and will lead the review and potential revision of the NERC Interpretation process. These standards needing revision are delineated in the 2014 – 2016 NERC Reliability Standards Development Plan, and will be ready to be reviewed and revised throughout 2015.

NPCC will provide support and coordination of NERC standards development activities as outlined in the 2014-2016 Reliability Standards Development Plan and the Standards Committee and ERO strategic goals and initiatives.

Regional Standards Development

The NPCC currently has two FERC approved Regional standards, Disturbance Monitoring and Underfrequency Load Shedding. NPCC has undertaken the review of the Disturbance Monitoring standard for adequacy from the perspective of a "bright line" BES definition and currently developing PRC-002-2 Disturbance Monitoring continent wide standard. This review of the standard and proposed revision to the standard will be performed in the 2014-2015 timeframe. In addition there are two other Regional standards that NPCC may review to determine if they should move forward into active formal development. These Regional Standards will include, but not be restricted to the following:

- Special Protection Systems (SPS) scheduled to begin development in 2014
  Balancing Authority Controls (BA - Reserve Sharing)

Whether NPCC pursues these Regional standard will depend in large part to how comprehensive their associated continent-wide standards are. NPCC will review the continent wide standards as they are develop, participating in those activities and providing supporting subject matter expertise as it is available.

Based on the portion of professional/technical staff time and other resources devoted to Reliability Standards development, NPCC estimates that it will expend approximately 10 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- Meeting expenses will be minimized due to a continued effort to keep costs down by holding more meetings via WebEx and teleconferences, at the NPCC offices or member facilities when possible, as well as lower meeting space rental rates through negotiations. However, meeting volume is expected to increase in 2015. Travel expenses due to continued practice of advance bookings, adjustments to class of hotel used, increased meetings at NPCC's offices, and meetings conducted via teleconference will be held to a minimum. Conference calls and Internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, will be conducted for business when practical.

Operating Expenses and Indirect Expenses

- 2015 Reliability Standards program funding is driven by the need for additional activities to support NERC standards activity to achieve a results based, adequate, set of steady state standards, FERC activity and increased number of rulings and directives are anticipated as a result of the NERC three year work plan. NPCC anticipates expanded activity and plans to prioritize the efforts of existing resources to meet this expanded workload to support reliability and the ERO Strategic Goals. In addition, as standards reviews increase in number, there may be a need to have contractors assist due to constrained resources of NPCC Staff and members.

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Reliability Standards Program

Funding sources and related expenses for the Reliability Standards section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures 2014 Budget & Projection, and 2015 Budget						
Reliability Standards						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 1,431,239	$ 1,431,239	$ -	$ 1,426,577	$ (4,663)
	Penalty Sanctions	16,091	16,091	-	29,552	13,462
Total ERO Funding		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
Expenses						
Personnel Expenses						
	Salaries	$ 502,840	$ 502,840	$ -	$ 535,458	$ 32,618
	Payroll Taxes	31,305	31,305	-	31,420	115
	Benefits	131,342	131,342	-	93,684	(37,658)
	Retirement Costs	87,449	87,449	-	85,075	(2,374)
Total Personnel Expenses		**$ 752,936**	**$ 752,936**	**$ -**	**$ 745,638**	**$ (7,299)**
Meeting Expenses						
	Meetings	$ 25,000	$ 25,000	$ -	$ 20,000	$ (5,000)
	Travel	110,000	110,000	-	115,000	5,000
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 135,000**	**$ 135,000**	**$ -**	**$ 135,000**	**$ -**
Operating Expenses						
	Consultants & Contracts	$ 30,000	$ 30,000	$ -	$ 25,000	$ (5,000)
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
	Depreciation	-	-	-	-	-
Total Operating Expenses		**$ 30,000**	**$ 30,000**	**$ -**	**$ 25,000**	**$ (5,000)**
	Total Direct Expenses	**$ 917,936**	**$ 917,936**	**$ -**	**$ 905,638**	**$ (12,299)**
Indirect Expenses		**$ 555,686**	**$ 555,686**	**$ -**	**$ 561,221**	**$ 5,535**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 1,473,622**	**$ 1,473,622**	**$ -**	**$ 1,466,858**	**$ (6,764)**
Change in Assets		**$ (26,292)**	**$ (26,292)**	**$ -**	**$ (10,729)**	**$ 15,563**
Fixed Assets						
	Depreciation	$ -	-	$ -	-	$ -
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(26,292)	(26,292)	-	(10,729)	15,563
Inc(Dec) in Fixed Assets (C)		**(26,292)**	**(26,292)**	**-**	**(10,729)**	**15,563**
TOTAL BUDGET (=B+C)		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ -**	**$ -**	**$ -**	**$ 0**	**$ (0)**

Compliance Monitoring and Enforcement and Organization Registration and Certification Program

Compliance Monitoring and Enforcement and Organization Registration and Certification Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	16.00	16.00	0.00
Direct Expenses	$5,080,485	$5,440,048	$359,564
Indirect Expenses	$3,034,462	$3,064,686	$30,225
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($35,575)	$63,410	$98,985
Total Funding Requirement	$8,079,371	$8,568,145	$488,774

Program Scope and Functional Description

The Compliance Monitoring and Enforcement and Organization Registration and Certification Program (CORC) Program scope covers: 1) the identification, registration and certification of those entities responsible for meeting the NERC Reliability Standards and any approved Regional Standards; 2) the implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) in the United States, including the compliance monitoring, assessment and enforcement of NERC Reliability Standards and Regional Reliability Standards. and 3) the implementation of compliance monitoring, assessment and enforcement recommendations in accordance with individual executed MOUs or Agreements in the Canadian Provinces of Ontario, Québec, New Brunswick and Nova Scotia.

The NPCC Compliance Committee (CC) is charged with providing objective stakeholder policy input to NPCC's implementation of the CMEP in the U.S. and compliance related activities under the above mentioned MOUs in the NPCC portion of Canada. With regard to NERC Reliability Standards and Regional Reliability Standards, the CC provides an oversight role of the independent NPCC compliance staff's implementation of the CMEP. In this oversight role the CC will review and endorse the processes used by the NPCC compliance staff in the conduct of the CMEP.

The NPCC compliance staff makes the initial and final determination of alleged violations and determines appropriate penalties and sanctions in accordance with the NERC *Sanction Guidelines*. To accomplish this objective, NPCC's compliance staff is further divided into four sub- program areas: Compliance Implementation and Registration; Compliance Audit Program; Compliance Enforcement; and Compliance Investigation:

Compliance Implementation and Registration

The Compliance Implementation and Registration sub-program is responsible for:

a) Identifying for registration, using a risk based registration model, all entities that are required to meet the NERC and Regional Reliability Standards. During the course of this activity, regular communication with registered entities is promoted through face-to face meetings, compliance workshops, teleconferences and email;
b) Development and maintenance of all CMEP Compliance Procedures, Compliance Instructions and all other CMEP related documentation;
c) Development and maintenance of Performance Metrics that are used to measure the quality and effectiveness of CMEP Implementation and its impact on the reliability of the Bulk Electric System;
d) Coordinating the implementation of NPCC Compliance Staff responsibilities as they pertain to the executed MOU with each of the Canadian Provinces in the NPCC Region.
e) Day-to-day implementation of the CMEP;
f) Development of annual CMEP Implementation Plan;
g) Monitoring and assessment of self-certification, self-report, exception reporting, periodic data and complaint submittals;
h) Development and maintenance of CMEP Data Administration Application (CDAA);
i) Development and maintenance of compliance website.
j) Support the anticipated expansion of the number of registered entities in NPCC due to the implementation of the FERC Order related to the definition of Bulk Electric System
k) Conduct Entity Impact Evaluations. Conduct certification(s) of newly identified Transmission Operators (TOPs), as needed.
l) Maintain database of BES assets subject to NERC and NPCC Reliability Standards
m) Participation on various NERC and NPCC working groups to remain apprised of changes to Compliance processes, and commonality of registration, monitoring, auditing, and enforcement approaches.

Compliance Audit Program

The Compliance Audit Program is charged with conducting both on-site and off-site compliance audits, and spot checks, of NERC Reliability Standards in accordance with the NERC Rules of Procedure and associated NPCC procedures developed under the NPCC Compliance Implementation Program. These audits are performed on the basis of risk to the BES. The yearly schedule is produced consistent with Risk Assessment of registered entities and the frequency of their last audit. The schedule is posted annually on NERC and NPCC public websites. Flexibility may be used in the predefined frequency based on the risk assessment and performance based assessment of each entity scheduled for an audit, and changes requiring certification. The audits are led by qualified senior NPCC Staff and the audit teams prepare public and non-public audit reports with their findings, including the identification of any possible violations. Contents and processing of the reports are in accordance with NERC directives for audit reporting. Specific lessons learned are factored into the audit program to promote continuous improvement and are presented at workshops in conjunction with the Compliance Implementation Program. The comprehensive spot-check program is established based on the NERC actively monitored list, NPCC's assessment of self-certifications, follow–ups on entities who have previously violated a Reliability Standard, follow-up on entities that have been involved in a significant system event, and other requirements which at the discretion

of NPCC could pose a higher risk to reliability if not followed properly. The schedule for Spot Checks is not public.

Resources from the Compliance Audit Program are also used to implement the Certification process for entities intending to register as new TOPs, BAs or RCs, as well as certification reviews of changes made by existing TOPs, BAs and RCs that meet the threshold requiring same. These actions are performed in support of the Compliance Registration Program which encompasses the Certification process. Resources for this activity, which is independent of the audit process, depend on the scope, function, and location of the entity being certified.

Compliance Investigation

A Compliance Investigation (CI) may be initiated at any time by NPCC in response to a system disturbance, complaint, or possible violation of a Reliability Standard identified by any other means. The CI process requires the establishment of an investigation team that coordinates with NERC and FERC as necessary; and also coordinates with the Situation Awareness Program Area.

Compliance Enforcement

In processing identified violations NPCC Compliance Enforcement will strive to promote both timeliness and transparency of compliance results, including those efforts associated with meeting the enforcement metrics described below. In addition NPCC will promote the use of self-identification of non-compliance and implementation of discretion, including increased utilization of streamlined tracks such as FFT and discretion as shown below.

Compliance Enforcement responsibilities:

a) Issuing all Notices as described in the CMEP including the Notice of Possible Violation (NOPV), Notice of Find, Fix and Track (FFT) Treatment; Notice of Alleged Violation (NOAV), and the Notice of Confirmed Violation (NOCV);
b) Conducting comprehensive enforcement investigations based on the facts and circumstances related to all possible violations of Reliability Standards, whether identified in an audit, a self-report, complaint, or other source, and determining whether further action is warranted;
c) Reviewing, approving, submitting to NERC and tracking the progress of all mitigation plans /mitigating activities associated with confirmed violations;
d) Coordinating settlement activities once they have been initiated and submitting settlement agreements to NERC for approval;
e) Identifying and processing candidates for the FFT Process;
f) Participating in the Hearing Process by representing NPCC before the Hearing Body. Compliance Hearings would be conducted at NPCC under the supervision of a qualified, independent hearing officer contracted by NPCC;
g) Issuing Remedial Action Directives when appropriate; and
h) Implementing of the Reliability Assurance Initiative (RAI), including :
    i. Notifying the registered entity, within 60 days on average, whether a non-compliance will proceed through enforcement, be treated as a compliance exception or additional information is needed (“Triage”);
    ii. Utilizing the Aggregation of Minimal Risk Process; and
    iii. Utilizing the Enforcement Discretion Process.

A set of enforcement metrics, that include those metrics included in the ERO Corporate Goals, are produced that cover the following:

a. Caseload Index and Violation Aging
b. Mitigation Aging
c. Percentage of self-identified violations
d. Percentage of minimal and moderate risk violations through FFT, SNOP or discretion

Each of these metrics will have target values defined that are consistent with those target values identified in the ERO Corporate Goals.

2015 Key Assumptions and Cost Impacts

2014	Projected 2015
3 Large On-Site Audits	4 Large On-Site Audits
0 Medium On-Site Audits	0 Medium On-Site Audits
3 Small On-Site Audits	3 Small On-Site Audits
12 On-Site CIP Audits	4 On-Site CIP Audits
20 Large Off-Site Audits	8 Large Off-Site Audits
7 Medium Off-Site Audits	21 Medium Off-Site Audits
7 Small Off-Site Audits	10 Small Off-Site Audits
22 Off-Site CIP Audits	24 Off-Site CIP Audits
300 Spot Checks	350 Spot Checks
8 On-site TFE Part B reviews	4 TFE Part B Reviews
200 Violations (Estimated)	200 Violations (Estimated)
Settlements Covering 100 Violations	Settlements Covering 100 Violations
2 Hearings (Unbudgeted)	2 Hearings (Unbudgeted)
1 CI (Estimated)	1 CI (Estimated)
0 Entity Certifications	2 Entity Certifications

- Regarding the Compliance Audit Program, Technical Feasibility Exception (TFE) reviews are conducted both on-site at the entity's facility and at the NPCC offices when possible. TFE's continue to be requested as entities replace and install new equipment/devices/components that meet the criteria set forth in Rules of Procedure Appendix 4D. Compliance estimates 4 on-site reviews will be performed in 2015.

- Increases in Audit costs reflect Risk Assessment activity that is the basis for audit scoping. The Risk Assessment includes an assessment of an entity's Internal Controls which will be used for future audits in the scoping and frequency of engagements.
- Potential increases due to the newly identified role related to implementing the QCMEP in Quebec and the continuing role of implementing the NB CMEP in New Brunswick.

- The 2015 Business Plan projects no increases in Enforcement Processing activities over the 2014 Budget.
- The 2015 Business Plan projects the need for 1 Compliance Investigation. These Compliance Investigations are manpower intensive for NPCC staff (requiring allocation of more resources and potentially higher than normal costs) since previous Compliance Investigations have also included entities outside of NPCC's footprint for which NPCC is the Compliance Enforcement Authority.

2015 Goals and Key Deliverables

- Conduct 2015 CMEP consistent with the Reliability Assurance Initiative, incorporating Risk Assessment; Internal Control assessment; Aggregation of Minimal Risk Violations; and Enforcement Discretion and all NERC Reliability Standards contained in the NERC actively-monitored list for 2015 and any approved and applicable Regional Reliability Standards
  - Process identified violations as effectively as possible, including the timely identification of a violation, timely issuance of violation notices including the NOPV; the Notice of Alleged Violation and the NOCV
  - Implement settlement process when applicable and send proper notifications to NERC and FERC
  - Conduct necessary Hearings related to resolution of outstanding disputes regarding violations and/or sanctions. Send results of hearings to NERC and FERC[17];
- Continue to enhance the settlement process by modifying existing practices and adopting new practices to reduce the duration of settlement negotiations without sacrificing the rigor and quality of the negotiated settlements. Develop and analyze appropriate performance metrics that track settlement process duration and utilize results of analysis to further enhance process.
- Implement compliance responsibilities identified in the approved Canadian MOUs[18];
- Annual report to NERC and Régie on NPCC implementation of QCMEP
- Annual report to NERC and New Brunswick Electric Utility Board (EUB) on NPCC implementation of NB CMEP.
- Review and revise NPCC Compliance Registry based on a risk-based approach[19] ;
- Evaluate CMEP and Canadian entity compliance program implementation with the objective of establishing a long-term strategy for compliance improvement, and initiate the implementation of the long term strategy[20];
- Provide NPCC Regional Entity input, through participation in appropriate NERC compliance committees, on policy and implementation issues related to compliance and enforcement including the development of compliance elements for all new or revised NERC Reliability Standards[21];

[17] In support of ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[18] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[19] In support of ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[20] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[21] ERO Goal 6. Promote a culture of reliability excellence.

- Provide required information to NERC on a timely basis including reporting of alleged violations and confirmed violations[22];
- Track the progress of, report status of, and approve mitigation plans[23];
- Conduct 2015 Compliance Audit Schedule based on risk to the BES and number of registered entities (Each audit covers a single registered entity that could be audited for multiple Functional Model types that they are registered for and is done in accordance with the 2015 Compliance Audit Program schedule)[24] ; and promote RAI initiatives by:
    - Utilizing the Audit Checklist and Auditor's Handbook for all on-site and off-site audits
    - Preparing a Risk Assessment and Internal Control Assessment for all on-site audits[25];
- In addition, 28 registered entities will be audited for the requirements of the version in place for CIP 002 to CIP 009. These will be separate audits. On-site CIP audits may be combined with the normally scheduled 2015 on-site audits[26];
- A spot check can be viewed as a limited unscheduled small off-site compliance audit that will be utilized to verify self-certification submittals that have been done earlier in the year or other requirements based on factors as described in the Compliance Audits section. In 2015 the number of spot checks to be done is estimated to be 350[27] ;
- Assure that NPCC Staff is trained to conduct Compliance Audits including CIP Compliance Audit training[28];
- Assure that NPCC Staff is trained to conduct Certification of entities intending to Register as BA, RC or TOP for the first time, or Certification Reviews of changes by existing BAs, RCs or TOPs that meet the criteria requiring a Certification Review[29];
- NPCC is working with the other Regions to access, train and perform certifications (and re-certification) in an effort to be consistent across the ERO[30] ;
- Continue to actively perform a risk profile of each entity prior to audit and upon completion of an audit, continue to identify risk and reliability gaps[31] ;

[22] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[23] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.; ERO Goal 5. Be accountable for mitigating reliability risks.
[24] In support of ERO Goal 3a. and 3b. Promote a culture of compliance that supports reliability excellence within industry.
[25] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[26] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[27] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[28] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[29] In support of Goal 2a. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. a. The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[30] In support of Goal 2a. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. a. The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[31] In support of Goal 4a. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. a. Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.

- Develop and implement compliance reform via the Reliability Assurance Initiative (RAI) by being an integral participant in committees and workgroups involved in the RAI[32];
- Promote a culture of compliance that addresses reliability risks of NPCC registered entities by using reliability gap analysis. Assess and evaluate registered entity's Internal Controls as part of the audit and spot check process[33];
- Continue to expand the use of discretion through the utilization of compliance exception. [34] ;
- NPCC will collaborate with NERC to promote better coordination, planning, delivery and management of training efforts across the enterprise through a unified learning management system (LMS), without adversely impacting region-specific training requirements;
- Continue to implement physical security outreach and Cyber Security outreach by visiting four registered entity sites to perform an assessment of their physical security, evaluate their Cyber Security and supply recommendations for improvements[35];
- Enhance the CDAA to expand its capabilities from both the registered entity perspective and the NPCC Compliance Staff perspective[36];
- Conduct 2015 Compliance Workshops and interim information sessions for registered entities as necessary as a part of Training and Education program area[37].

Adopt and promote practices to enhance the benefits of the self-reporting of violations by both the Regional Entity and the registered entity. This would include improvement to the registered entity internal processes used for identifying and submitting self-reports (e.g. adoption of an aggregated approach for submittal of self-reports, etc.), improvement in the way Regional Entities process self-reports and the streamlining and standardizing of the amount and type of data needed to evaluate a self-report.

[32]In support of Goal 3a. Promote a culture of compliance that supports reliability excellence within industry. a. Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues.

[33]In support of Goal 3a and 4a Goal 3. Promote a culture of compliance that supports reliability excellence within industry. Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues. Goal 4. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. a. Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.

[34]In support of Goal 2b. Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. 2.b. The ERO holds industry accountable for violations that create serious risk to the BES; resulting actions are timely and transparent to industry.

[35]In support of Goal 4c. Goal 4. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

[36]In support of Goal 5c. Goal 5. Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness. 5.c. The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.

[37]In support of Goal 5a. Goal 5. Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness. 5.a. The ERO acts in a coordinated and collaborative manner with stakeholders.

Based on the portion of professional/technical staff time and other resources devoted to Compliance monitoring and enforcement and organizational registration and certification, NPCC estimates that it will expend 58 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- Meeting expenses will be minimized due to a continued effort to keep costs down by holding more meetings via teleconference, at the NPCC offices or member facilities, combining or appending meetings to other mandatory training/meetings, as well as lower meeting space rental rates through negotiations. Travel expenses due to continued practice of advance bookings, adjustments to class of hotel used, increased meetings at NPCC's offices, and meetings conducted via teleconference will be held to a minimum, however, the amount of activity is expected to increase in 2015. Conference calls and internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, will be conducted for business when possible.

Operating Expenses and Indirect Expenses

- Consultant and contractor costs increased due to increased workload related to the initial implementation of RAI, incorporating Risk Assessment and Internal Control assessment. Without this one time ramp up in RAI endeavors for 2015, contractor costs would have remained relatively flat. These joint ERO Enterprise initiatives are intended to benefit the registered entities, Regional Entities and NERC. With a risk and performance based assessment of each registered entity, audits will transition to a periodicity more reflective of the risk profile of the entity such that some audits will be more in-depth while others may have a reduced scope which will require less independent contractor resources.

- NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- Software development costs related to CMEP Data Administration Application (CDAA) and Compliance Issues Tracking System (CITS) enhancements are projected to continue into 2015.

Compliance Monitoring and Enforcement and Organization Registration and Certification Program

Funding sources and related expenses for the compliance enforcement and organization registration and certification section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Compliance Monitoring and Enforcement and Organization Registration and Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 7,991,503	$ 7,991,503	$ -	$ 8,406,767	$ 415,263
Penalty Sanctions	87,868	87,868	-	161,378	73,510
Total ERO Funding	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
Expenses					
Personnel Expenses					
Salaries	$ 2,287,504	$ 2,287,504	$ -	$ 2,393,832	$ 106,328
Payroll Taxes	162,571	162,571	-	162,511	(59)
Benefits	537,087	537,087	-	479,499	(57,588)
Retirement Costs	298,890	298,890	-	284,206	(14,684)
Total Personnel Expenses	**$ 3,286,052**	**$ 3,286,052**	**$ -**	**$ 3,320,048**	**$ 33,997**
Meeting Expenses					
Meetings	$ 25,000	$ 25,000	$ -	$ 32,000	$ 7,000
Travel	375,000	375,000	-	360,000	(15,000)
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 400,000**	**$ 400,000**	**$ -**	**$ 392,000**	**$ (8,000)**
Operating Expenses					
Consultants & Contracts	$ 1,394,433	$ 1,394,433	$ -	$ 1,728,000	$ 333,567
Office Rent	-	-	-	-	-
Office Costs	-	-	-	-	-
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 1,394,433**	**$ 1,394,433**	**$ -**	**$ 1,728,000**	**$ 333,567**
Total Direct Expenses	**$ 5,080,485**	**$ 5,080,485**	**$ -**	**$ 5,440,048**	**$ 359,564**
Indirect Expenses	**$ 3,034,462**	**$ 3,034,462**	**$ -**	**$ 3,064,686**	**$ 30,225**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 8,114,946**	**$ 8,114,946**	**$ -**	**$ 8,504,735**	**$ 389,788**
Change in Assets	**$ (35,575)**	**$ (35,575)**	**$ -**	**$ 63,410**	**$ 98,985**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	108,000	108,000	-	122,000	14,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(143,575)	(143,575)	-	(58,590)	84,985
Inc(Dec) in Fixed Assets (C)	**(35,575)**	**(35,575)**	**-**	**63,410**	**98,985**
TOTAL BUDGET (=B+C)	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ 0**

Reliability Assessment and Performance Analysis Program

Reliability Assessment and Performance Analysis Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	5.83	5.83	0.00
Direct Expenses	$1,888,972	$1,958,577	$69,605
Indirect Expenses	$1,105,682	$1,116,695	$11,013
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($52,315)	($21,349)	$30,967
Total Funding Requirement	$2,942,339	$3,053,923	$111,585

Program Scope and Functional Description

NPCC, through its top technical committee, the Reliability Coordinating Committee (RCC), integrates the deliverables of its Task Force's and Working Group's Reliability Assessment and Performance Analysis related activities. Consistent with the applicable NERC Reliability Standards, these efforts include:

- Reviewing the adequacy of the NPCC systems to supply load considering forecast demand, installed and planned supply and demand resources and required reserves in accordance with NPCC Reliability Directory No. 1 and other related reliability directories; and,
- Assessing the impact of planned transmission and resource additions or modifications on NPCC system reliability in accordance with NPCC Reliability Directory No. 1 and other related reliability directories.

Seasonal assessments of the overall NPCC resource adequacy assessments are performed and possible actions to mitigate any potential problems are identified. NPCC reviews operations and disturbances both internal and external to the Region in order to identify any lessons to be learned and recommends any necessary follow-up actions.

If appropriate, enhancements to Regional Standards or NPCC's more stringent, Regionally-specific reliability requirements are also recommended. NPCC promotes and conducts both inter-Area and inter-Regional studies to enhance reliability and operational effectiveness, and provides a forum for the discussion and coordination of operating issues within the NPCC Region and with other Regions.

2015 Key Assumptions

Support of identified key NERC Reliability Assessment and Performance Analysis (RAPA) projects; [38] NERC and Regional Entities will gather data or perform analysis in support of U.S. Federal and NERC initiatives, such as:

- Report Recommendation from the "*NERC Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances (GMD) on the Bulk Power System*", including:
  i. enhancing system models in support of the study of GMD impacts;
  ii. Enhancing GMD notification procedures; and,
  iii. Determining optimum locations for monitoring capability on transformers, based on studies and operational experience.
- Follow-up study from the recommendations of the "*2013 NERC Special Reliability Assessment: Increasing Dependence on Natural Gas for Electric Power – Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System;*"
- System frequency response analysis; and,
- Assessing reliability issues resulting from compliance to final EPA environmental regulations, reliable integration of new technologies as renewable energy, smart grid, energy storage, and/or reliability assessment of increased penetration of electric vehicles.

In support of NERC's 2015 Business Plan and Budget Program Area Services and Activities, NPCC will continue to:

- Vet proposed and future metric development, collection, and analysis with industry stakeholders and identify and spotlight trends through assessments of the availability data systems and metrics (e.g., TADS, DADS, GADS, TADS, SED, etc.)
- Conduct post-seasonal assessments (Summer and Winter) and additional scenario and special reliability assessments as required. Specialized contractors may be used to complete detailed analysis to support scenario assessments. Special reliability assessments currently proposed may include: changes in resource mix due to environmental regulations, electric/gas system interdependency, delays in proposed transmission development in the reliable integration of renewable resources.

In addition, NPCC supports:

- Development of NERC's Reliability Assessment Data System (RADS), [39] for the reporting and validation of the NERC Reliability Assessment Subcommittee Seasonal and Long-Term Reliability Assessment data requirements.

[38] In support of ERO Goal 4.- Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence

[39] In support of ERO Goal 5.c - The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.

- Evaluation of a common set of probabilistic reliability indices and probabilistic-based work products to supplement the NERC Long-Term Reliability Assessments;
- Coordination with event analysis, lesson learned [40] and model validation activities. [41] Specialized contractors may be used to complete detailed analysis to support model data collection and validation;
- Support of NERC PMO IT deployments; [42] and,
- Provide support and technical input for related BES risks identified by the NERC Reliability Issues Steering Committee (RISC). [43]

Definition of the Bulk Electric System (BES) Definition [44]

Implementation of the Bulk Electric System (BES) definition and Exception Process as of the July 1, 2014 BES Effective Date is not expected to significantly impact resources requirements in this program area for 2015. NPCC's 2014 survey of its registered entities did not indicate that an overwhelming number of NPCC BES Exception requests would be sought based on the filed BES Definition. Based on the Commission approved BES Definition [45] and the NPCC BES 2014 survey results, the 2015 RAPA personnel should be sufficient to process any NPCC BES Exception requests received in 2015.

NPCC will use the NERC PMO developed BESnet application and related BES reference and guidance documents to assist industry in the implementation of the BES definition approved by the Federal Energy Regulatory Commission. The BES reference and guidance documents, processes and tool are designed to provide industry with certainty and clarity about the implementation of the revised BES definition.

The procedure to request an exception from application of the BES definition is set forth in Appendix 5C to the NERC Rules of Procedure, effective July 1, 2014. The REMG formed the BES Exception Process Working Group (BEPWG) in 2012 – comprised of representations from the eight Regional Entities and NERC staff - to help create an efficient and effective Regional mechanism for processing Entity self-determined BES notifications and BES Exception requests. The activities of the BEPWG are expected to continue in 2015, in order to provide a Regional forum for consistent Regional BES Exception request review and 'lessons learned.'

[40] In support of ERO Goal 4.b - Events and system performance are consistently analyzed for sequence, cause, and remediation to identify reliability risks and trends and lessons learned.
[41] In support of ERO Goal 4.d - Reliability models and data accurately represent system behavior and are shared among stakeholders.
[42] In support of ERO Goal 5.c - The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.
[43] In support of ERO Goal 4.a - Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.
[44] In support of ERO Goal 2.a - The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[45] FERC Order Accepting the Revised [BES] Definition at: http://www.nerc.com/pa/RAPA/BES%20DL/2014-03-20%20BES%20-%20FERC%20Order%20Approving%20Revised%20Definition.pdf

Eastern Interconnection Reliability Assessment Group [46]

The primary function of the Eastern Interconnection Reliability Assessment Group (ERAG) is to augment reliability of the bulk-power system in the Eastern Interconnection through periodic reviews of generation and transmission expansion. These assessments are conducted by the ERAG Steering Committees. In addition, ERAG has the responsibility to develop the annual set of seasonal and future steady state and dynamic simulation base cases for use by the Regional Entities and other industry groups in the Eastern Interconnection. This is done through the ERAG Multi-Regional Modeling Working Group (MMWG). NPCC participates in the ERAG activities as one of the six Eastern Interconnection Regional Entities.

NPCC RAPA staff participates with the ERAG Management Committee and acts as the liaison between the ERAG MMWG and the NPCC SS-37 Working Group; activities include:

Management Committee Activities

- ✓ Oversee the steady state and dynamic simulation base case development;
- ✓ Make necessary changes to the modeling of governor-turbine control systems to achieve frequency response that more closely reflects actual response during system frequency deviation events. Oversee ERAG Multi-Regional Modeling Working Group (MMWG) changes to the dynamics base cases;
- ✓ Continue the review of the NERC governor survey information to assess how to revise the governor-turbine plant control models at most generators;
- ✓ Review the 2015 Summer and 2015-2016 Winter Assessments, including, the MRSS (MRO-RFC-SERC-SPP) and the R-N (RFC-NPCC) Assessments of anticipated inter-Regional, inter-Balancing Authority transfer limit conditions and sensitivities;
- ✓ Participate in discussions with NERC staff, North American Transmission Forum, NERC System Analysis and Modeling Subcommittee, FERC staff and possibly North American Generation Forum representatives regarding base case modeling improvements and future general industry modeling improvements;
- ✓ Develop ERAG Strategic Direction (i.e. anticipated new developments in MMWG process and system assessments); and,
- ✓ Confirm MMWG cases and assessments continue to have sufficient protections in place for use and transmittal of confidential data and information.

Multi-Regional Modeling Working Group Items

- ✓ Complete the steady state and dynamic simulation base cases for the 2015 series of cases;
- ✓ Complete necessary changes to the modeling of governor-turbine control systems to achieve frequency response that more closely reflects actual response during system frequency deviation events;
- ✓ Continue the review of the NERC governor survey information to assess how to revise the governor-turbine plant control models at most generators. Recommend the necessary changes in the models for specific generators;
- ✓ Incorporate dispatch information into the future and seasonal ERAG MMWG base cases so that the dispatches are more closely aligned with economic dispatch practices;

[46] In support of ERO Goal 4.d - Reliability models and data accurately represent system behavior and are shared among stakeholders.

- ✓ Determine how the Regional MMWG case development processes will change due to the use of the new web-based System Dynamics Data Base program;
- ✓ Verify procedures in the MMWG manual are followed;
- ✓ Check and confirm that the dynamic model data passes all applicable checks and acceptance criteria. Include 60 second steady state simulation of each case to detect numerical errors; and,
- ✓ Apply changes to the MMWG dynamics case so they are available for interconnection dynamics studies.

System Assessments Items

- ✓ Completion of 2015 Summer and 2015-2016 Winter Assessments, including, the MRSS and the R-N Assessments of anticipated inter-Regional, inter-Balancing Authority transfer limit conditions and sensitivities; and,
- ✓ Take additional steps to achieve consistency among the MRSS and the R-N study forums assessments and practices. Make additional recommendations to the ERAG Management Committee on how to complete this process.

NERC [47]

Through its Task Forces and Working Groups, NPCC will continue to provide the NPCC Regional perspective with active NPCC RAPA staff participation on the NERC Planning and Operating Committees and key related NERC Subcommittees, Task Forces and Working Groups:

- ✓ Reliability Assessment Data Working Group (RADWG);
- ✓ Protection System Mis-operations Task Force (PSMTF);
- ✓ Spare Equipment Database Task Force (SEDTF);
- ✓ Demand Response Availability Data System Working Group (DADSWG);
- ✓ Generating Availability Data System Working Group (GADSWG);
- ✓ Transmission Availability Data System Working Group (TADSWG);
- ✓ Model Validation Working Group (MVWG);
- ✓ Reliability Assessment Subcommittee (RAS) - Seasonal and Long-Term Reliability Assessments;
- ✓ System Analysis and Modeling Subcommittee (SAMS);
- ✓ Performance Analysis Subcommittee (PAS);
- ✓ Regional support and coordination of the NERC:
  - o Generator Availability Data System (GADS);
  - o Demand Availability Data System (DADS);
  - o Transmission Availability Data System (TADS);
  - o Spare Equipment Data Base System (SEDS);
- ✓ Incorporating any probabilistic reliability metrics required for the 2015 NERC Long-Term Reliability Assessment through the NPCC 2015 Long Range Adequacy Overview;
- ✓ Providing analytic support to ERO-RAPA group for the:
  - o Analysis of Relay and Special Protection System mis-operations;
  - o Regional coordination of data required for the calculation of metrics proposed by the NERC Reliability Metrics Working Group; and,
  - o Other activities as directed by the ERO-Executive Management Group.

[47] In support of ERO Goal 4 - Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence.

As well as:

- ✓ Updating the NPCC Electric System Map; Producing the annual NPCC Load, Capacity, Energy, Fuels, and Transmission (LCEFT) Report
- ✓ Liaison with the New York Defensive Strategies Working Group in coordination and implementation of Synchro-Phasor measurement devices on the NPCC and neighboring systems and monitor related efforts of the NERC North American Synchro-Phasor Initiative;
- ✓ Processing BES Exception requests received through the BES Exception Process;
- ✓ Participating in on-going NERC analysis of the Eastern Interconnection Frequency Response;
- ✓ Developing NPCC guidelines for load modeling in system reliability studies;
- ✓ Conducting NPCC resource adequacy assessments addressing impacts of emerging reliability issues identified by NERC (e.g., environmental requirements, gas-electric system interdependency, distributed generation, delays in transmission plans, etc.);
- ✓ Coordinating any resulting NPCC inter-Area reliability analyses required to assess the proposed integration of related large-scale renewable resource proposals from Regional activities;
- ✓ Completing the 2015 NERC Seasonal (and post Seasonal) Reliability Assessments; and,
- ✓ Completing the 2015 NERC Long-Term Reliability Assessment.

2015 Goals and Key Deliverables

Task Force on Coordination of Planning

The primary mission of the NPCC Task Force on Coordination of Planning (TFCP) is to promote reliability through the coordination of NPCC Area and NERC planning processes and activities. In addition, the TFCP provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

TFCP activities include, but are not limited to:

- Leading the NPCC Task Force review of the revision of NPCC criteria, guidelines, and procedures related to planning, and of those documents which provide for the uniform implementation, interpretation and monitoring of compliance with criteria, guidelines and procedures related to planning.
- Supporting the NPCC Directory Project by either drafting, reviewing or approving directories.
- Coordinating, monitoring, reviewing, and making recommendations on proposed or modified Special Protection Systems.
- Facilitating Wide-Area Planning by supporting the Joint ISO/RTO Planning Committee Activities, implementation of the Northeast Planning Protocol, and performing any NPCC interconnection reliability analyses, as required.
- Reviewing the overall reliability of the NPCC Areas and performing multi-Area probabilistic reliability assessments.
- Identifying and assisting in the development of new Regional Reliability Standards.
- Assisting the NPCC Compliance Subcommittee, to monitor and coordinate the compliance efforts of the Areas with NPCC planning documents and registered entities with NERC Reliability Standards.

- Reviewing the Standards Authorization Requests and NERC Reliability Standards as well as participating in the NERC process. Educating and informing NPCC membership and registered entities of developments.
- Ensuring coordination of data and assumptions for conducting NPCC planning studies (i.e. load forecasts, reserve requirements, DOE EIA 411 data, and new facilities)
- Monitoring the activities of other NPCC Task Forces to ensure coordination with planning activities.
- Reviewing the adequacy of the NPCC systems to supply load considering forecast demand, installed and planned supply and demand resources and required reserve margins in accordance with NPCC Directory No. 1 based on a schedule set forth in the Reliability Assessment Program.
- Coordinating the review of the compliance of future Area plans with the Basic Criteria, including an analysis of resource and transmission system additions, and the potential inter-Area effects of special protection systems, in accordance with NPCC Reliability Directory No.1 based on a schedule set forth in the Reliability Assessment Program. (Specific projects, which in the opinion of the Task Force could have an impact on the reliability of the NPCC Bulk Power System, may be reviewed outside of the set schedule).

Key TFCP Reliability Assessment and Performance Analysis Deliverables

- ✓ Coordinating activities related to reactive power and voltage control practices, which includes Under Voltage Load Shedding (UVLS) with the Task Force on Coordination of Operation and the Task Force on System Studies to ensure that developments in the NERC Planning Committee and its Subcommittees are addressed.
- ✓ Monitoring the actions of the NERC Performance Analysis Subcommittee (PAS).
- ✓ Monitoring the actions of the NERC System Analysis and Modeling Subcommittee (SAMS).
- ✓ Overseeing the A-10 BPS Implementation Plan.
- ✓ Overseeing the summer 2015 and winter 2015-2016 NPCC multi-area probabilistic reliability evaluations.
- ✓ Overseeing the 2015 NPCC Long-Range Adequacy Overview.
- ✓ Evaluating and approving Balancing Authority Area Transmission Reviews.
- ✓ Coordinating, monitoring, reviewing, and making recommendations on the retirement of existing in-service Special Protection Systems (SPS); and the implementation of proposed new or modified Special Protection Systems.
- ✓ Review the NPCC SPS criteria with respect to proposed NERC SPS Standards.
- ✓ Monitoring industry practices and making recommendations to NPCC on transmission adequacy standards related to intermittent generation such as wind or solar-voltaic.
- ✓ Reviewing and giving direction to other task forces on changes required to the Underfrequency Load Shedding (UFLS) program required to take into account increasing amounts of distribution connected generation and/or intermittent generation.
- ✓ Evaluating and recommending approval of NPCC Balancing Authority Area Resource Adequacy Assessments.
- ✓ Monitoring the developments in demand resources, energy efficiency, distributed generation and conservation methods including all intermittent renewable resources.
- ✓ Conducting resource adequacy assessment studies addressing emerging reliability issues as identified by the NERC Planning Committee (e.g., environmental requirements, etc.)
- ✓ Supporting Joint ISO/RTO Planning Committee activities.

- ✓ Facilitating Wide-Area Planning through participation in Regional and coordinating any resulting required inter-Area Reliability Assessment of the proposed integration related large-scale renewable resource proposals.
- ✓ Completion of the NERC 2015 Long-Term Reliability Assessment.
- ✓ Completion of the 2015 Review of NPCC Interconnection Assistance Reliability Benefits Study.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFCP activities and processes.

Task Force on System Studies

The primary mission of the NPCC Task Force on System Studies (TFSS) is to provide active overall coordination of system studies of the reliability of the interconnected bulk power systems and for the review of certain NPCC documents. In addition, the TFSS provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The activities of the TFSS include, but are not limited to:

- Participating with the Task Force on Coordination of Planning, the Task Force on Coordination of Operation, and the Task Force on System Protection in reviews of the NPCC Reliability Directory No.1 and other NERC Reliability Standards and NPCC criteria, guidelines, procedures and documents which provide for the uniform implementation, interpretation and monitoring of conformance to criteria, guidelines and procedures related to system studies.
- Conducting NPCC Balancing Authority Area Reviews, in accordance with NPCC Reliability Directory No. 1, based on material presented by the Balancing Authority Areas. These reviews will assess the impact of planned transmission and resource additions or modifications on system reliability, and determine the Balancing Authority Area's conformance with the NPCC Basic Criteria.
- Reviewing and approving changes to Balancing Authority Areas' lists of bulk power system elements, in accordance with the *Classification of Bulk Power System Elements* (Document A-10). Annually review and update the NPCC BPS List.
- Reviewing and classifying new and modified Special Protection Systems, in accordance with NPCC Reliability Directory No. 7. Annually reviewing and updating the NPCC Special Protection System List.
- Conducting such load flow, transient stability, and other studies as required analyzing the overall reliability of the planned bulk power transmission systems of NPCC and the interconnections between NPCC and other Regional reliability organizations. As a part of this effort, analyze potential inter-Area effects of Special Protection Systems.
- Conducting analytical studies as appropriate to support the coordination of system planning, system operation and system protection in NPCC.
- Maintaining, through the SS-37 Working Group, a library of load flow base cases and associated dynamics data, for use in and support of Balancing Authority Area Reviews, overall transmission assessments, operational studies, inter-Regional studies, etc. Coordinate this effort with the NERC inter-Regional base case development process.
- In conjunction with other Task Forces, reviewing major system disturbances to ascertain the adequacy of the interconnected systems. Also, reviewing any associated recommendations for system modifications and considering the need for criteria changes.

- Identifying and recommending improved system study techniques. This includes, but is not limited to, the following:
  - improved techniques and models for power system simulation;
  - improved techniques for power system Reliability Assessment;
- Conducting a periodic review of the adequacy of the NPCC underfrequency load shedding program. Annually reviewing and updating the NPCC underfrequency load shedding database.
- Maintaining a listing and monitoring the status of major transmission and generation projects within NPCC.
- Maintaining liaison with other NPCC Task Forces and report to the Reliability Coordinating Committee as required.
- Monitoring the work of industry research and development organizations such as the IEEE, Canadian Electricity Association, Electric Power Research Institute, CIGRE and other technical organizations.
- Annually developing updates to the NPCC Electric System Map

Key TFSS Reliability Assessment and Performance Analysis Deliverables:

- ✓ Conducting Balancing Authority Area reviews, in accordance with the *Guidelines for NPCC Area Transmission Reviews* (Appendix B of NPCC Reliability Directory No. 1), based on material presented by the Balancing Authority Areas. These reviews assess the impact of planned transmission and resource additions or modifications on system reliability, and determine the Area's conformance with the NPCC Basic Criteria. Through the Area Transmission Reviews, re-evaluate the performance and classification of existing SPSs and Dynamic Control Systems as appropriate.
- ✓ Reviewing and classifying new and modified Special Protection Systems, in accordance with NPCC Reliability Directory No. 7 *Procedure for NPCC Review of New or Modified Bulk Power System Special Protection Systems* as required.
- ✓ Reviewing and approving changes to the Balancing Authority Areas' lists of bulk power system elements, in accordance with the *Classification of Bulk Power System Elements* (Document A-10), as required.
- ✓ Updating the NPCC Bulk Power System List.
- ✓ Through the ad hoc Load Modeling Task Force, address the recommendations from the SS-38 Load Modeling White Paper regarding the use of dynamic load models for transient stability analysis.
- ✓ Perform the Overall NPCC Transmission Assessment.
- ✓ Reviewing and updating NPCC Undervoltage Load Shedding Database.
- ✓ Participation in on-going NERC analysis of the Eastern Interconnection Frequency Response.
- ✓ Through the SS-37 Working Group, develop the annual library of power flow base cases and associated dynamic models for use by NPCC members and input into the development of the MMWG library of power flow and dynamic cases and databases for the Eastern Interconnection
  - i. Final development of NPCC power flow models for 2015
  - ii. Final development of NPCC dynamic models for 2015
  - iii. Address wind modeling issues including maintaining a database of NPCC wind models for use in the MMWG library of power flow and dynamic cases and databases for the Eastern Interconnection.
- ✓ Annually performing event replication and exercise the procedure. Reviewing existing Regional criteria and procedures for validation of data used in power flow and dynamic

simulations by benchmarking against actual system performance. If the existing criteria or procedures are found to be deficient, propose changes to provide for adequate data validation

- ✓ Updating the NPCC SS-37 Working Group Procedure Manual and other related documents including the Master Tie line Data, and Interchange Schedule, as required.
- ✓ Providing mid-term updates to the Library of NPCC/MMWG cases
- ✓ Enhancing the governor modeling on a unit by unit basis suitable for use in the system simulation.
- ✓ Annually reviewing and updating a list of NPCC underfrequency load shedding.
- ✓ Coordinate activities with those of the New York State Defensive Strategies Working Group, regarding the coordination and implementation of Synro-Phasor measurement devices.
- ✓ Incorporate NPCC guidelines for load and power system modeling approved by the RCC
- ✓ Classification of Bulk Power System Elements.
- ✓ Participate at Siemens PTI User Group meetings to provide PSSE program enhancements
- ✓ Supporting Regional system studies to integrate large-scale renewable resources.
- ✓ Provide support to NERC Event Analysis process, as needed.
- ✓ Develop updates to the NPCC Electric System Map.
- ✓ Provide support to the NERC Model Validation Working Group (MVWG) as needed.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFSS activities and processes.

Task Force on System Protection (TFSP)

The purpose of the NPCC Task Force on System Protection (TFSP) is to promote the reliable and efficient operation of the interconnected bulk power systems in Northeastern North America through the establishment of directories, criteria, guidelines, and procedures and coordination of design, relative to the protection associated with the bulk power systems. In addition, the TFSP provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The Reliability Assessment and Performance Analysis activities of the TFSP include, but are not limited to:

- Assessing proposed protection systems and special protection systems in accordance with NPCC Reliability Directory No. 4 and No. 7.
- Reviewing and analyzing the performance of protection systems following selected major power system disturbances and events, inside as well as outside NPCC in accordance with NPCC Reliability Directory No. 4. Issue recommendations for changes to NPCC Documents, as appropriate.
- Providing technical advice on protection issues to NPCC and coordinate with other Task Forces on the application of Intelligent Electronic Devices (IEDs) that include functions related to energy management systems in addition to their protective functions, in order to safeguard the integrity of the protective functions.
- Through the SP-7 Working Group, review, on a quarterly basis all protection system (including special protection system) misoperations reported to NPCC.
- Reviewing and assessing significant protection issues of common interest or informational value.
- Reviewing and assessing regulatory and industry based documents as they relate to system protection.

- Maintaining an effective liaison with North America groups working in the protection areas (for example: NERC System Protection & Control Subcommittee.)
- Exchanging information with other power pools, Regional Reliability Councils, Regional Transmission Organizations and other industry groups on matters concerned with system protection.
- Identifying the need for special studies and new documents, recommend action to the Reliability Coordinating Committee.

Key TFSP Reliability Assessment and Performance Analysis Deliverables:

- ✓ Assessing proposed protection systems and special protection systems for compliance with NPCC Directory No. 4 and No. 7 criteria.
- ✓ Reviewing and analyzing the performance of protection systems in power system disturbances and events, brought to the attention of the Task Force, inside as well as outside NPCC in accordance with *Procedures for Task Force on System Protection Review of Disturbances* (Document C-30). Issuing recommendations for changes to NPCC Documents, as appropriate.
- ✓ Develop a new NPCC Directory for Disturbance Monitoring Equipment for related criteria, guides and procedures.
- ✓ Participate or serve as lead Task Force in the development and/or implementation of Regional Reliability Standards.
- ✓ Providing support to the NERC Event Analysis process as required.
- ✓ Participate in the ongoing development and submission of NPCC input into the development of related NERC Reliability Standards.
- ✓ Conducting any follow-up to the bulk power system protection risk assessment as directed by the Reliability Coordinating Committee.
- ✓ Through the SP-7 Working Group, monitor the review of protection system (including special protection system) mis-operations as they occurred in the NPCC Region and participation in providing the NPCC input for NERC Metric ALR4-1 on Protection Mis-operations.
- ✓ Monitor and review industry activities on the mitigation of the effects of SMD on protection systems. Report to RCC on any significant findings.
- ✓ Review mitigations and/or progress reports for BPS Risk Reduction Implementation at each meeting and annually report to the RCC on the status of this implementation.
- ✓ Participate in the development and submission of NPCC inputs/comments into the development of protection related NERC technical documents.
- ✓ Review best practices from its members and industry to pull together design considerations for the new IEC 61850 protection implementation with the output being possible additions to NPCC Directory No. 4 and Directory No. 7.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFSP activities and processes.

Task Force on Coordination of Operation

The NPCC Task Force on Coordination of Operation (TFCO) facilitates the coordination of operations among the NPCC Reliability Coordinator areas and adjacent NERC Regions to enhance the reliability of the bulk power system. In addition, the TFCO provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The activities of the NPCC TFCO include, but are not limited to:

- Conducting seasonal reviews of the overall reliability of the generation and transmission systems in NPCC, and coordinating these efforts with parallel assessments conducted by the NPCC Task Force on Coordination of Planning and by NERC. Reviewing the operational preparedness of NPCC and recommending possible actions to mitigate any potential problems identified for each operating period.
- Reviewing operations and system disturbances and providing any necessary follow-up, including the recommendation of remedial or mitigating actions.
- Facilitating the reliable operational integration of new bulk power system facilities.
- Coordinating the development of operating NPCC requirements and procedures affecting the reliability and operability of the bulk power system in coordination with, and as directed by, NERC and NPCC.
- Promoting and sponsoring inter-Balancing Authority Area and inter-Regional studies to enhance reliability and operational effectiveness of the bulk power system.
- Providing coordination of operating issues with other NPCC Task Forces and other Regions.
- Reviewing, and acting upon, NERC actions, motions and recommendations in relation to the operation of the power system.
- Formulating the position of the TFCO on NERC Standards, and providing this position to the NPCC Regional Standards Committee as appropriate.
- Providing assistance as requested by the NPCC Regional Standards Committee in the development of Regional Standards and Directories.
- Providing assistance as requested by the NPCC Compliance Committee in monitoring and coordinating the compliance efforts of the registered entities of NPCC.

Key TFCO Reliability Assessment and Performance Analysis Deliverables:

- ✓ Review and analyze the performance of Simultaneous Activation of Reserve implementation following an event to enhance the process. Manage the implementation of action items emanating from the NERC report, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System-June 2010," and its subsequent reports:
  - ➢ Severe Impact Resilience Severe Impact Resilience Task Force
  - ➢ Geomagnetic Disturbance Task Force
  - ➢ Cyber Attack Task Force
  - ➢ Spare Equipment Database Task Force
  - ➢ Smart Grid Task Force
- ✓ Monitor the development of the NERC North American Synchro-Phasor Initiative in its effort to establish an effective control monitoring tool.
- ✓ Provide assistance to the NPCC Regional Standards Committee in the second phase of the NPCC directories process.
- ✓ Review NPCC Reliability Coordinator Area Restoration Plans.
- ✓ Complete the NPCC 2015 summer and winter Operational Reliability Assessments.
- ✓ Completion of the NERC 2015 Seasonal Reliability Assessments.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFCO activities and processes.
- ✓ Support the implementation of the NERC Cyber Standards, as required.

NPCC Regulatory/Governmental Affairs Advisory Group

The purpose of the NPCC Regulatory/Governmental Affairs Advisory Group is to promote NPCC interaction and coordination with Federal/State/Provincial governmental and/or regulatory agencies on a coordinated Regional basis, and identify and develop policy input for NPCC and Northeast Regional governmental and/or regulatory bodies.

The NPCC Governmental/Regulatory Affairs Advisory Group provides a forum where industry and governmental and/or regulatory representatives can exchange views and strive to develop consensus policy recommendations on reliability issues specific to the NPCC Region (Northeastern United States and Eastern Canada) and share actionable information among NPCC, NERC and other related governmental and/or regulatory agencies related to Regional energy and reliability matters.

Based on the portion of professional/technical staff time and other resources devoted to Reliability Assessment and Performance Analysis, NPCC estimates that it will expend 21 percent of its resources on these activities.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- While the amount of activity continues to increase in 2015, due to the volume of work described above, meeting expenses will be minimized to the extent possible due to continued efforts to keep costs down by holding meetings via conference calls and internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, conducting meetings at the NPCC offices or member facilities, as well as negotiating lower meeting space rental rates.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Reliability Assessment and Performance Analysis Program

Funding sources and related expenses for the Reliability Assessment and Performance Analysis section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Reliability Assessment and Performance Analysis

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 2,910,322	$ 2,910,322	$ -	$ 2,995,121	$ 84,799
Penalty Sanctions	32,017	32,017	-	58,802	26,785
Total ERO Funding	**$ 2,942,339**	**$ 2,942,339**	**$ -**	**$ 3,053,923**	**$ 111,585**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 2,942,339**	**$ 2,942,339**	**$ -**	**$ 3,053,923**	**$ 111,585**
Expenses					
Personnel Expenses					
Salaries	$ 904,028	$ 904,028	$ -	$ 937,098	$ 33,070
Payroll Taxes	60,329	60,329	-	61,387	1,058
Benefits	226,225	226,225	-	196,252	(29,973)
Retirement Costs	190,390	190,390	-	172,840	(17,550)
Total Personnel Expenses	**$ 1,380,972**	**$ 1,380,972**	**$ -**	**$ 1,367,577**	**$ (13,395)**
Meeting Expenses					
Meetings	$ 45,000	$ 45,000	$ -	$ 41,000	$ (4,000)
Travel	175,000	175,000	-	185,000	10,000
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 220,000**	**$ 220,000**	**$ -**	**$ 226,000**	**$ 6,000**
Operating Expenses					
Consultants & Contracts	$ 275,000	$ 275,000	$ -	$ 365,000	$ 90,000
Office Rent	-	-	-	-	-
Office Costs	13,000	13,000	-	-	(13,000)
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 288,000**	**$ 288,000**	**$ -**	**$ 365,000**	**$ 77,000**
Total Direct Expenses	**$ 1,888,972**	**$ 1,888,972**	**$ -**	**$ 1,958,577**	**$ 69,605**
Indirect Expenses	**$ 1,105,682**	**$ 1,105,682**	**$ -**	**$ 1,116,695**	**$ 11,013**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 2,994,654**	**$ 2,994,654**	**$ -**	**$ 3,075,272**	**$ 80,618**
Change in Assets	**$ (52,315)**	**$ (52,315)**	**$ -**	**$ (21,349)**	**$ 30,967**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(52,315)	(52,315)	-	(21,349)	30,967
Inc(Dec) in Fixed Assets (C)	**(52,315)**	**(52,315)**	**-**	**(21,349)**	**30,967**
TOTAL BUDGET (=B+C)	2,942,339	2,942,339	-	3,053,923	111,585
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ 0**	**$ 0**	**$ -**	**$ 0**	**$ 0**

Training, Education, and Operator Certification Program

Training, Education, and Operator Certification Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.10	0.10	0.00
Direct Expenses	$177,787	$180,222	$2,434
Indirect Expenses	$18,965	$19,154	$189
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($897)	($366)	$531
Total Funding Requirement	$195,855	$199,010	$3,154

Program Scope and Functional Description

The NPCC Training, Education, and Operator Certification program supports NERC Rules of Procedure Section 900. The program provides education and training necessary to understand and operate the bulk electric system. The target audience of the program is bulk power system operating personnel - including system operations personnel, operations support personnel (engineering and information technology), supervisors and managers, and training personnel. This program also supports the administration of records necessary to maintain status as a NERC Continuing Education provider. NPCC staff training and development is incorporated within each respective program area.

Training Program Background and Description

NPCC establishes and coordinates programs for system operator training relating to inter-Reliability Coordinator area matters, criteria, terminology, standards and operating procedures and instructions. It develops and conducts training seminars, held twice yearly, at which potential operational problems for the coming season are discussed, the implementation of NPCC standards and procedures are discussed, significant disturbances are reviewed for lessons to be learned and table-top drills and communication and coordination exercises are conducted. The seminars promote camaraderie and better communication among system operators from the NPCC Reliability Coordinator Areas.

NPCC shares, evaluates and proposes new techniques and training aids as they become available; reviews opportunities to consolidate training among the NPCC Reliability Coordinators, which includes opportunities to share training material and training sessions and exchanges information on internal methods of system operator selection and training.

In addition, NPCC participates in the activities of the NERC Staff Training Group (STG). The main objective of the NERC STG is to coordinate the development of Regional Entity and NERC staff training and registered entity education materials to support and continually enhance reliability across North America for the benefit of all bulk electric system users, owners, and operators. The main focus of this group has been on NERC compliance auditor training.

Funding Drivers and Reliability Benefits

- Provide two high-quality continuing education seminars for system operators
    - System operators participating in the Seminars get exposure to NPCC issues and current industry operations topics, review recent NPCC or major external disturbances, discuss projected conditions for the coming summer or winter peak season and participate in hands on "table top exercises" pertaining to system operation practices. PJM operators also attend and participate in these seminars.
    - Seminar attendees also receive Continuing Education Hours (CEHs) and each Balancing Authority Area utilizes the seminar content by including it in their internal training programs to provide CEHs to all system operators
    - The seminars help to improve system operation coordination through better camaraderie among operators
- Review and revise the curriculum of the training seminars to better emphasize NERC standards, Regional Standards and business practices, NPCC wide-area operations and Regionally-specific criteria and procedures.[48]
- Enhance the system operator's awareness and knowledge of the standards, criteria and procedures they apply in real time operation.[49]
- Provide more sharing of new training approaches, exchange of information on internal methods of system operator selection, training material and training sessions.
    - Enhance efficiency and cost savings in the training programs in the NPCC Balancing Authority Areas
- Provide a forum among NPCC Reliability Coordinator / Balancing Authority (RC / BA) Areas for sharing of approaches to meet the requirements of the NERC PER standards. The sharing of approaches used by some NPCC Areas to address the PER-005-1, Requirement 3.1 on Training using simulator technology has been especially valuable to CO-2 Working Group members.
- Determine what changes would be needed for the NPCC Reliability Coordinator / Balancing Authority Areas to meet proposed expanded Systematic Approach to Training (SAT) requirement for operations support staff in PER-005-2.

2015 Key Assumptions

NPCC will conduct two workshops in 2015, for NPCC Stakeholders, for the express purpose of providing the most current and applicable information related to the development of NERC and Regional Reliability Standards and the implementation of the Compliance Monitoring and Enforcement Program (CMEP). These workshops are specifically designed, primarily through the conduct of targeted breakout class room sessions and presentations on current industry related activities, to provide for the most efficient exchange of information between the NPCC Compliance and Standards Staff and the NPCC Stakeholders. Presentations in the past have been conducted by FERC, NERC and Stakeholder representatives in addition to NPCC Staff members. To supplement these workshops, NPCC is also considering expanding the use of on-

[48] In support of ERO goal 4.b. Provide lessons learned and recommendations from events and identified risks.
[49] In support of ERO goal 4.b. Analyze significant events to identify gaps in standards, compliance effectiveness, registration, and risk controls effectiveness.

line webinars. These webinars will focus on a specific topic pertinent to developments related to compliance program implementation, standards development or technical topics.

NPCC also regularly conducts spring and fall System Operator Seminars. These seminars involve system operators from the NPCC Reliability Coordinator / Balancing Authority Areas and PJM. These will be held in early May and early November.

With the exception of meeting expenses, it is proposed that the NPCC resources to support Training and Education will remain virtually unchanged for the calendar year. In 2015, to be consistent with NERC and other Regional Entities, NPCC will charge for participation in NPCC workshops in an effort to defray some of the costs.

2015 Goals and Key Deliverables

- Prepare and conduct the spring and autumn NPCC System Operator Seminars
- Review approaches to reliability related-task definition, task instruction, and instruction tracking on an individual basis. Coordinate the effects of the PER-005-2 expanded SAT training requirements within the NPCC RC / BA Area programs.
- Expand the content of the Reliability Coordinator training programs, based on the new requirements generated by PER-005-2.
- Continue collaboration and sharing of the intended RC / BA approaches, experiences and materials to task identification and training development associated with NERC Standard PER-005-2.
- Create and expand the restricted-access NPCC repository of training resources and learning verification activities addressing fundamental power system topics, training methods and operation procedure training exercises, which may be shared as elements of operator training in compliance with NERC Standard PER-005, “System Personnel Training”.
- Participate in NERC Staff Training Group activities and provide NPCC input to the development of training policies by this group.

Based on the portion of professional/technical staff time and other resources devoted to training, education, and operator certification, NPCC estimates that it will expend 1 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Training, Education, and Operator Certification Program

Funding sources and related expenses for the training, education, and operator certification section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Training, Education, and Operator Certification

		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 131,306	$ 131,306	$ -	$ 134,001	$ 2,695
	Penalty Sanctions	549	549	-	1,009	459
Total ERO Funding		**$ 131,855**	**$ 131,855**	**$ -**	**$ 135,010**	**$ 3,154**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	64,000	64,000	-	64,000	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 195,855**	**$ 195,855**	**$ -**	**$ 199,010**	**$ 3,154**
Expenses						
Personnel Expenses						
	Salaries	$ 17,448	$ 17,448	$ -	$ 18,460	$ 1,012
	Payroll Taxes	1,063	1,063	-	1,274	211
	Benefits	4,500	4,500	-	4,052	(448)
	Retirement Costs	4,776	4,776	-	4,436	(341)
Total Personnel Expenses		**$ 27,787**	**$ 27,787**	**$ -**	**$ 28,222**	**$ 434**
Meeting Expenses						
	Meetings	$ 135,000	$ 135,000	$ -	$ 137,000	$ 2,000
	Travel	15,000	15,000	-	15,000	-
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 150,000**	**$ 150,000**	**$ -**	**$ 152,000**	**$ 2,000**
Operating Expenses						
	Consultants & Contracts	$ -	$ -	$ -	$ -	$ -
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
	Depreciation	-	-	-	-	-
Total Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Total Direct Expenses	**$ 177,787**	**$ 177,787**	**$ -**	**$ 180,222**	**$ 2,434**
Indirect Expenses		**$ 18,965**	**$ 18,965**	**$ -**	**$ 19,154**	**$ 189**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 196,753**	**$ 196,753**	**$ -**	**$ 199,376**	**$ 2,623**
Change in Assets		**$ (897)**	**$ (897)**	**$ -**	**$ (366)**	**$ 531**
Fixed Assets						
	Depreciation	$ -	-	$ -	$ -	$ -
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(897)	(897)	-	(366)	531
Inc(Dec) in Fixed Assets (C)		**(897)**	**(897)**	**-**	**(366)**	**531**
TOTAL BUDGET (=B+C)		195,855	195,855	-	199,010	3,154
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ 0**

Situation Awareness and Infrastructure Security Program

Situation Awareness and Infrastructure Security Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.00	3.00	0.00
Direct Expenses	$922,070	$937,689	$15,619
Indirect Expenses	$568,962	$574,629	$5,667
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($26,920)	($10,986)	$15,935
Total Funding Requirement	$1,464,111	$1,501,332	$37,221

Program Scope and Functional Description

The Situation Awareness and Infrastructure Security Program is the combination of near real time awareness of conditions on the bulk power system with the programs necessary to increase the physical and cyber security of the electricity infrastructure, including the operation and maintenance of tools and other support services for the benefit of Reliability Coordinators and the system operators within the registered entities. Maintaining the real-time awareness of conditions on the interconnected bulk power systems by the NPCC Reliability Coordinator is critical to maintaining reliable operation within NPCC, including the communication of information concerning system conditions and abnormal events among the neighboring system operators responsible for the reliable operation of the bulk power systems. When a disturbance does occur, it is critical to use the event as a learning opportunity and provide a forum for the active coordination of reliability and operation among the NPCC Reliability Coordinator areas and neighboring NERC Regions to enhance the reliability of the interconnected bulk power system through the lessons to be learned which can be gleaned from such an event.

Event Analysis Program[50]

NERC and the industry pursue three avenues in the analysis of a disturbance: the identification of lessons to be learned, a formal cause code analysis and a review of applicable standards.

The Event Analysis Program recognizes that many events which occur on the bulk power system beyond the routine reporting requirements previously in place can have varying levels of significance to the electric system, providing otherwise unrealized lessons to be learned from these events and the trending of such events to identify possible reliability concerns. By integrating a "bottom-up" approach to a disturbance review within the framework of the NERC Event Analysis Program, consistency, comparability, flexibility and timeliness in the event analysis process will be promoted by NPCC, the registered entities and NERC in a collaborative initiative. Upon the identification of an event, the goal of the Event Analysis Program is to:

- identify what transpired;
- categorize the event within the NERC Event Analysis Program;

[50] In support of ERO Goal 4.b. Events and system performance are consistently analyzed for sequence, cause, and remediation to identify reliability risks and trends and lessons learned.

- establish the sequence of events;
- understand the essential root causes of the event;
- identify recommendations or corrective actions; and
- develop and disseminate to the industry, lessons to be learned so that the operational reliability of the bulk power system can be further enhanced.

In assessing any system event, it is recognized that, if the timely dissemination of lessons learned from an event or disturbance is to be realized, any potential compliance implications associated with an event must be addressed and dismissed. Throughout an event analysis effort, to make this process successful and complete, and to solidify the "bottom-up" approach, registered entities are encouraged to establish a liaison between the event analysis and compliance functions internal to the registered entity during the event analysis process. This serves to facilitate the development of a registered entity compliance self-assessment report which will perform a sufficiency review of the reliability standards deemed applicable to the event, assisting in the self-reporting of possible violations should any be discovered.

To complete this effort, the entity, the Region and NERC staff collaborate to assess the NERC Event Analysis Report and perform a formal cause code analysis, identifying a root cause and complementing any lessons learned gathered from the disturbance.

The adoption by NERC of the Event Analysis Program brings clarity and certainty about what system events are relevant to analyze and to what level of detail, targeting potential vulnerabilities to the reliability of the bulk power system for detailed and in depth analysis; only concise and succinct reviews are desired for more minor events. It also delineates the expectations of roles and responsibilities of the registered entities, NPCC and NERC in a uniform review of system disturbances by the industry, and, ultimately, the program promotes the timely development and dissemination of valuable lessons learned to the industry. The identification and tracking of emerging common elements in system events will further distinguish trends which may be of concern to reliability. By rigorously pursuing the lesser events on the system and learning from these disturbances, the larger event can be avoided or mitigated.

NPCC Staff works step-by-step with the registered entity in the total event analysis process, permitting the entity to assume the primary role in the initial analysis, the development of lessons learned which may benefit the industry and the Standards sufficiency review.

NERC Alert Process[51]

NPCC Staff works with the registered entities to appropriately respond to the NERC Alert system, a process through which notifications of potential threats to electric reliability are disseminated to the industry with the expectations placed on the entity proportional to the severity of the Alert being issued.

NPCC Staff is also working closely with the NERC Staff to incorporate greater efficiencies, industry input and precision into the NERC proposal for a more streamlined NERC Alert process which can disseminate critical information to the appropriate Subject Matter Expert within the organization who can promptly act on the alert.

[51] In support of ERO Goal 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

Operational Status[52]

On an ongoing, but non-real time basis, NPCC monitors the operational status of the bulk power system and coordinates normal and pre-emergency communication, awareness and assistance in addition to the same during an emergency among the Reliability Coordinators within NPCC and its neighboring RCs: the New Brunswick Power Corporation, Hydro-Québec TransÉnergie, the ISO New England, Inc., the New York ISO and the Independent Electricity System Operator in Ontario. The industry is notified of significant bulk power system events that have occurred in one Reliability Coordinator Area, and which have the potential to impact reliability in other NPCC Reliability Coordinator Areas or Regions external to NPCC. These events include contingencies on the bulk power system, potential shortfalls of operating reserve, operating problems, potential security threats and potential threats or disruptions to the cyber systems.

The "NPCC Emergency Preparedness Conference Call Procedures" provide a mechanism that enables the Reliability Coordinator in NPCC, and, as circumstances may require, their counterparts in neighboring Regions, to rapidly communicate the status of current operating conditions, to facilitate the procurement of assistance during emergency conditions and to identify potential physical or cyber threats to the system.

Items of particular concern that can be discussed during the calls may include, but are not limited to, the following: anticipated weather conditions critical to the system or systems experiencing or projecting resource deficiencies; load forecast; largest first and second contingencies; potential need for emergency transfers; operating reserve requirements and expected available operating reserve capacity deficiencies; potential fuel shortages or potential fuel supply disruptions which could lead to energy shortfalls; identified or projected voltage conditions; status of short term transactions; additional capability available within four hours and additional capability available within twelve hours; generator outages; significant transmission outages; expected transfer limits and limiting elements; anticipated implementation of NERC Transmission Loading Relief (TLR); changes in the status of relay protection systems; arming of special protection systems not normally armed; and/or the application of abnormal operating procedures.

NPCC has also established a daily conference call to serve as a complement to the NPCC Emergency Preparedness Conference Call. The participants of the call are the Reliability Coordinators within NPCC and its neighboring RCs, the Midwest ISO and PJM. The conference call is implemented through a bridge, the initiation of the call quickly ringing all pre-selected telephones simultaneously. The goal of the call is to alert all Reliability Coordinators of emerging problems. If no system difficulties are anticipated for the day, no unnecessary information is to be discussed. Subjects for discussion are limited to credible events which could impact the ability of an entity to serve its load and meet its operating reserve obligations or would impose a burden to the interconnection, including the following: Projected Load; Adverse Weather; Operating Reserve; Generation; Transmission; and Sabotage. If conditions worsen in the course of the day, the NPCC Emergency Preparedness Conference Call will be implemented.

NPCC monitors the status of the bulk power system through the NERC Situational Awareness-FERC, NERC, Regions (SAFNR) initiative, a near real-time operating display for the United States portion of the Reliability Coordinators footprints of North America. Transmission voltage

[52] In support of ERO Goal 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

levels of 230 kV and above are displayed, and the tool provides the ability to "drill down" to detailed bus information.

To ensure the capability for continued voice communications among NPCC and its Reliability Coordinators, a satellite telephone network was also established, and it is tested on a monthly basis. This back-up communications system will function in the event of a collapse of the Public Switched Telephone Network (PSTN), and cross-border voice communications can still be maintained among the Canadian Reliability Coordinators of NPCC and the Reliability Coordinators in the United States.

Critical Infrastructure Objectives

NPCC's critical infrastructure objectives are defined within the scope of the NPCC Task Force on Infrastructure Security & Technology, (TFIST) and include, but are not confined to:

- Providing a forum for NPCC review of proposed and posted documents from the NERC Critical Infrastructure Protection Committee (CIPC)
- Representing and advocating NPCC's position in the activities of NERC groups involved in the development and/or implementation of physical and cyber security

NPCC's 2015 critical infrastructure goals and objectives, as identified by the 2014-2015 Work Plan of the Task Force on Infrastructure Security and Technology include, but are not confined to:

- Oversee the implementation of version 5 of the CIP Standards
- Monitor the Homeland Security Information Network (HSIN), ES-ISAC, Critical Information Protection Information Sharing (CIPIS), NERC Alerts and Canadian Information Sharing and share information with CO-8[53]
- Coordinate Cyber Protection activities, discussions and hold workshops as may be required to maintain Cyber Security of BES Cyber Assets.[54]
- Provide continued support and participation in NERC's Critical Infrastructure Protection Committee (CIPC)[55]
- Review and submit comments on NERC proposed Reliability Standards, modified Reliability Standards, proposed Guidelines and modified Guidelines related to Infrastructure Security and Technology
- Keep current on all governmental agencies regarding applicable security recommendations and requirements, and other applicable security and reliability recommendations and keep the RCC and its committees appropriately informed, e.g. Sector Specific Plan.
- Develop and maintain levels of expertise in those areas of concern to the task force through activities such as periodic workshop presentations, seminars, and meetings, open to the general NPCC membership[56].
- Regarding the Cross Border Emergency Telecommunications recommendation
    - Continue to annually report to RCC on this testing

[53] In support of ERO Goal 5.b. Issue and track security recommendations to protect the bulk power system (related to 5.a.ii.)

[54] In support of ERO Goal 1. b. Facilitate smooth transition of new standards (e.g., CIP Version 5); and ERO Goal 3.a. Initiate compliance phase-in learning periods for new standards

[55] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[56] In support of ERO Goal 5.b. Expand the use and value of security threat and vulnerability information sharing, analytics, and analysis

    - Continue to support CO-8's monthly testing
- Assess the telecommunications industry's desire to convert Frame Relay customers to Multiprotocol Label Switching (MPLS) and potentially provide recommendations to RCC

System Operations Security Objectives

NPCC's system operations security objectives are defined within the scope of the NPCC Task Force on Coordination of Operation (TFCO) and include, but are not confined to:

- Coordinating inter-Regional pre-emergency actions in the event of a threat to the security of the Northeastern North American bulk power supply system[57]
- Assisting in the development of real time operating tools assuring cyber security concerns are addressed[58]

NPCC's 2015 operational situation awareness goals and objectives, as identified by the 2014-2015 Work Plan of the NPCC Task Force on Coordination of Operation (TFCO) include, but are not confined to:

- Continue to monitor the reliable implementation of version 5 of the Cyber Standards.[59]
- Work directly with applicable NPCC Task Forces to provide an in depth assessment of Lessons Learned unique to the NPCC members and NPCC criteria.

2015 Key Assumptions

- The monitoring of Lessons Learned will be a major focus of NERC in 2015.
- Critical infrastructure protection will fully integrate the requirements of version 5 of the Cyber Standards in 2015.

2015 Goals and Key Deliverables

- Continue to monitor the reliable implementation of version 5 of the Cyber Standards.
- Work directly with applicable NPCC Task Forces to provide an in depth assessment of Lessons Learned unique to the NPCC members and NPCC criteria.
- Establish a unique NPCC Event Analysis web site to post NPCC Lessons Learned.
- Contribute to the reduction of Category 3 events and no Category 4 or 5 events in NPCC- by disseminating to the RCC compiled information on NPCC Region specific, as well as industry wide, event related causal analysis and analysis of Lessons Learned.[60]

Based on the portion of professional/technical staff time and other resources devoted to situation awareness and infrastructure security, NPCC estimates that it will expend 10 percent of its resources on this activity.

[57] In support of ERO Goal 5.b.Issue and track security recommendations to protect the bulk power system (related to 5.a.ii.)

[58] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[59] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[60] In support of ERO Goal 4.b. Provide lessons learned and recommendations from events and identified risks

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense relects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.
- Consultants and contracts expense increase in support of NPCC's efforts to assess and improve system frequency and generator governor response.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Situation Awareness and Infrastructure Security Program

Funding sources and related expenses for the situation awareness and infrastructure security section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Situation Awareness and Infrastructure Security

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 1,447,636	$ 1,447,636	$ -	$ 1,471,074	$ 23,438
Penalty Sanctions	16,475	16,475	-	30,258	13,783
Total ERO Funding	**$ 1,464,111**	**$ 1,464,111**	**$ -**	**$ 1,501,332**	**$ 37,221**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 1,464,111**	**$ 1,464,111**	**$ -**	**$ 1,501,332**	**$ 37,221**
Expenses					
Personnel Expenses					
Salaries	$ 522,672	$ 522,672	$ -	$ 541,258	$ 18,586
Payroll Taxes	32,961	32,961	-	32,811	(150)
Benefits	88,851	88,851	-	80,801	(8,049)
Retirement Costs	117,586	117,586	-	107,819	(9,767)
Total Personnel Expenses	**$ 762,070**	**$ 762,070**	**$ -**	**$ 762,689**	**$ 619**
Meeting Expenses					
Meetings	$ 25,000	$ 25,000	$ -	$ 15,000	$ (10,000)
Travel	60,000	60,000	-	60,000	-
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 85,000**	**$ 85,000**	**$ -**	**$ 75,000**	**$ (10,000)**
Operating Expenses					
Consultants & Contracts	$ 75,000	$ 75,000	$ -	$ 100,000	$ 25,000
Office Rent	-	-	-	-	-
Office Costs	-	-	-	-	-
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 75,000**	**$ 75,000**	**$ -**	**$ 100,000**	**$ 25,000**
Total Direct Expenses	**$ 922,070**	**$ 922,070**	**$ -**	**$ 937,689**	**$ 15,619**
Indirect Expenses	**$ 568,962**	**$ 568,962**	**$ -**	**$ 574,629**	**$ 5,667**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 1,491,031**	**$ 1,491,031**	**$ -**	**$ 1,512,318**	**$ 21,286**
Change in Assets	**$ (26,920)**	**$ (26,920)**	**$ -**	**$ (10,986)**	**$ 15,935**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(26,920)	(26,920)	-	(10,986)	15,935
Inc(Dec) in Fixed Assets (C)	**(26,920)**	**(26,920)**	**-**	**(10,986)**	**15,935**
TOTAL BUDGET (=B+C)	1,464,111	1,464,111	-	1,501,332	37,221
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ (0)**

Administrative Services

Administrative Services Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	9.00	9.00	0.00
Total Direct Expenses	$5,689,616	$5,746,287	$56,671
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Less: Other Funding Sources	$0	$0	$0
Total Allocation to Regional Entity Division Programs as Indirect Expenses	($5,283,757)	($5,336,385)	($52,629)
Total Allocation to Criteria Services Division Programs as Indirect Expenses	($405,859)	($409,902)	($4,043)
Funding Requirement for Working Capital and Operating Reserves	($300,126)	($355,161)	($55,035)

Program Scope and Functional Description

Administrative services support the previously identified five program areas of: reliability standards; compliance monitoring and enforcement and organization registration and certification; training, education, and operator certification; reliability assessment and performance analysis; and situation awareness and infrastructure security. Administrative services consist of: technical committees and members' forums; general and administrative; legal and regulatory; information technology; human resources; and finance and accounting.

Methodology for Allocation of Administrative Services Expenses to Programs

NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflect implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Administrative Services

Funding sources and related expenses for the Administrative Services section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures 2014 Budget & Projection, and 2015 Budget ADMINISTRATIVE SERVICES						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ (300,126)	$ (300,126)	$ -	$ (355,161)	$ (55,035)
	Penalty Sanctions	-	-	-	-	-
Total ERO Funding		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
Expenses						
Personnel Expenses						
	Salaries	$ 1,676,735	$ 1,676,735	$ -	$ 1,769,318	$ 92,583
	Payroll Taxes	96,083	96,083	-	97,804	1,722
	Benefits	442,256	442,256	-	402,307	(39,949)
	Retirement Costs	425,270	425,270	-	435,638	10,368
Total Personnel Expenses		**$ 2,640,344**	**$ 2,640,344**	**$ -**	**$ 2,705,068**	**$ 64,724**
Meeting Expenses						
	Meetings	$ 110,000	$ 110,000	$ -	$ 120,000	$ 10,000
	Travel	155,000	155,000	-	155,000	-
	Conference Calls	77,000	77,000	-	45,000	(32,000)
Total Meeting Expenses		**$ 342,000**	**$ 342,000**	**$ -**	**$ 320,000**	**$ (22,000)**
Operating Expenses						
	Consultants & Contracts	$ 150,000	$ 150,000	$ -	$ 124,000	$ (26,000)
	Office Rent	737,272	737,272	-	751,500	14,228
	Office Costs	523,500	523,500	-	578,700	55,200
	Professional Services	966,500	966,500	-	1,025,000	58,500
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	80,000	80,000	-	40,000	(40,000)
	Depreciation	250,000	250,000	-	202,019	(47,981)
Total Operating Expenses		**$ 2,707,272**	**$ 2,707,272**	**$ -**	**$ 2,721,219**	**$ 13,947**
	Total Direct Expenses	**$ 5,689,616**	**$ 5,689,616**	**$ -**	**$ 5,746,287**	**$ 56,671**
Indirect Expenses		**$ (5,689,616)**	**$ (5,689,616)**	**$ -**	**$ (5,746,287)**	**$ (56,671)**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ -**	**$ -**	**$ -**	**$ (0)**	**$ (0)**
Change in Assets		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
Fixed Assets						
	Depreciation	(250,000)	(250,000)	$ -	(202,019)	$ 47,981
	Computer & Software CapEx	-	-	-	100,000	100,000
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	250,000	250,000	-	102,019	(147,981)
Inc(Dec) in Fixed Assets (C)		**-**	**-**	**-**	**-**	**-**
TOTAL BUDGET (=B+C)		-	-	-	(0)	(0)
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**

Technical Committees and Member Forums

Technical Committees and Members Forum Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.50	0.50	0.00
Total Direct Expenses	$75,711	$73,779	($1,932)
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

The success of the NPCC programs depends on the active and direct volunteerism and participation of its members. The stakeholders are the source of expertise in the industry. To promote the reliable and efficient operation of the interconnected bulk power systems in Northeastern North America, NPCC invites high level policy makers from Federal, Provincial and State regulatory and/or governmental authorities and senior executives within NPCC and NERC to identify and discuss emerging issues related to the reliability of the NPCC Region.

2015 Key Assumptions

- NPCC's standing committee and subgroup structure for effective stakeholder involvement will continue in 2015
- NPCC will continue to utilize methods to encourage active involvement in its Regional programs that require less stakeholder travel and face-to-face meetings, as the economy improves in 2015
- NPCC will continue to invest in technology and innovation to allow efficient collaboration on technical issues related to reliability

2015 Goals and Key Deliverables

The 2015 NPCC General Meeting provides an opportunity for NPCC Members to meet high level policy makers from Federal, Provincial and State regulatory and/or governmental authorities and senior NERC and NPCC executives to discuss topics related to the reliable planning and operation of the power system, including consideration of emerging reliability, critical infrastructure and environmental issues.

2015 Public Information Committee Goals and Objectives

The objective of the NPCC Public Information Committee is to highlight and summarize NPCC activities and accomplishments in the past year, disseminate and coordinate the appropriate release of information to the media, respond to related requests for information, and coordinate with related NPCC Area, NERC media and public information activities. Activities anticipated for include, but are not limited to:

- Conducting the Media Event – release of the Summer 2015 NPCC Reliability Assessment

- Participation in NERC Regional communication initiatives:
    - Regional communications teleconferences as required
    - Coordination of Emergency or Blackout communications plans
    - Coordination with other NERC activities as required (i.e., situation awareness, event analysis, reliability assessments, etc.)

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

General and Administrative

General and Administrative Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.50	2.50	0.00
Total Direct Expenses	$3,293,356	$3,209,290	($84,066)
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	($300,126)	($355,161)	($55,035)

Program Scope and Functional Description

The NPCC general and administrative function provides executive management of the corporation, management of NPCC office, and other administrative support programs.

NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Funding Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Legal and Regulatory

Legal and Regulatory Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$621,004	$628,183	$7,179
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC's professional legal services provide counsel to the President and CEO, Board of Directors, Vice President and COO, Treasurer and staff on a wide range of legal and regulatory matters including legislation, corporate law, code of conduct, confidentiality, governance, employment law, tax matters, contract law and other areas affecting NPCC. Regulatory counsel provides legal advice to advance significant corporate policy and strategic planning initiatives and also provides legal support to other program areas on matters arising in connection with the performance of NPCC's delegated functions. Regulatory counsel drafts agreements and pleadings and provides interpretations of relevant statutes, regulations, court opinions, and regulatory decisions of FERC, state agencies and provincial authorities. Outside counsel, as necessary, reviews items filed with the governmental agencies for legal sufficiency, maintains relationships with U.S. and Canadian jurisdictions and provides contract review.

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Information Technology

Information Technology Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.00	3.00	0.00
Total Direct Expenses	$1,037,624	$1,111,674	$74,050
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC's Information Technology services ensure information assets and the environment in which they operate are secure and in conformance to NPCC IT Policies and Procedures. NPCC maintains an offsite backup server for continuity of essential operations in the event that its primary location is unavailable.

2015 Key Assumptions

- Continue to develop and maintain the compliance portal through collaboration with other Regions and NERC (CUG).
- Achieve greater consistency with the other Regions and NERC by participating in the NERC IT Steering Group (ITSG) and deriving the efficiencies and cost savings which may result from the projects of this group.[61]
    - The ERO EMG identifies and prioritizes ERO-wide applications to be developed under a PMO housed at NERC. The NERC IT budget does not supplant the Regional Entities' need for IT expenditures for specific regional projects, but to the extent that agreed-upon ERO Enterprise applications provide greater efficiencies, there should not be any unnecessary, redundant expenditures at the regional level.
- Support the Event Analysis program through continued participation in the tools used for the tracking and analysis of system events.[62]
- Support the Bulk Electric System Exception Process "BEP" to enable and facilitate tracking and processing of exceptions submitted.[63] Maintenance of the BESNET support services such as updates, patching, coordinating issues with NERC.
- Support Cyber Security Reviews done by compliance to provide advisory role during those reviews.

[61] ERO Goal 7.b. Develop test and deploy ERO enterprise applications, platform and database

[62] ERO Goal 6.b. Evaluate event disturbances using phasor measurements and other methods to assess sufficiency of data and models;
ERO Goal 4.b. Provide lessons learned and recommendations from events and identified risks;
ERO Goal 4.b. Merge event driven databases and cause codes into one (e.g., event analysis, TADS, GADS, relay mis-operations)

[63] ERO Goal 2.a. Develop and implement BES exception process.

2015 Goals and Key Deliverables

Responsibilities encompass a variety of complex technical, administrative, and supervisory work in the development, installation, and maintenance of information technology systems. IT goals include, but are not limited to:

- Create an information security program and environment aimed at reducing breach of security risks
- Determine long-term software and systems needs and hardware acquisitions
- Develop and implement information security standards and procedures
- Ensure all information systems are functional and secure, and that all applications running on those systems meet business requirements for performance, availability, and security
- Plan and implement organization-wide information systems, services, and network facilities, including local area networks, wide-area networks, and peripheral systems
- Provide outreach and education to NPCC members in IT best practices
- Continually improve Disaster Recovery policies and practices to ensure continuity of service

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Human Resources

Human Resources Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$178,931	$183,817	$4,886
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC has assembled an exceptional team of highly qualified employees to carry out the activities of NPCC. The human resources function, in adherence with applicable federal and state laws, designs, plans, and implements human resources policies and procedures, including staffing, compensation, benefits, employee relations, and training and development.

An enhanced employee time tracking system was implemented in 2013 based on FERC audit recommendations. Employee time tracking and reporting is also handled by the human resources program area.

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Accounting and Finance

Accounting and Finance Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$482,991	$494,544	$11,554
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

The accounting and finance function directs the overall financial plans and accounting practices of the organization; oversees treasury, accounting, budget, tax, and audit activities; and oversees financial and accounting system controls and standards. NPCC uses a CPA firm to prepare its unaudited statements of activities and financial statements for quarterly reviews. Independent audits have identified this system as a best practice.

2015 Goals and Key Deliverables

The objectives are to provide or obtain the financial and accounting services for NPCC and coordinate with NERC requirements:

- Utilize the NERC System of Accounts for consistency
- Utilize an accrual method of accounting for consistency with NERC in methodology
- Cash Management
- Budget Development using the NERC budget template formats
- Forecasts and Projections
- Alignment of NPCC Committees, Task Forces and Working Groups with the programs
- Payroll and expense administration
- Preparation of unaudited Quarterly Financial Statements
- IRS Reporting
- Annual Independent Audit initiated by the Regional Entity

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Regional Entity Assessment Analysis

In the area of assessments there are distinct funding mechanisms as outlined in the following table. For the Regional Entity division, the North American Electric Reliability Corporation (NERC) will assess load serving entities (LSEs) or their designees (within NPCC the designees are the Balancing Authority Areas (BAAs) for New York, New England, New Brunswick, Nova Scotia, Ontario and Québec) based upon 2013 proportional Net Energy for Load (NEL) and other specific program area funding arrangements and make quarterly remittances to the Regional Entity on or about the 15th day of January, April, July and October. For funding associated with the criteria services division, the Independent System Operators/Balancing Authority Areas (ISO/BAAs) will be assessed by NPCC for their proportional share of the divisional budget based upon 2012 NEL within the Region. Non ISO/BAA Full Members will be assessed no membership fee.

NPCC Cost Allocation Methodology

The accompanying table provides information regarding cost allocation for both the Regional Entity division and the criteria services division of NPCC, including the details associated with the funding of the Compliance Program within the RE division. For purposes of determining assessments to support NPCC's resource requirements, costs are allocated among the BAAs within NPCC as the designees for the load-serving-entities in New York, New England, Ontario, Québec, New Brunswick and Nova Scotia (Column A-1).

In order to reflect and respect the international membership and nature of NPCC, the compliance responsibilities and authorities within the U.S., and the specific compliance responsibilities within each of the Canadian provinces within NPCC, the attendant costs of portions of the compliance program differ among the areas within the Regional Entity. Within the U.S. portion of NPCC all costs attributable to delegated (statutory) functions performed by NPCC, including all compliance functions, are assessed based on a NEL allocation. Within the Canadian portion of NPCC those costs attributable to compliance functions performed by NPCC on behalf of provincial governmental and/or regulatory authorities are allocated consistent with the unique Memoranda of Understanding or Agreements that have been entered into for those provinces. To address these different compliance regimes, NPCC developed a composite cost allocation methodology that allocates compliance costs on a fair and equitable basis within the Regional Entity.

As an initial step of that methodology, the NEL for each of the BAAs and their relative percentage to the NPCC total NEL is calculated for the most recent year for which data is available, the second previous year (Columns B-1 and C-1, respectively). In order to establish the RE division funding requirements for each balancing authority area on a NEL basis for all programs except for compliance (Column F-1), the proposed expenses and fixed assets of all other programs are calculated (Column D-1) and the adjustment for the RE division cash reserve requirement is identified (Column E-1). Any penalty monies received from NPCC registered entities within the U.S. prior to June 30th of the year preceding the business plan and budget year are then allocated among the NPCC program areas based on their FTE ratio and between the U.S. BAAs based on their relative NELs (Columns B-1a., C-1a. and G-1, respectively). Consistent with each of the Canadian provincial MOUs and agreements, all penalty monies resulting from compliance actions within Canada, if any, would remain within the applicable province. The total budgeted fees for NPCC workshop participation are indicated as a credit

(Column H-1), with the resultant addition being the RE division assessment, without the compliance program costs, calculated on a NEL basis (Column I-1).

In accordance with the *NPCC Amended and Restated Bylaws* the CS division proposed expenses and fixed assets of all programs are calculated (Column J-1) and the adjustment for the CS division cash reserve requirement is identified (Column K-1), with the resultant addition being the CS division funding requirement and assessment, calculated on a NEL basis (Column L-1).

For costs associated with the RE division compliance program, NPCC's allocation methodology apportions X% of the costs for the program, attributed to CORC Fundamentals (CF), between the BAAs in the United States and Canada on a NEL basis (Column B-2).

Audits and Investigations (AI) related costs, representing X% of the costs of the compliance program, are allocated between U.S. and Canadian BAAs in NPCC, and among the Canadian provinces, using an audit-based methodology (Columns C-2a., C-2c., and D-2b., respectively). The audit-based methodology incorporates relative costs based on categories of compliance audits which are reflective of their size and complexity, as well as the differing compliance program implementation models that are utilized in NPCC due to the international nature of the Regional Entity. The portion allocated to the U.S. BAAs in NPCC is calculated using the audit-based methodology, and this amount is then re-allocated between the New York and New England BAAs based on their relative NEL (Columns C-2b. and D-2a.).

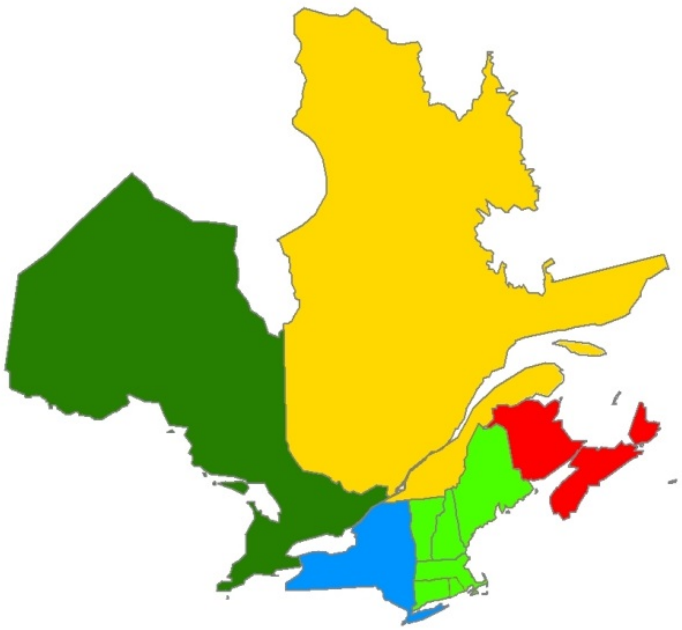
The remaining X% of the costs of the compliance program represent Mitigation and Enforcement (ME) related costs and are allocated between U.S. and Canadian BAAs in NPCC, and among the Canadian provinces, using an enforcement activity based methodology, (Columns E-2a., E-2c., and F-2b., respectively). Based on historical data, NPCC reviewed each BAAs percentage of violations, mitigation plans and settlement agreements to determine each BAAs total average percentage of enforcement activities. The portion allocated to the U.S. BAAs in NPCC is calculated using the enforcement activity based methodology, and this amount is then re-allocated between the New York and New England BAAs based on their relative NEL (Columns E-2b. and F-2a.).

Any penalty monies received from NPCC registered entities within the U.S. by June 30th of the year preceding the business plan and budget year are then allocated among the NPCC program areas based on their FTE ratio and between the U.S. BAAs based on their relative NELs, and then added to the total compliance program expenses and fixed assets to yield a total compliance program assessment (Columns C-1a., H-2, G-2 and I-2, respectively).

Finally, the total RE division funding requirements and assessments by BAA are tabulated and the total funding requirements and assessments for NPCC, both the RE and CS divisions, are combined (Column M).

Table to be Inserted

Section B – Supplemental Financial Information
2015 Business Plan and Budget



Section B — Supplemental Financial Information

Reserve Balance

Table B-1 – Reserve Balance

Working Capital and Operating Reserve Analysis 2014-2015
REGIONAL ENTITY DIVISION

	Total Reserve	Operating Reserve	Working Capital
Beginning Total Reserve, December 31, 2013	**5,245,194**	4,013,698	1,231,496
Plus: 2014 ERO Funding (from LSEs or designees)	13,611,880	13,611,880	0
Plus: 2014 Other funding sources	217,000	217,000	0
Less: 2014 Projected expenses & capital expenditures	(14,129,006)	(14,129,006)	0
Projected Total Reserve, December 31, 2014	**4,945,068**	**3,713,572**	**1,231,496**
Desired Total Reserve, December 31, 2015 [1]	**4,589,907**	3,358,411 [2]	1,231,496 [3]
31.06% of Total Regional Entity Budget of $14,778,539			
Less: Projected Working Capital and Operating Reserve, December 31, 2014	(4,945,068)	(3,713,572)	(1,231,496)
Increase(decrease) in assessments to achieve desired Total Reserve	**(355,161)**	(355,161)	0

2015 Expenses and Capital Expenditures	14,778,539
Less: Penalty Sanctions [4]	(281,000)
Less: Other Funding Sources	(64,000)
Adjustment to achieve desired Total Reserve balance	(355,161)
2015 Assessment	**14,078,378**

[1] Total Reserve within a range of 16.67% - 33.33% of Budget.
[2] Operating Reserve within a range from 8.33% to 25.00% of Budget. $3,358,411 represents 22.72% of the 2015 budget of $14,778,539
[3] Working Capital equal to 8.33% of Budget. $1,231,496 represents 8.33% of the 2015 budget of $14,778,539
[4] Represents collections prior to June 30, 2014.

Explanation of Changes in Reserve Policy from Prior Year

On October 29, 2013 NPCC's Board of Directors approved management's proposed Working Capital and Operating Reserve Policy. The policy calls for a range between 8.33% (30 days) and 25.00% (90 days) rather than the specific required level of Operating Reserves of 8.33%. This range will allow for more stability in Assessments. The Working Capital required balance remains unchanged at 8.33% (30 days).

Breakdown by Statement of Activity Sections

The following detailed schedules are in support of the Regional Entity division Statement of Activities on page 13 of the 2015 Business Plan and Budget. All significant variances have been disclosed by program area in the preceding pages.

Penalty Sanctions

U.S. penalty monies received prior to June 30, 2014 are to be used to offset assessments in the 2015 Budget, as documented in the NERC Policy – Accounting, Financial Statement, and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standard. Penalty monies received from July 1, 2014 through June 30, 2015 will be used to offset U.S. load serving entity designee assessments in the 2016 Budget.

All penalties received prior to June 30, 2014 are detailed below, including date received and the penalty amount.

Allocation Method: U.S. penalty sanctions received have been allocated to the following Regional Entity division programs to reduce assessments: Reliability Standards; Compliance Monitoring & Enforcement and Organization Registration & Certification; Reliability Assessments and Performance Analysis; Training, Education and Operator Certification; and Situation Awareness and Infrastructure Security. U.S. penalty sanctions are allocated based upon the number of FTEs in the Program divided by the aggregate total FTEs in the Programs receiving the allocation.

Table B-2 – Penalty Sanctions

Penalty Sanctions Received Prior to June 30, 2014	Date Received	Amount Received
Penalty Payment 1	7/5/2013	$ 50,000.00
Penalty Payment 2	7/5/2013	$ 10,000.00
Penalty Payment 3	7/5/2013	$ 30,000.00
Penalty Payment 4	7/5/2013	$ 25,000.00
Penalty Payment 5	9/4/2013	$ 7,000.00
Penalty Payment 6	10/16/2013	$ 25,000.00
Penalty Payment 7	11/1/2013	$ 5,000.00
Penalty Payment 8	1/8/2014	$ 25,000.00
Penalty Payment 9	3/6/2014	$ 14,000.00
Penalty Payment 10	4/30/2014	$ 90,000.00
Total Penalties Received		**$ 281,000.00**

Table B-3 – Supplemental Funding

Outside Funding Breakdown By Program (excluding ERO Assessments & Penalty Sanctions)	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget
Reliability Standards				
Total	$ -	$ -	$ -	$ -
Compliance Monitoring, Enforcement & Org. Registration				
	$ -	$ -	$ -	$ -
	-	-	-	-
Total	$ -	$ -	$ -	$ -
Reliability Assessment and Performance Analysis				
	$ -	$ -	$ -	$ -
	-	-	-	-
Total	$ -	$ -	$ -	$ -
Training and Education				
Workshops	$ 64,000	$ 64,000	$ 64,000	$ -
Total	$ 64,000	$ 64,000	$ 64,000	$ -
Situation Awareness and Infrastructure Security				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Technical Committees and Member Forums				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Administrative Services Programs				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Total Outside Funding	$ 64,000	$ 64,000	$ 64,000	$ -

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- NPCC assumed no interest income because of continuing low market interest rates.

Table B-4 – Personnel Expenses

Personnel Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Salaries					
Salary	$ 5,886,227	$ 5,886,227	$ 6,175,425	$ 289,198	4.9%
Employment Agency Fees	$ 15,000	$ 15,000	$ 10,000	$ (5,000)	-33.3%
Temporary Office Services	$ 10,000	$ 10,000	$ 10,000	$ -	0.0%
Total Salaries	$ 5,911,227	$ 5,911,227	$ 6,195,425	$ 284,198	4.8%
Total Payroll Taxes	$ 384,311	$ 384,311	$ 387,209	$ 2,898	0.8%
Benefits					
Education Reimbursement	$ -	$ -	$ 10,000	$ 10,000	-
Training and Seminars	$ 36,123	$ 36,123	$ 36,123	$ -	0.0%
Medical Insurance	$ 915,306	$ 915,306	$ 720,337	$ (194,969)	-21.3%
Life-LTD-STD Insurance	$ 63,552	$ 63,552	$ 64,366	$ 815	1.3%
Worker's Compensation	$ 14,700	$ 14,700	$ 14,700	$ -	0.0%
Vacation	$ 400,580	$ 400,580	$ 410,868	$ 10,288	2.6%
Relocation	$ -	$ -	$ -	$ -	-
Total Benefits	$ 1,430,261	$ 1,430,261	$ 1,256,395	$ (173,866)	-12.2%
Retirement					
Pension Contribution	$ 590,892	$ 590,892	$ 353,723	$ (237,169)	-40.1%
Employee Savings Plan	$ 478,469	$ 478,469	$ 644,290	$ 165,821	34.7%
Savings Admin	$ 32,000	$ 32,000	$ 32,000	$ -	0.0%
Deferred Compensation	$ 23,000	$ 23,000	$ 60,000	$ 37,000	160.9%
Total Retirement	$ 1,124,361	$ 1,124,361	$ 1,090,013	$ (34,348)	-3.1%
Total Personnel Costs	**$ 8,850,160**	**$ 8,850,160**	**$ 8,929,041**	**$ 78,881**	**0.9%**
FTEs	36.86	36.86	36.86	-	0.0%
Cost per FTE					
Salaries	$ 160,370	$ 160,370	$ 168,080	$ 7,710	4.8%
Payroll Taxes	$ 10,426	$ 10,426	$ 10,505	$ 79	0.8%
Benefits	$ 38,803	$ 38,803	$ 34,086	$ (4,717)	-12.2%
Retirement	$ 30,504	$ 30,504	$ 29,572	$ (932)	-3.1%
Total Cost per FTE	**$ 240,102**	**$ 240,102**	**$ 242,242**	**$ 2,140**	**0.9%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- The increase in Salaries reflects an overall general wage increase of 3%, at risk (variable incentives) compensation at less than 100% of program levels, and implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Pension contribution decreased while employee savings plan increased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.
- The decrease in Employment Agency Fee is due to no planned staff additions in 2015. Agencies would be used only to fill positions vacated during the year.
- A 2% vacancy factor is assumed based on historical vacancy trends.

Table B-5 – Consultants and Contracts

Consultants	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Consultants					
Reliability Standards	$ -	$ -	$ -	$ -	-
Compliance Enforcement and Organization Registration and Certification	$ 10,000	$ 10,000	$ 15,000	$ 5,000	50.0%
Reliability Assessment and Performance Analysis	$ -	$ -	$ -	$ -	-
Training and Education	$ -	$ -	$ -	$ -	-
Situation Awareness and Infrastructure Security	$ -	$ -	$ -	$ -	-
Member Forums	$ -	$ -	$ -	$ -	-
General and Administrative	$ 50,000	$ 50,000	$ 35,000	$ (15,000)	-30.0%
Legal and Regulatory	$ -	$ -	$ -	$ -	-
Information Technology	$ -	$ -	$ -	$ -	-
Human Resources	$ -	$ -	$ -	$ -	-
Accounting and Finance	$ -	$ -	$ -	$ -	-
Consultants Total	**$ 60,000**	**$ 60,000**	**$ 50,000**	**$ (10,000)**	**-16.7%**

Contracts	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards	$ 30,000	$ 30,000	$ 25,000	$ (5,000)	-16.7%
Compliance Enforcement and Organization Registration and Certification	$ 1,384,433	$ 1,384,433	$ 1,713,000	$ 328,567	23.7%
Reliability Assessment and Performance Analysis	$ 275,000	$ 275,000	$ 365,000	$ 90,000	32.7%
Training and Education	$ -	$ -	$ -	$ -	-
Situation Awareness and Infrastructure Security	$ 75,000	$ 75,000	$ 100,000	$ 25,000	33.3%
Member Forums	$ -	$ -	$ -	$ -	-
General and Administrative	$ 90,000	$ 90,000	$ 82,000	$ (8,000)	-8.9%
Legal and Regulatory	$ -	$ -	$ -	$ -	-
Information Technology	$ -	$ -	$ -	$ -	-
Human Resources	$ -	$ -	$ -	$ -	-
Accounting and Finance	$ 10,000	$ 10,000	$ 7,000	$ (3,000)	-30.0%
Contracts Total	**$ 1,864,433**	**$ 1,864,433**	**$ 2,292,000**	**$ 427,567**	**22.9%**
Total Consultants and Contracts	**$ 1,924,433**	**$ 1,924,433**	**$ 2,342,000**	**$ 417,567**	**21.7%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- Compliance Enforcement and Organization Registration and Certification consultant and contractor costs increased due to increased workload related to the initial implementation of the RAI, incorporating Risk Assessment and Internal Control assessment. Without this one time ramp up in RAI endeavors for 2015, contractor costs would have remained relatively flat. These joint ERO Enterprise initiatives are intended to benefit the registered entities, Regional Entities and NERC. With a risk and performance based assessment of each registered entity, audits will transition to a periodicity more reflective of the risk profile of the entity such that some audits will be more in-depth while others may have a reduced scope which will require less independent contractor resources.

- Reliability Assessment and Performance Analysis contracts expense increase is related to implementation of the revised BES definition.

Table B-6 – Office Rent

Office Rent	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Office Rent	$ 654,772	$ 654,772	$ 645,000	$ (9,772)	-1.5%
Utilities	$ 35,000	$ 35,000	$ 40,000	$ 5,000	14.3%
Maintenance	$ 15,000	$ 15,000	$ 22,000	$ 7,000	46.7%
Security	$ 2,500	$ 2,500	$ 2,500	$ -	0.0%
Real Estate Taxes	$ 30,000	$ 30,000	$ 42,000	$ 12,000	40.0%
Total Office Rent	**$ 737,273**	**$ 737,273**	**$ 751,501**	**$ 14,228**	**1.9%**

Table B-7 – Office Costs

Office Costs	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Telephone	$ 110,000	$ 110,000	$ 110,000	$ -	0.0%
Internet Expense	$ 80,000	$ 80,000	$ 80,000	$ -	0.0%
Office Supplies	$ 35,000	$ 35,000	$ 36,000	$ 1,000	2.9%
Computer Supplies and Maintenance	$ 213,000	$ 213,000	$ 260,000	$ 47,000	22.1%
Subscriptions & Publications	$ 13,000	$ 13,000	$ 13,500	$ 500	3.8%
Dues	$ 4,000	$ 4,000	$ 4,000	$ -	0.0%
Postage	$ 1,500	$ 1,500	$ 1,200	$ (300)	-20.0%
Express Shipping	$ 10,000	$ 10,000	$ 10,000	$ -	0.0%
Copying	$ 25,000	$ 25,000	$ 25,000	$ -	0.0%
Reports	$ -	$ -	$ 5,000	$ 5,000	-
Stationary and Office Forms	$ 5,000	$ 5,000	$ 3,000	$ (2,000)	-40.0%
Equipment Repair/Service Contracts	$ 10,000	$ 10,000	$ 8,000	$ (2,000)	-20.0%
Bank Charges	$ 30,000	$ 30,000	$ 23,000	$ (7,000)	-23.3%
Sales and Use Tax	$ -	$ -	$ -	$ -	-
Merchant Credit Card Fees	$ -	$ -	$ -	$ -	-
Presentation and Publicity	$ -	$ -	$ -	$ -	-
Total Office Costs	**$ 536,500**	**$ 536,499**	**$ 578,700**	**$ 42,200**	**7.9%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- Computer Supplies and Maintenance expense is based on contracts currently in place and historical actual expense.

Table B-8 - Professional Services

Professional Services	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
BOT Fee	$ 280,000	$ 280,000	$ 325,000	$ 45,000	16.1%
BOT Search Fee	$ -	$ -	$ -	$ -	-
Legal - Reorganization	$ -	$ -	$ -	$ -	-
Accounting & Auditing Fees	$ 300,000	$ 300,000	$ 310,000	$ 10,000	3.3%
Legal Fees - Other	$ 350,000	$ 350,000	$ 350,000	$ -	0.0%
Insurance - Commercial	$ 36,500	$ 36,500	$ 40,000	$ 3,500	9.6%
Total Services	**$ 966,500**	**$ 966,501**	**$ 1,025,000**	**$ 58,500**	**6.1%**

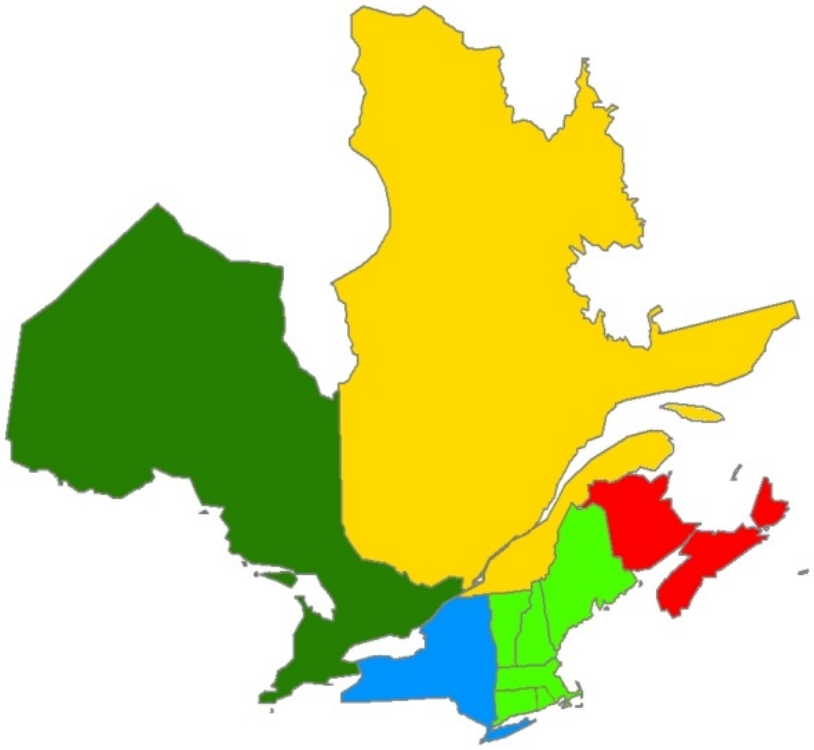
Table B-9 – Other Non-Operating Expenses

Other Non-Operating Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Interest Expense	$ -	$ -	$ -	$ -	-
Office Relocation	$ -	$ -	$ -	$ -	-
Total Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**-**

Table B-10 – 2016 and 2017 Projections

Table to be Inserted

Section C – Criteria Services Division Activities
2015 Business Plan and Budget



Section C —2014 Criteria Services Division Business Plan and Budget

Criteria Services Division (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.14	2.14	0.00
Total Direct Expenses	$683,240	$729,550	$46,310
Total Indirect Expenses	$405,859	$409,902	$4,043
Other Non-Operating Expenses	$0	$0	$0
Working Capital and Operating Reserves Requirement	($75,391)	($94,220)	($18,829)
Inc(Dec) in Fixed Assets	($24,000)	($10,011)	$13,989
Funding Requirement	$989,708	$1,035,221	$45,513

NPCC Regionally-Specific Criteria Services Background

NPCC Criteria Services division activities are based on the development, maintenance and promulgation of Regionally-specific more stringent criteria as well as criteria establishing resource adequacy requirements within the Region. These criteria contain requirements which are more stringent and more specific than the existing NERC Reliability Standards requirements. These criteria require continual evaluation to ensure they are "not inconsistent with" any NERC reliability standards.

Membership and Governance

Full members are subject to compliance with Regionally-specific criteria, in addition to continent-wide Reliability Standards, and receive criteria-related services from the Criteria Services division.

Full Members, aside from those who perform the Balancing Authority function, are not assessed an annual membership fee. Those that perform Balancing Authority functions are assessed and remit a proportional net energy for load share of expenses for criteria services. NPCC would also directly assign criteria service division costs to a Balancing Authority Area or entity, where significant costs are incurred for that Balancing Authority Area. The funding for NPCC's Criteria Services division is approved by the NPCC Board of Directors.

Criteria Services Division Functional Scope

Through its Criteria Services division, NPCC promotes the reliable and efficient operation of the international, interconnected bulk power systems in Northeastern North America through the establishment of Regionally-specific criteria, and monitoring and enforcement of compliance with such criteria.

NPCC provides Full Members with Regional reliability assurance services, and acts as the vehicle through which States and Provinces can fulfill their political mandates, with respect to resource adequacy, as well as overseeing the Northeastern North American electric infrastructure.

Major 2015 Assumptions and Cost Impacts

The Criteria Services division services are expected to remain stable throughout 2015 when compared to the Regional Entity division.

- The Criteria Compliance Enforcement Program (CCEP) review and evaluation process has matured and been enhanced after its inception in 2012. Criteria Compliance submittals to the CC are done as necessary.
- Past non-compliances, if any, followed the due process stated in the CCEP-1 process document and proper resolution/enforcement action taken.

2015 Primary Goals and Objectives

- Review, maintain, and revise the NPCC Regional Reliability Directories to facilitate compliance assessments and ensure the Criteria portions of the Directories are "not inconsistent" with, nor duplicative with, the approved and effective NERC Standards.
- The criteria services division and CCEP Working Group (reporting to the Compliance Committee) will work with the various Task Forces to develop Criteria Compliance Reporting Forms for additional NPCC Directories to ensure that the more stringent or Regionally-specific criteria is being met.
- The criteria services division and CCEP working group will work with TFCO, TFCP, TFSS, and TFSP to review criteria and measures within each specific NPCC Directory to identify and develop them into specific reporting forms for approval.
- Review impact of Bulk Electric System definition on Directory and Criteria content and compliance reporting.
- Review impact of Sector or NPCC organizational changes on the Directory and Criteria review, enforcement and arbitration processes
- Assist Legal with preparation of revised Directories for Regulatory filings with the individual Provinces in accordance with their respective Memorandum of Understandings (MOUs) as well as the State of New York Public Service Commission
- Facilitate any requested interpretations for NPCC Criteria with the necessary subject matter experts and identify potential opportunities for clarifications of the Criteria.

NPCC Reliability Directory Maintenance and Development

The NPCC Regional Reliability Directories were developed to demonstrate that the NPCC more stringent criteria are not inconsistent with the NERC Reliability Standards as mandated by the NERC Rules of Procedure. The Directory project was also undertaken to remove any redundancies with the NERC Reliability Standards and to clearly delineate the more stringent NPCC criteria requirements. In 2013 the directories were further reviewed and revision of the directories is underway to transition the criteria language into a "requirement type" format. This further revision facilitates the NPCC Region's CCEP and ensures the continued delineation of the more stringent and more specific Regional criteria from the latest approved and effective set of NERC ERO standards.

In 2015, work will proceed with maintenance and revision of the Directories to address any future redundancies with NERC or NPCC Reliability Standards as well as the continued need for additional more stringent or specific NPCC Regional criteria requirements as new NERC Reliability Standards are developed and existing standards are revised. NPCC will continue to rely on contractors for subject matter expertise on an as-needed basis throughout 2015. The amount of Regional documents being converted into Directories and the maintenance of the Directories require subject matter expert input. In addition, changes will be necessary to bring the Phase II Directory project to completion. This project will require significant resources to translate the existing criteria language into "requirements" that are clear, concise and measurable. Also a standards template will be applied to the existing Directories to make them more consistent with the look of the standards. As NERC standards improve, the need for NPCC Directories and amount of criteria contained therein will gradually decrease over time however in the interim, significant review is necessary to ensure the criteria remain "not inconsistent with" the NERC standards as outlined in the NERC Rules of Procedure.

The following Directories will either be under revision or reviewed for further development based on a schedule set forth in the NPCC Reliability Assessment Program:

Operations and Planning Directories

Directory #1, *Basic Criteria for Design and Operation of Interconnected Power Systems*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing NERC TPL, BAL, IRO, INT, MOD, TOP, PRC and VAR standards. The NPCC Task Force on Coordination of Planning will lead a multi-disciplinary working group, consisting of operations and planning subject matter experts to review and revise this directory to reflect the FERC ruling on TPL and other TOP changes.

Directory #2, *Emergency Operations*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing NERC EOP and TOP standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 3, *Maintenance Requirements for BPS Protection*
This Directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain applicable NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 4, *BPS Protection*
This Directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain applicable NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 5, *Operating Reserve Requirements*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing applicable NERC BAL, INT, and IRO standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 7, *Special Protection Systems*
This Directory documents NPCC's Regionally-specific, more stringent criteria for application and approval of SPS. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 8 System Restoration
This Directory documents NPCC's Regionally-specific, more stringent criteria with which each applicable entity must plan for and perform power system restoration following a major or a total blackout, and demonstrates coordination and consistency with applicable NERC EOP standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 9, *Verification of Generator Gross and Net Reactive Power Capability*
This Directory documents NPCC's Regionally-specific, more stringent criteria for verifying the Gross Reactive Power
Capability and Net Reactive Power Capability of generators or generating facilities. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 11, *Disturbance Monitoring*, This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain existing NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision until such time as the NPCC PRC-002-01 Disturbance Monitoring Regional Standard is adopted by FERC and the applicable governmental authorities.

Directory # 12, *UFLS Program*, This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain existing NERC and NPCC developing PRC standard(s). The NPCC Task Force on System Studies will lead this review and revision until such time as the NPCC PRC-006-01 UFLS Regional Standard is approved by the NPCC membership, NERC BOT, the FERC and all the applicable governmental authorities in the Provinces of Canada within NPCC's footprint.

NPCC Criteria Compliance Background

The NPCC criteria services division promotes the reliable operation of the bulk power system through implementation of a comprehensive compliance program. The compliance program that includes monitoring, assessing and enforcing compliance with more stringent, Regionally specific NPCC Criteria requirements, is known as the NPCC Criteria Compliance and Enforcement Program (CCEP) described in process document CCEP-1. This program was developed by the criteria services division and the CCEP Working Group under the purview of the NPCC Compliance Committee. The products of this program support the various Task Forces in their assessments of the NPCC Directories in meeting their goals for the Reliability Coordinating Committee as stated in Section A of this Business Plan.

The more stringent, Regionally-specific NPCC Criteria requirements reflect the unique operational and planning aspects of the bulk power system within the NPCC Region and are included in the NPCC "A" documents and their successors, the NPCC Directories.

NPCC issues non-monetary sanctions to enforce compliance with NPCC Criteria.

- The CCEP program is described in document CCEP-1, *NPCC Criteria Compliance and Enforcement Program (CCEP) Process Document*
- The implementation plan is described in document CCEP-2, *Implementation Plan for 2011 NPCC Criteria Compliance and Enforcement Program*
- On April 5, 2011, the above became effective upon Full Member approval of CCEP-1, and CCEP-2 and retired the following
    - NPCC Criteria A-8, Reliability Compliance and Enforcement Program (RCEP)
    - NPCC Guide B-22, Guidelines for Implementation of the NPCC Inc. Compliance Program
    - NPCC Procedure C-32, Review Process for NPCC Reliability Compliance Enforcement Program
    - Each of the above have been annotated as "retired effective 4/5/11 upon Full Member approval of CCEP-1… and CCEP-2…" on the NPCC public website

The CCEP-1 document

- recognizes the applicability of NPCC's Regionally-specific, more stringent reliability criteria to the Full Members of NPCC, consistent with the *Amended and Restated ByLaws*, and respects the provisions of the several Canadian Memoranda of Understanding in the execution of the processes described
- provides a comprehensive CCEP Process Diagram showing the process of evaluating and approving Criteria Certification submittals, and additional processes and responsibilities in the event that non-compliances, disputes and sanctions arise
- describes the roles and responsibilities of Reporting Members, CC, RCC and Enforcement Panel in the compliance review and enforcement process
- describes Levels of Non-Compliance, associated non-monetary Sanctions, Lateness Policy and the Arbitration/Dispute Resolution process
- addresses Mitigation Plans for any violations under the enforcement process; and
- lists the mandatory Certification Forms to be submitted for review by the Task Forces to ensure compliance with NPCC Directories are being met

The CCEP currently requires annual submittal of Certification Forms by the Reliability Coordinators and Balancing Authorities to confirm compliance with various NPCC Directories. Currently the required Certification forms are for Directory #1- *Area Transmission Review*, Directory #8 - *Key Facility List*, Directory #9 – *Generator Real Power Verification*, Directory #10 - *Verification of Generator Gross and Net Reactive Power Capability*, and Directory #12 - *UFLS Program Requirements*. In 2014 NPCC anticipates expansion of the CCEP to include compliance assessment activities to all active Directories.

The CCEP identifies those specific NPCC Directories that are subject to monitoring, assessment and enforcement. These Directories also are subject to NPCC Criteria Compliance Audits.

The NPCC Compliance Committee (CC) has final approval of compliance assessments related to CCEP. The CCEP describes the roles and responsibilities of committees and panels used to resolve contested compliance and/or sanction or penalty determinations related to NPCC Directories.

Explanation of Significant Variances – 2015 Budget versus 2014 Budget

Personnel Expenses

- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.

2014 Budget and Projection and 2015 Budget Comparisons

Statement of Activities 2014 Budget & Projection, and 2015 Budget CRITERIA SERVICES DIVISION						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ -	$ -	$ -	$ -	$ -
	Penalty Sanctions	-	-	-	-	-
Total ERO Funding		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Membership Dues	989,708	989,708	-	760,033	(229,675)
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 989,708**	**$ 989,708**	**$ -**	**$ 760,033**	**$ (229,675)**
Expenses						
Personnel Expenses						
	Salaries	$ 312,166	$ 312,166	$ -	$ 369,319	$ 57,153
	Payroll Taxes	21,536	21,536	-	22,681	1,145
	Benefits	64,153	64,153	-	76,900	12,747
	Retirement Costs	129,818	129,818	-	145,639	15,821
Total Personnel Expenses		**$ 527,674**	**$ 527,674**	**$ -**	**$ 614,539**	**$ 86,866**
Meeting Expenses						
	Meetings	$ 10,000	$ 10,000	$ -	$ 10,000	$ -
	Travel	63,000	63,000	-	63,000	-
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 73,000**	**$ 73,000**	**$ -**	**$ 73,000**	**$ -**
Operating Expenses						
	Consultants & Contracts	$ 55,000	$ 55,000	$ -	$ 30,000	$ (25,000)
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	3,567	3,567	-	2,000	(1,567)
	Depreciation	24,000	24,000	-	10,011	(13,989)
Total Operating Expenses		**$ 82,567**	**$ 82,567**	**$ -**	**$ 42,011**	**$ (40,556)**
	Total Direct Expenses	**$ 683,240**	**$ 683,240**	**$ -**	**$ 729,550**	**$ 46,310**
Indirect Expenses		**$ 405,859**	**$ -**	**$ -**	**$ 409,902**	**$ 4,043**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 1,089,100**	**$ 1,089,100**	**$ -**	**$ 1,139,452**	**$ 50,353**
Change in Assets		**$ (99,391)**	**$ (99,391)**	**$ -**	**$ (379,419)**	**$ (280,027)**
Fixed Assets						
	Depreciation	$ (24,000)	(24,000)	$ -	$ (10,011)	$ 13,989
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	-	-	-	-	-
Inc(Dec) in Fixed Assets (C)		**(24,000)**	**(24,000)**	**-**	**(10,011)**	**13,989**
TOTAL BUDGET (=B+C)		1,065,100	1,065,100	-	1,129,441	64,342
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (75,391)**	**$ (75,391)**	**$ -**	**$ (369,408)**	**$ (294,016)**

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
CRITERIA SERVICES DIVISION						
Operational Programs						
Reliability Standards	1.07	1.07	1.00	0.07	1.07	0.00
Compliance Enforcement and Organization Registration and Certification	0.00	0.00	0.00	0.00	0.00	0.00
Training and Education	0.00	0.00	0.00	0.00	0.00	0.00
Reliability Assessment and Performance Analysis	1.07	1.07	1.00	0.07	1.07	0.00
Situation Awareness and Infrastructure Security	0.00	0.00	0.00	0.00	0.00	0.00
Total FTEs Operational Programs	**2.14**	**2.14**	**2.00**	**0.14**	**2.14**	**0.00**
Administrative Programs						
Member Forums	0.00	0.00	0.00	0.00	0.00	0.00
General and Administrative	0.00	0.00	0.00	0.00	0.00	0.00
Information Technology	0.00	0.00	0.00	0.00	0.00	0.00
Legal and Regulatory	0.00	0.00	0.00	0.00	0.00	0.00
Human Resources	0.00	0.00	0.00	0.00	0.00	0.00
Accounting and Finance	0.00	0.00	0.00	0.00	0.00	0.00
Total FTEs Administrative Programs	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Total FTEs	**2.14**	**2.14**	**2.00**	**0.14**	**2.14**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

Reserve Analysis 2014-2015

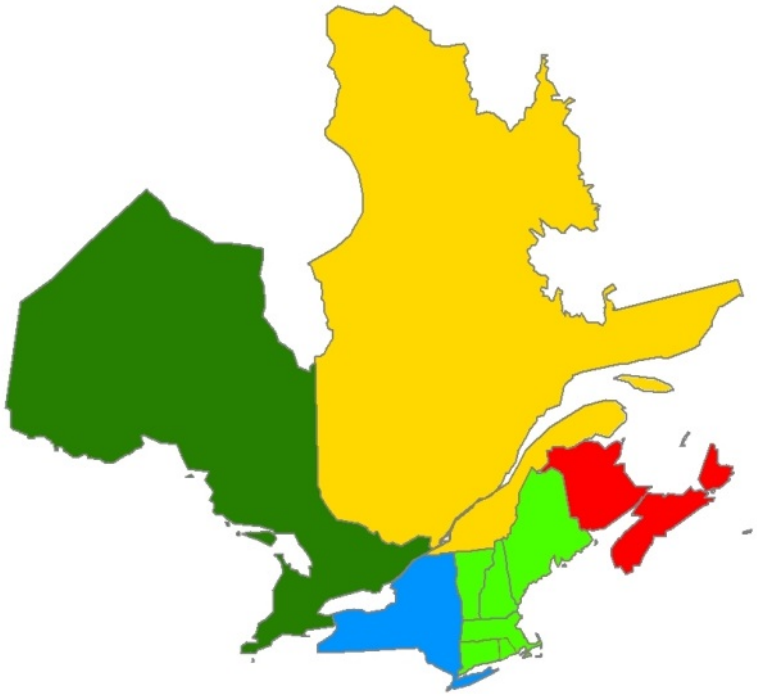
Working Capital and Operating Reserve Analysis 2014-2015			
CRITERIA SERVICES DIVISION			
	Total Reserve	**Operating Reserve**	**Working Capital**
Beginning Working Capital and Operating Reserves, December 31, 2013	816,612	727,857	88,755
2014 Non-Statutory Funding (from members)	989,708	989,708	0
2014 Other funding sources	0	0	0
Less: 2014 Projected expenses & fixed asset additions	(1,065,100)	(1,065,100)	0
Projected Working Capital, December 31, 2014	**741,220**	**652,465**	**88,755**
Desired Working Capital and Operating Reserve, December 31, 2015	**647,000**	552,884	94,116
Less: Projected Working Capital Reserve Balance December 31, 2014	(741,220)	(652,465)	(88,755)
Increase(decrease) in assessments to achieve desired Total Reserve	(94,220)	(99,581)	5,361
2015 Funding requirement for expenses and fixed asset additions	1,129,441		
Adjustment to achieve desired Working Capital and Operating Reserve balance	(94,220)		
2015 Funding and reserve requirement	1,035,221		

Explanation of Changes in Reserve Policy from Prior Year

On October 29, 2013 NPCC's Board of Directors approved management's proposed Working Capital and Operating Reserve Policy. The policy calls for a range between 8.33% (30 days) and 25.00% (90 days) rather than the specific required level of Operating Reserves of 8.33%. This range will allow for more stability in Assessments. The Working Capital required balance remains unchanged at 8.33% (30 days).

Section D – Additional Consolidated Financial Statements

2015 Business Plan and Budget



Section D

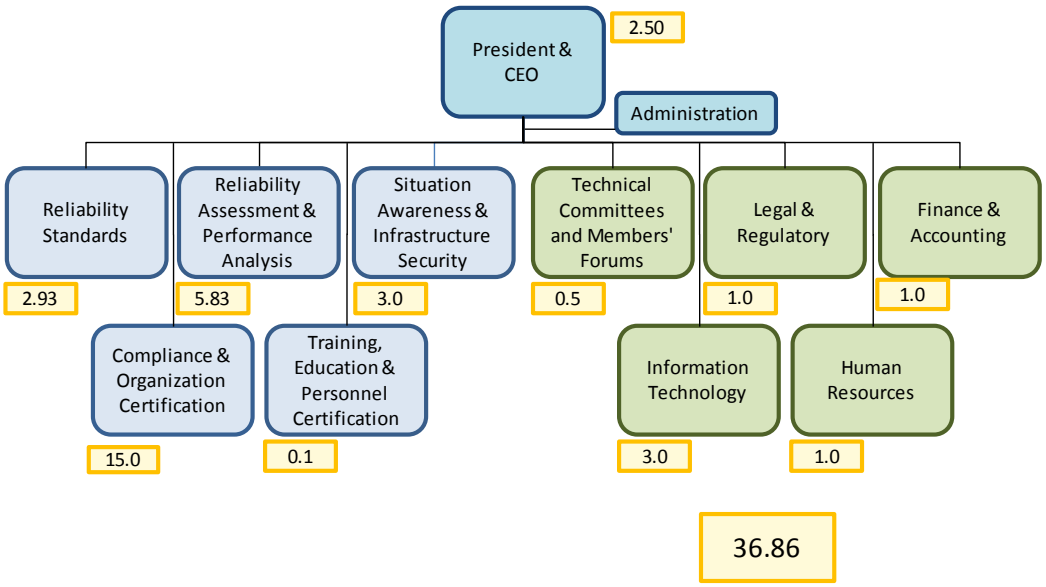
Statement of Financial Position

Table to be Inserted

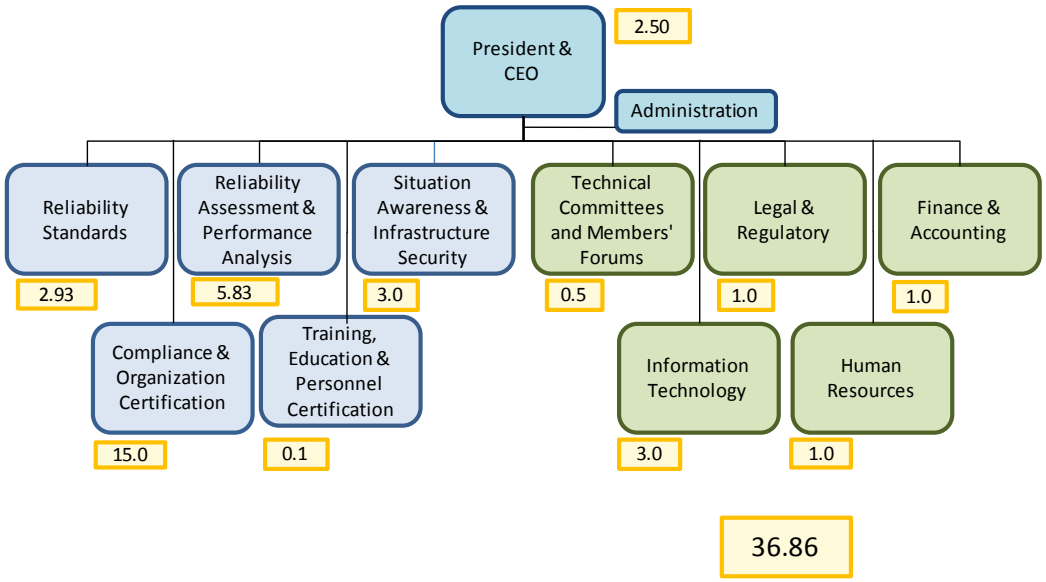
Table to be Inserted

Table to be Inserted

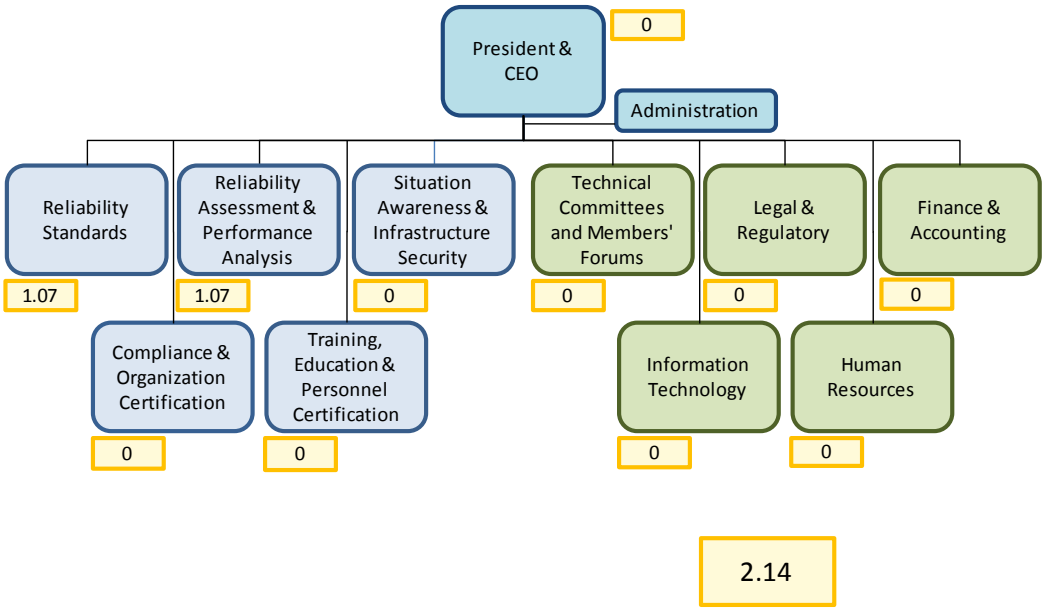
2014 Budget Staff Allocations - RE Division



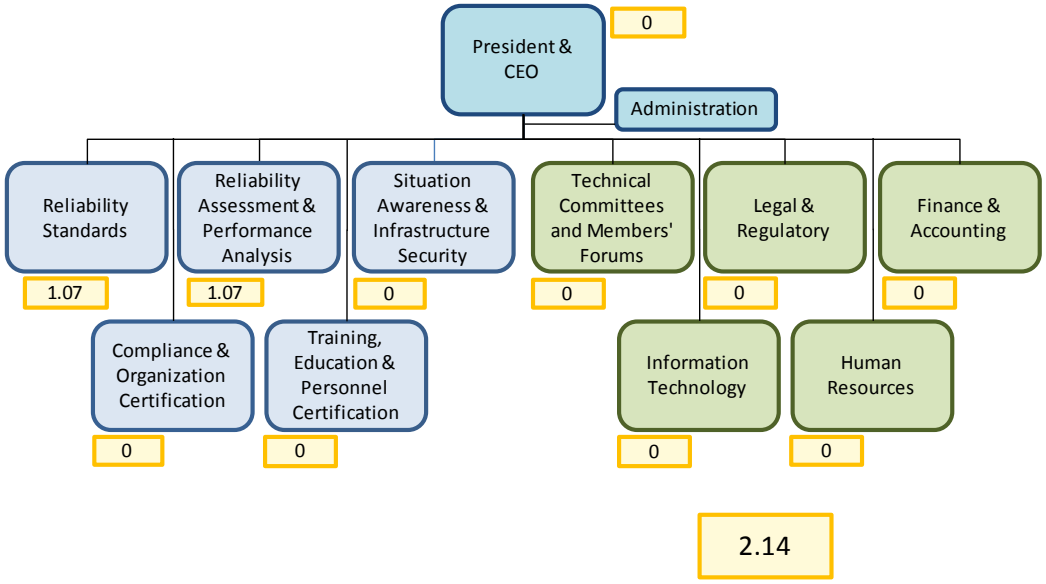
2015 Budget Staff Allocations - RE Division

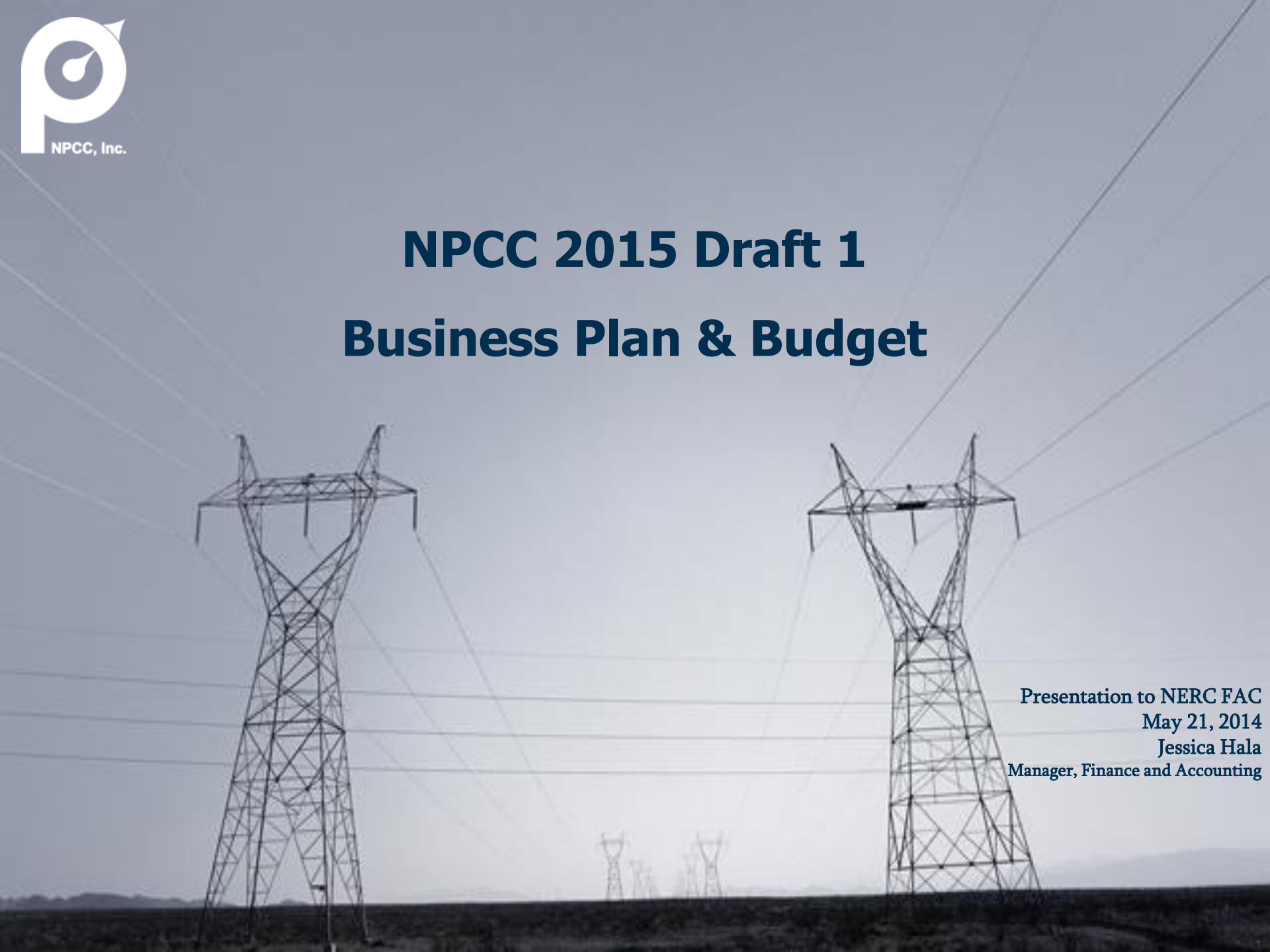


2014 Budget Staff Allocations - CS Division



2015 Budget Staff Allocations - CS Division





NPCC 2015 Draft 1

Business Plan & Budget

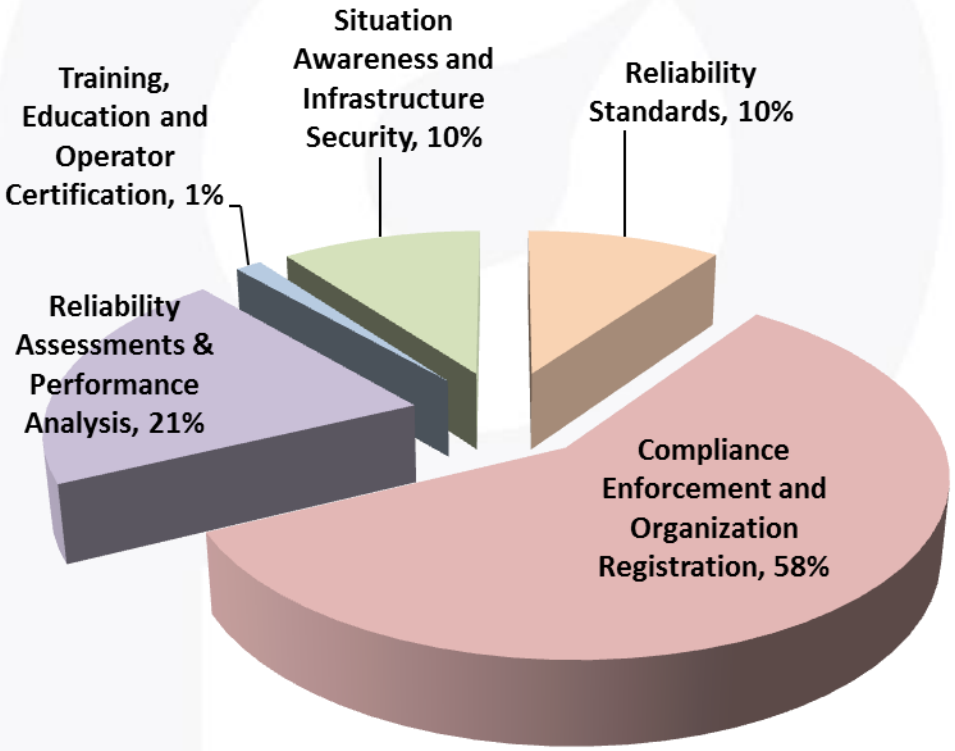
Presentation to NERC FAC
May 21, 2014

Jessica Hala
Manager, Finance and Accounting

2015 Budget Overview

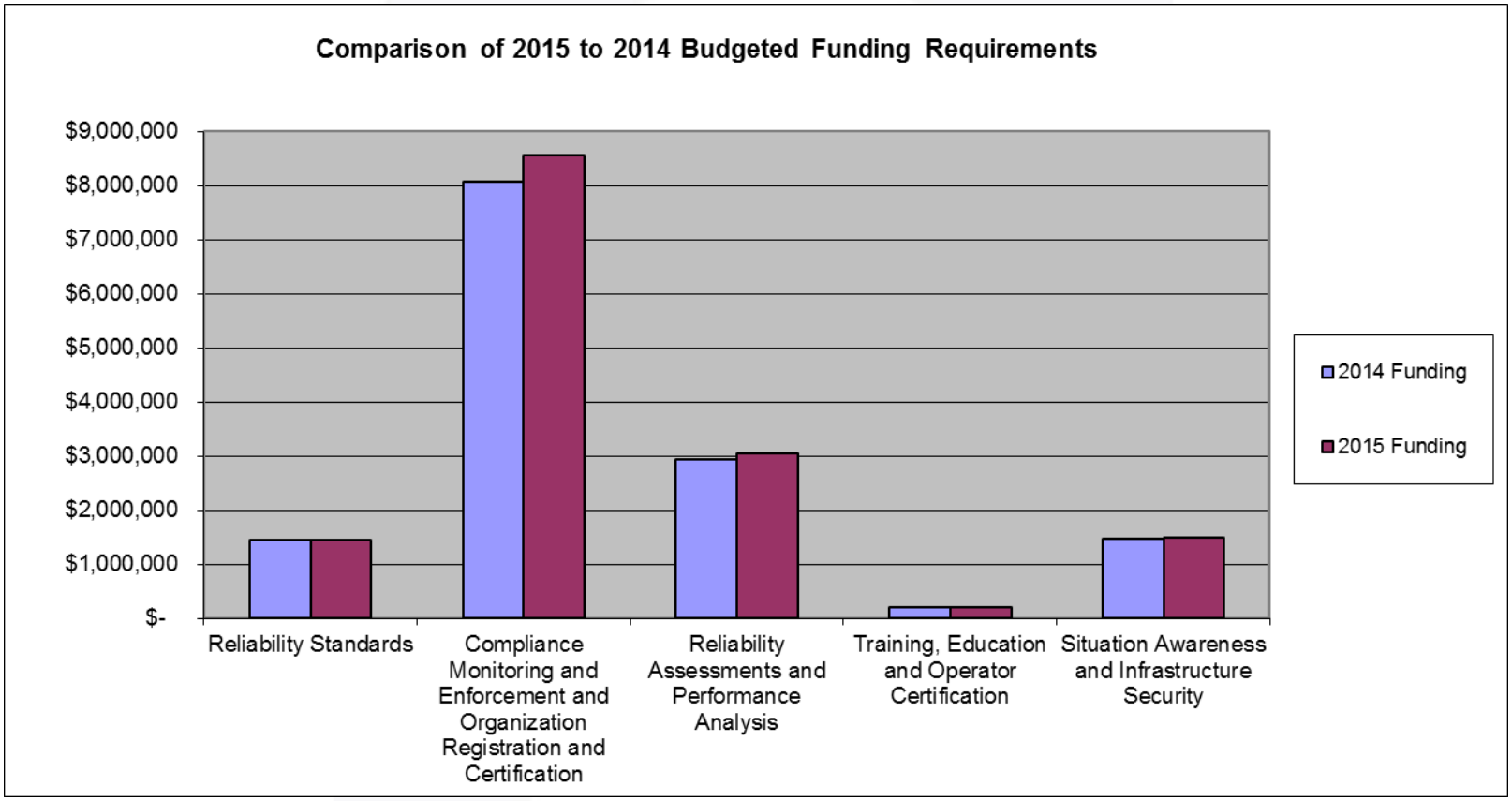
- Staffing Flat
  - 39 FTEs (Regional Entity Division 36.86, Criteria Services Division 2.14)
  - Currently one open position in Standards program area
- Salaries
  - Average wage package increase of 3%
  - Vacancy rate of 2% based on recent trends (currently one open position after 6 months fully staffed)
- Change in Operating Reserves requirement from fixed 8.33% (30 days) to a range between 8.33% and 25.00% (90 days) to provide more stability in annual funding assessments

2015 Total Resources by Program Area Regional Entity (RE) Division



Summary Comparison by Program

Regional Entity (RE) Division



2014-2015 RE Budget Comparison

	2015	2014	Variance	% Variance	Explanation
Funding					
Assessments	14,078,378	13,611,880	466,498	3.43%	
Penalties	281,000	153,000	128,000	83.66%	
Other Income	64,000	64,000	-	0.00%	
Total Funding	14,423,378	13,828,880	594,498		
Expenses					
Personnel Expenses	8,929,241	8,850,160	79,081	0.89%	3% average wage package increase; 2% vacancy rate
Meetings	365,000	365,000	-	0.00%	
Travel	890,000	890,000	-	0.00%	
Conference Calls	45,000	77,000	(32,000)	-41.56%	Lower negotiated rate with a new vendor
Consultants and Contracts	2,342,000	1,924,433	417,567	21.70%	Increase in compliance and RAPA
Rent & Improvements	751,500	737,272	14,228	1.93%	
Office Costs	578,700	536,500	42,200	7.87%	Increase in computer/network maintenance costs
Professional Services	1,025,000	966,500	58,500	6.05%	
Miscellaneous	40,000	80,000	(40,000)	-50.00%	Continuing efforts to control costs
Depreciation	202,019	250,000	(47,981)	-19.19%	Assets becoming fully depreciated in 2014
Indirect Expenses	(409,902)	(405,859)	(4,043)	1.00%	
Other Non-Operating Expenses	-	-	-		
Total Expenses	14,758,558	14,271,006	487,552	3.42%	
Increase(Decrease) in Fixed Assets	19,981	(142,000)	161,981		
Total Budget	14,778,539	14,129,006	649,533	4.60%	
Change in Working Capital	(355,161)	(300,126)	(55,035)		

NPCC, Inc.

FTE Comparison

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
REGIONAL ENTITY DIVISION						
Operational Programs						
Reliability Standards	2.93	2.93	2.00	0.93	2.93	0.00
Compliance Monitoring and Enforcement and Organization Registration and Certification	16.00	16.00	16.00	0.00	16.00	0.00
Training, Education, and Operator Certification	0.10	0.10	0.10	0.00	0.10	0.00
Reliability Assessment and Performance Analysis	5.83	5.83	4.90	0.93	5.83	0.00
Situation Awareness and Infrastructure Security	3.00	3.00	3.00	0.00	3.00	0.00
Total FTEs Operational Programs	**27.86**	**27.86**	**26.00**	**1.86**	**27.86**	**0.00**
Administrative Programs						
Technical Committees and Member Forums	0.50	0.50	0.50	0.00	0.50	0.00
General and Administrative	2.50	2.50	2.50	0.00	2.50	0.00
Information Technology	3.00	3.00	3.00	0.00	3.00	0.00
Legal and Regulatory	1.00	1.00	1.00	0.00	1.00	0.00
Human Resources	1.00	1.00	1.00	0.00	1.00	0.00
Accounting and Finance	1.00	1.00	1.00	0.00	1.00	0.00
Total FTEs Administrative Programs	**9.00**	**9.00**	**9.00**	**0.00**	**9.00**	**0.00**
Total FTEs	**36.86**	**36.86**	**35.00**	**1.86**	**36.86**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

Resource Adequacy

- Resource assessment and reprioritization from the 2014 Business Plan and Budget has been conducted and will continue through 2015.

- Full impact of Reliability Assurance Initiative (RAI), Risk Assessment, Internal Control Evaluation, and CIP V5 implementation is currently unknown
  - Compliance staffing, in combination with increase in contractors, is expected to be adequate
- Full impact of revised BES definition implementation is currently unknown
  - RAPA staffing, in combination with increase in contractors, is expected to be adequate to address BES identification/exception requests

Process Improvements

- Implementation of CEAP in NERC Standards Development Process
- Utilization of consistent audit checklist and handbook with audits informed by evaluation of entity risk profile
- Enhanced FFT and introduction of compliance exception principles
- Expedited processing of self-reports
- Increased scheduling rigor in settlement processing
- Implementation of efficient BES Notification and Exception Processing
- Improved integration of Events Analysis processing across ERO

Alignment of RE and ERO

- Fully aligned with ERO Enterprise Strategic Plan and Performance Metrics
- Functional initiatives/activities within program areas references applicable ERO goals within the business plan using footnotes
- CS Division continues to support international, interconnected BPS reliability through compliance monitoring with more-stringent, regionally-specific reliability criteria

Efficiency and Controlling Costs

- Ongoing efforts to hold more meetings on site and via conference call or webinar.
- Limiting number of staff attending offsite meetings.
- Continued expansion of pre-audit processing to contain the time required of an audit team to be on-site in order to complete an audit and, therefore, to complete audits more cost-efficiently.

Working Capital and Operating Reserves

- Change in Operating Reserves requirement from fixed 8.33% (30 days) to a range between 8.33% and 25.00% (90 days) to provide more stability in annual funding assessments.

- Working Capital requirement remains unchanged with a targeted level of 8.33% (30 days) of the annual budget.

- No utilization of reserves is contemplated; Board authorization would be required

Questions?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Processes Manual

VERSION 3

Effective: June 26, 2013

to ensure the reliability of the bulk power system

Table of Contents

Section 1.0: Introduction 3
Section 2.0: Elements of a Reliability Standard 6
Section 3.0: Reliability Standards Program Organization 10
Section 4.0: Process for Developing, Modifying, Withdrawing or Retiring a Reliability Standard 14
Section 5.0: Process for Developing a Defined Term 26
Section 6.0: Processes for Conducting Field Tests and Collecting and Analyzing Data 28
Section 7.0: Process for Developing an Interpretation 30
Section 8.0: Process for Appealing an Action or Inaction 34
Section 9.0: Process for Developing a Variance 36
Section 10.0: Processes for Developing a Reliability Standard Related to a Confidential Issue 38
Section 11.0: Process for Approving Supporting Documents 43
Section 12.0: Process for Correcting Errata 44
Section 13.0: Process for Conducting Periodic Reviews of Reliability Standards 45
Section 14.0: Public Access to Reliability Standards Information 46
Section 15.0: Process for Updating Standard Processes 47
Section 16.0: Waiver 48

Section 1.0: Introduction

1.1: Authority
This manual is published by the authority of the NERC Board of Trustees. The Board of Trustees, as necessary to maintain NERC's certification as the Electric Reliability Organization ("ERO"), may file the manual with Applicable Governmental Authorities for approval as an ERO document. When approved, the manual is appended to and provides implementation detail in support of the ERO Rules of Procedure Section 300 — Reliability Standards Development.

Capitalized terms not otherwise defined herein, shall have the meaning set forth in the Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure.

1.2: Scope
The policies and procedures in this manual shall govern the activities of the North American Electric Reliability Corporation ("NERC") related to the development, approval, revision, reaffirmation, and withdrawal of Reliability Standards, Interpretations, Violation Risk Factors ("VRFs"), Violation Severity Levels ("VSLs"), definitions, Variances, and reference documents developed to support standards for the Reliable Operation and planning of the North American Bulk Power Systems.

This manual also addresses the role of the Standards Committee, drafting team and ballot body in the development and approval of Compliance Elements in conjunction with standard development.

1.3: Background
NERC is a nonprofit corporation formed for the purpose of becoming the North American ERO. NERC works with all stakeholder segments of the electric industry, including electricity users, to develop Reliability Standards for the reliability planning and Reliable Operation of the North American Bulk Power Systems. In the United States, the Energy Policy Act of 2005 added Section 215 to the Federal Power Act for the purpose of establishing a framework to make Reliability Standards mandatory for all Bulk Power System owners, operators, and users. Similar authorities are provided by Applicable Governmental Authorities in Canada. NERC was certified as the ERO effective July 2006. *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 (2007).

1.4: Essential Attributes of NERC's Reliability Standards Processes
NERC's Reliability Standards development processes provide reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing a proposed Reliability Standard consistent with the attributes necessary for American National Standards Institute ("ANSI") accreditation. The same attributes, as well as transparency, consensus-building, and timeliness, are also required under the ERO Rules of Procedure Section 304.

- ***Open Participation***
  Participation in NERC's Reliability Standards development balloting and approval processes shall be open to all entities materially affected by NERC's Reliability Standards. There shall be no financial barriers to participation in NERC's Reliability Standards balloting and approval processes. Membership in the Registered Ballot Body shall not be conditional upon membership in any organization, nor unreasonably restricted on the basis of technical qualifications or other such requirements.

- ***Balance***
  NERC's Reliability Standards development processes shall not be dominated by any two interest categories, individuals, or organizations and no single interest category, individual, or organization is able to defeat a matter.

  NERC shall use a voting formula that allocates each industry Segment an equal weight in determining the final outcome of any Reliability Standard action. The Reliability Standards development processes shall have a balance of interests. Participants from diverse interest categories shall be encouraged to join the Registered Ballot Body and participate in the balloting process, with a goal of achieving balance between the interest categories. The Registered Ballot Body serves as the consensus body voting to approve each new or proposed Reliability Standard, definition, Variance, and Interpretation.

- ***Coordination and harmonization with other American National Standards activities***
  NERC is committed to resolving any potential conflicts between its Reliability Standards development efforts and existing American National Standards and candidate American National Standards.

- ***Notification of standards development***
  NERC shall publicly distribute a notice to each member of the Registered Ballot Body, and to each stakeholder who indicates a desire to receive such notices, for each action to create, revise, reaffirm, or withdraw a Reliability Standard, definition, or Variance; and for each proposed Interpretation. Notices shall be distributed electronically, with links to the relevant information, and notices shall be posted on NERC's Reliability Standards web page. All notices shall identify a readily available source for further information.

- ***Transparency***
  The process shall be transparent to the public.

- ***Consideration of views and objections***
  Drafting teams shall give prompt consideration to the written views and objections of all participants as set forth herein. Drafting teams shall make an effort to resolve each objection that is related to the topic under review.

- ***Consensus Building***
  The process shall build and document consensus for each Reliability Standard, both with regard to the need and justification for the Reliability Standard and the content of the Reliability Standard.

- ***Consensus vote***
  NERC shall use its voting process to determine if there is sufficient consensus to approve a proposed Reliability Standard, definition, Variance, or Interpretation. NERC shall form a ballot pool for each Reliability Standard action from interested members of its Registered Ballot Body. Approval of any Reliability Standard action requires:

  - A quorum, which is established by at least 75% of the members of the ballot pool submitting a response excluding unreturned ballots; and
  - A two-thirds majority of the weighted Segment votes cast shall be affirmative. The number of votes cast during all stages of balloting except the final ballot is the sum of affirmative and negative votes with comments, excluding abstentions, non-responses, and

negative votes without comments. During the final ballot, the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and non-responses.

- ***Timeliness***
  Development of Reliability Standards shall be timely and responsive to new and changing priorities for reliability of the Bulk Power System.

- ***Metric Policy***
  The International System of units is the preferred units of measurement in NERC Reliability Standard. However, because NERC's Reliability Standards apply in Canada, the United States and portions of Mexico, where applicable, measures are provided in both the metric and English units.

1.5: Ethical Participation

All participants in the NERC Standard development process, including drafting teams, quality reviewers, Standards Committee members and members of the Registered Ballot Body, are obligated to act in an ethical manner in the exercise of all activities conducted pursuant to the terms and conditions of the Standard Processes Manual and the standard development process.

Section 2.0: Elements of a Reliability Standard

2.1: Definition of a Reliability Standard

A Reliability Standard includes a set of Requirements that define specific obligations of owners, operators, and users of the North American Bulk Power Systems. The Requirements shall be material to reliability and measurable. A Reliability Standard is defined as follows:

> "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. *See* Appendix 2 to the NERC Rules of Procedure, Definitions Used in the Rules of Procedure.

2.2: Reliability Principles

NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American Bulk Power Systems.[1] Each Reliability Standard shall enable or support one or more of the reliability principles, thereby ensuring that each Reliability Standard serves a purpose in support of reliability of the North American Bulk Power Systems. Each Reliability Standard shall also be consistent with all of the reliability principles, thereby ensuring that no Reliability Standard undermines reliability through an unintended consequence.

2.3: Market Principles

Recognizing that Bulk Power System reliability and electricity markets are inseparable and mutually interdependent, all Reliability Standards shall be consistent with the market interface principles.[2] Consideration of the market interface principles is intended to ensure that Reliability Standards are written such that they achieve their reliability objective without causing undue restrictions or adverse impacts on competitive electricity markets.

2.4: Types of Reliability Requirements

Generally, each Requirement of a Reliability Standard shall identify what Functional Entities shall do, and under what conditions, to achieve a specific reliability objective. Although Reliability Standards all follow this format, several types of Requirements may exist, each with a different approach to measurement.

- **Performance-based Requirements** define a specific reliability objective or outcome achieved by one or more entities that has a direct, observable effect on the reliability of the Bulk Power System, *i.e.* an effect that can be measured using power system data or trends. In its simplest form, a performance-based requirement has four components: *who,*

[1] The intent of the set of NERC Reliability Standards is to deliver an adequate level of reliability. The latest set of reliability principles and the latest set of characteristics associated with an adequate level of reliability are posted on the Reliability Standards Resources web page.

[2] The latest set of market interface principles is posted on the Reliability Standards Resources web page.

under what conditions (if any), shall perform what action, to achieve what particular result or outcome.

- **Risk-based Requirements** define actions by one or more entities that reduce a stated risk to the reliability of the Bulk Power System and can be measured by evaluating a particular product or outcome resulting from the required actions. A risk-based reliability requirement should be framed as: *who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the Bulk Power System.*

- **Capability-based Requirements** define capabilities needed by one or more entities to perform reliability functions and can be measured by demonstrating that the capability exists as required. A capability-based reliability requirement should be framed as: *who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the Bulk Power System.*

The body of reliability Requirements collectively provides a defense-in-depth strategy supporting reliability of the Bulk Power System.

2.5: Elements of a Reliability Standard

A Reliability Standard includes several components designed to work collectively to identify what entities must do to meet their reliability-related obligations as an owner, operator or user of the Bulk Power System.

The components of a Reliability Standard may include the following:

Title: A brief, descriptive phrase identifying the topic of the Reliability Standard.

Number: A unique identification number assigned in accordance with a published classification system to facilitate tracking and reference to the Reliability Standards.[3]

Purpose: The reliability outcome achieved through compliance with the Requirements of the Reliability Standard.

Applicability: Identifies which entities are assigned reliability requirements. The specific Functional Entities and Facilities to which the Reliability Standard applies.

Effective Dates: Identification of the date or pre-conditions determining when each Requirement becomes effective in each jurisdiction.

Requirement: An explicit statement that identifies the Functional Entity responsible, the action or outcome that must be achieved, any conditions achieving the action or outcome, and the reliability-related benefit of the action or outcome. Each Requirement shall be a statement for which compliance is mandatory.

Compliance Elements: Elements to aid in the administration of ERO compliance monitoring and enforcement responsibilities.[4]

[3] Reliability Standards shall be numbered in accordance with the NERC Standards Numbering Convention as provide on the Reliability Standards Resources web page.

- ***Measure:*** Provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.

- ***Violation Risk Factors and Violation Severity Levels:*** Violation risk factors (VRFs) and violation severity levels (VSLs) are used as factors when determining the size of a penalty or sanction associated with the violation of a requirement in an approved reliability standard.[5] Each requirement in each reliability standard has an associated VRF and a set of VSLs. VRFs and VSLs are developed by the drafting team, working with NERC Staff, at the same time as the associated reliability standard, but are not part of the reliability standard. The Board of Trustees is responsible for approving VRFs and VSLs.

  - ***Violation Risk Factors***
    VRFs identify the potential reliability significance of noncompliance with each requirement. Each requirement is assigned a VRF in accordance with the latest approved set of VRF criteria.[6]

  - ***Violation Severity Levels***
    VSLs define the degree to which compliance with a requirement was not achieved. Each requirement shall have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs. Each requirement is assigned one or more VSLs in accordance with the latest approved set of VSL criteria.7

Version History: The version history is provided for informational purposes and lists information regarding prior versions of Reliability Standards.

Variance: A Requirement (to be applied in the place of the continent-wide Requirement) that is applicable to a specific geographic area or to a specific set of Registered Entities.

Compliance Enforcement Authority: The entity that is responsible for assessing performance or outcomes to determine if an entity is compliant with the associated Reliability Standard. The Compliance Enforcement Authority will be NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

***Application guidelines*:** Guidelines to support the implementation of the associated Reliability Standard.

***Procedures*:** Procedures to support implementation of the associated Reliability Standard.

The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes, to establish the relevant scope and technical paradigm, and to

---

[4] It is the responsibility of the ERO staff to develop compliance tools for each standard; these tools are not part of the standard but are referenced in this manual because the preferred approach to developing these tools is to use a transparent process that leverages the technical and practical expertise of the drafting team and ballot pool..
[5] The *Sanction Guidelines of the North American Electric Reliability Corporation* identifies the factors used to determine a penalty or sanction for violation of reliability standard and is posted on the NERC Web Site.
[6] The latest set of approved VRF Criteria is posted on the Reliability Standards Resources Web Page.
[7] The latest set of approved VSL Criteria is posted on the Reliability Standards Resources Web Page.

provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority.

Section 3.0: Reliability Standards Program Organization

3.1: Board of Trustees

The NERC Board of Trustees shall consider for adoption Reliability Standards, definitions, Variances and Interpretations and associated implementation plans that have been processed according to the processes identified in this manual. Once the Board adopts a Reliability Standard, definition, Variance or Interpretation, the Board shall direct NERC Staff to file the document(s) for approval with Applicable Governmental Authorities.

3.2: Registered Ballot Body

The Registered Ballot Body comprises all entities or individuals that qualify for one of the Segments approved by the Board of Trustees[8], and are registered with NERC as potential ballot participants in the voting on Reliability Standards. Each member of the Registered Ballot Body is eligible to join the ballot pool for each Reliability Standard action.

3.3: Ballot Pool

Each Reliability Standard action has its own ballot pool formed of interested members of the Registered Ballot Body. The ballot pool comprises those members of the Registered Ballot Body that respond to a pre-ballot request to participate in that particular Reliability Standard action. The ballot pool votes on each Reliability Standards action. The ballot pool remains in place until all balloting related to that Reliability Standard action has been completed.

3.4: Standards Committee

The Standards Committee serves at the pleasure and direction of the NERC Board of Trustees, and the Board approves the Standards Committee's Charter.[9] Standards Committee members are elected by their respective Segment's stakeholders. The Standards Committee consists of two members of each of the Segments in the Registered Ballot Body.[10] A member of the NERC Reliability Standards Staff shall serve as the non-voting secretary to the Standards Committee.

The Standards Committee is responsible for managing the Reliability Standards processes for development of Reliability Standards, definitions, Variances and Interpretations in accordance with this manual. The responsibilities of the Standards Committee are defined in detail in the Standards Committee's Charter. The Standards Committee is responsible for ensuring that the Reliability Standards, definitions, Variances and Interpretations developed by drafting teams are developed in accordance with the processes in this manual and meet NERC's benchmarks for Reliability Standards as well as criteria for governmental approval.[11]

The Standards Committee has the right to remand work to a drafting team, to reject the work of a drafting team, or to accept the work of a drafting team. The Standards Committee may disband a drafting team if it determines (a) that the drafting team is not producing a standard in a timely manner; (b) the drafting

[8] The industry Segment qualifications are described in the Development of the Registered Ballot Body and Segment Qualification Guidelines document posted on the Reliability Standards Resources web page and are included in Appendix 3D of the NERC Rules of Procedure.

[9] The Standards Committee Charter is posted on the Reliability Standards Resources web page.

[10] In addition to balanced Segment representation, the Standards Committee shall also have representation that is balanced among countries based on Net Energy for Load ("NEL"). As needed, the Board of Trustees may approve special procedures for the balancing of representation among countries represented within NERC.

[11] The Ten Benchmarks of an Excellent Reliability Standard and FERC's Criteria for Approving Reliability Standards are posted on the Reliability Standards Resources web page.

team is not able to produce a standard that will achieve industry consensus; (c) the drafting team has not addressed the scope of the SAR; or (d) the drafting team has failed to fully address a regulatory directive or otherwise provided a responsive or equally efficient and effective alternative. The Standards Committee may direct a drafting team to revise its work to follow the processes in this manual or to meet the criteria for NERC's benchmarks for Reliability Standards, or to meet the criteria for governmental approval; however, the Standards Committee shall not direct a drafting team to change the technical content of a draft Reliability Standard.

The Standards Committee shall meet at regularly scheduled intervals (either in person, or by other means). All Standards Committee meetings are open to all interested parties.

3.5: NERC Reliability Standards Staff

The NERC Reliability Standards Staff, led by the Director of Standards, is responsible for administering NERC's Reliability Standards processes in accordance with this manual. The NERC Reliability Standards Staff provides support to the Standards Committee in managing the Reliability Standards processes and in supporting the work of all drafting teams. The NERC Reliability Standards Staff works to ensure the integrity of the Reliability Standards processes and consistency of quality and completeness of the Reliability Standards. The NERC Reliability Standards Staff facilitates all steps in the development of Reliability Standards, definitions, Variances, Interpretations and associated implementation plans.

The NERC Reliability Standards Staff is responsible for presenting Reliability Standards, definitions, Variances, and Interpretations to the NERC Board of Trustees for adoption. When presenting Reliability Standards-related documents to the NERC Board of Trustees for adoption or approval, the NERC Reliability Standards Staff shall report the results of the associated stakeholder ballot, including identification of unresolved stakeholder objections and an assessment of the document's practicality and enforceability.

3.6: Drafting Teams

The Standards Committee shall appoint industry experts to drafting teams to work with stakeholders in developing and refining Standard Authorization Requests ("SARs"), Reliability Standards, definitions, and Variances. The NERC Reliability Standards Staff shall appoint drafting teams that develop Interpretations. The NERC Reliability Standards Staff shall provide, or solicit from the industry, essential support for each of the drafting teams in the form of technical writers, legal, compliance, and rigorous and highly trained project management and facilitation support personnel.

Each drafting team may consist of a group of technical, legal, and compliance experts that work cooperatively with the support of the NERC Reliability Standards Staff.[12] The technical experts provide the subject matter expertise and guide the development of the technical aspects of the Reliability Standard, assisted by technical writers, legal and compliance experts. The technical experts maintain authority over the technical details of the Reliability Standard. Each drafting team appointed to develop a Reliability Standard is responsible for following the processes identified in this manual as well as procedures developed by the Standards Committee from the inception of the assigned project through the final acceptance of that project by Applicable Governmental Authorities.

Collectively, each drafting team:

- Drafts proposed language for the Reliability Standards, definitions, Variances, and/or Interpretations and associated implementation plans.

[12] The detailed responsibilities of drafting teams are outlined in the Drafting Team Guidelines, which is posted on the Reliability Standards Resources web page.

- Develops and refines technical documents that aid in the understanding of Reliability Standards.
- Works collaboratively with NERC Compliance Monitoring and Enforcement Staff to develop Reliability Standard Audit Worksheets ("RSAWs") at the same time Reliability Standards are developed.
- Provides assistance to NERC Staff in the development of Compliance Elements of proposed Reliability Standards.
- Solicits, considers, and responds to comments related to the specific Reliability Standards development project.
- Participates in industry forums to help build consensus on the draft Reliability Standards, definitions, Variances, and/or Interpretations and associated implementation plans.
- Assists in developing the documentation used to obtain governmental approval of the Reliability Standards, definitions, Variances, and/or Interpretations and associated implementation plans.

All drafting teams report to the Standards Committee.

3.7: Governmental Authorities

The Federal Energy Regulatory Commission ("FERC") in the United States of America, and where permissible by statute or regulation, the provincial government of each of the eight Canadian Provinces (Manitoba, Nova Scotia, Saskatchewan, Alberta, Ontario, British Columbia, New Brunswick and Quebec) and the National Energy Board of Canada have the authority to approve each new, revised or withdrawn Reliability Standard, definition, Variance, VRF, VSL and Interpretation following adoption or approval by the NERC Board of Trustees.

3.8: Committees, Subcommittees, Working Groups, and Task Forces

NERC's technical committees, subcommittees, working groups, and task forces provide technical research and analysis used to justify the development of new Reliability Standards and provide guidance, when requested by the Standards Committee, in overseeing field tests or collection and analysis of data. The technical committees, subcommittees, working groups, and task forces provide feedback to drafting teams during both informal and formal comment periods.

The Standards Committee may request that a NERC technical committee or other group prepare a Technical document to support development of a proposed Reliability Standard.

The technical committees, subcommittees, working groups, and task forces share their observations regarding the need for new or modified Reliability Standards or Requirements with the NERC Reliability Standards Staff for use in identifying the need for new Reliability Standards projects for the three-year *Reliability Standards Development Plan*.

3.9: Compliance and Certification Committee

The Compliance and Certification Committee is responsible for monitoring NERC's compliance with its Reliability Standards processes and procedures and for monitoring NERC's compliance with the Rules of Procedure regarding the development of new or revised Reliability Standards, definitions, Variances, and Interpretations. The Compliance and Certification Committee may assist in verifying that each proposed Reliability Standard is enforceable as written before the Reliability Standard is posted for formal stakeholder comment and balloting.

3.10: Compliance Monitoring and Enforcement Program

As applicable, the NERC Compliance Monitoring and Enforcement Program Staff manages and enforces compliance with approved Reliability Standards. Compliance Monitoring and Enforcement Staff are responsible for the development of select compliance tools. The drafting team and the Compliance Monitoring and Enforcement Program Staff shall work together during the Reliability Standard development process to ensure an accurate and consistent understanding of the Requirements and their intent, and to ensure that applicable compliance tools accurately reflect that intent. The goal of this collaboration is to ensure that application of the Reliability Standards in the Compliance Monitoring and Enforcement Program by NERC and the Regional Entities is consistent.

The Compliance Monitoring and Enforcement Program is encouraged to share its observations regarding the need for new or modified Requirements with the NERC Reliability Standards Staff for use in identifying the need for new Reliability Standards projects.

3.11: North American Energy Standards Board ("NAESB")

While NERC has responsibility for developing Reliability Standards to support reliability, NAESB has responsibility for developing business practices and coordination between reliability and business practices as needed. NERC and NAESB developed and approved a procedure[13] to guide the development of Reliability Standards and business practices where the reliability and business practice components are intricately entwined within a proposed Reliability Standard.

[13] The NERC NAESB Template Procedure for Joint Standards Development and Coordination is posted on the Reliability Standards Resources web page.

Section 4.0: Process for Developing, Modifying, Withdrawing or Retiring a Reliability Standard

There are several steps to the development, modification, withdrawal or retirement of a Reliability Standard.[14]

The development of the *Reliability Standards Development Plan* is the appropriate forum for reaching agreement on whether there is a need for a Reliability Standard and the scope of a proposed Reliability Standard. A typical process for a project identified in the *Reliability Standards Development Plan* that involves a revision to an existing Reliability Standard is shown below. Note that most projects do not include a field test.

[14] The process described is also applicable to projects used to propose a new or modified definition or Variance or to propose retirement of a definition or Variance.

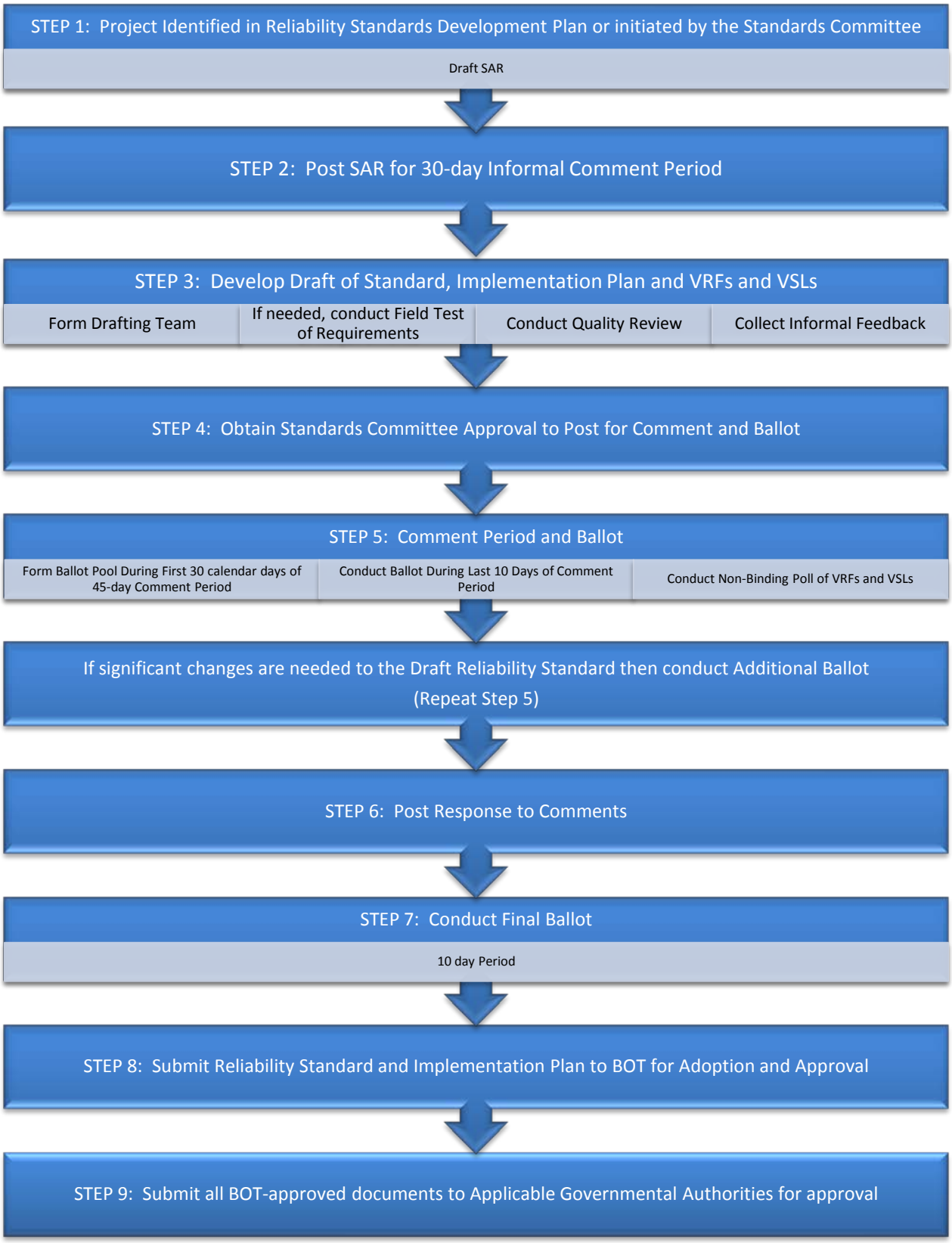


FIGURE 1: Process for Developing or Modifying a Reliability Standard

4.1: Posting and Collecting Information on SARs

Standard Authorization Request

A Standard Authorization Request ("SAR") is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions or the benefit of retiring one or more approved Reliability Standards. Any entity or individual, including NERC committees or subgroups and NERC Staff, may propose the development of a new or modified Reliability Standard, or may propose the retirement of a Reliability Standard (in whole or in part), by submitting a completed SAR[15] to the NERC Reliability Standards Staff. The Standards Committee has the authority to approve the posting of all SARs for projects that propose (i) developing a new or modified Reliability Standard or definition or (ii) propose retirement of an existing Reliability Standard (or elements thereof).

The NERC Reliability Standards Staff sponsors an open solicitation period each year seeking ideas for new Reliability Standards projects (using *Reliability Standards Suggestions and Comments forms*). The open solicitation period is held in conjunction with the annual revision to the *Reliability Standards Development Plan*. While the Standards Committee prefers that ideas for new projects be submitted during this annual solicitation period through submittal of a *Reliability Standards Suggestions and Comments Form*,[16] a SAR proposing a specific project may be submitted to the NERC Reliability Standards Staff at any time.

Each SAR that proposes a "new" or substantially revised Reliability Standard or definition should be accompanied by a technical justification that includes, as a minimum, a discussion of the reliability-related benefits and costs of developing the new Reliability Standard or definition, and a technical foundation document (*e.g.*, research paper) to guide the development of the Reliability Standard or definition. The technical document should address the engineering, planning and operational basis for the proposed Reliability Standard or definition, as well as any alternative approaches considered during SAR development.

The NERC Reliability Standards Staff shall review each SAR and work with the submitter to verify that all required information has been provided. All properly completed SARs shall be submitted to the Standards Committee for action at the next regularly scheduled Standards Committee meeting.

When presented with a SAR, the Standards Committee shall determine if the SAR is sufficiently complete to guide Reliability Standard development and whether the SAR is consistent with this manual. The Standards Committee shall take one of the following actions:

- Accept the SAR.
- Remand the SAR back to the requestor or to NERC Reliability Standards Staff for additional work.
- Reject the SAR. The Standards Committee may reject a SAR for good cause. If the Standards Committee rejects a SAR, it shall provide a written explanation for rejection to the sponsor within ten days of the rejection decision.
- Delay action on the SAR pending one of the following: (i) development of a technical justification for the proposed project; or (ii) consultation with another NERC Committee to determine if there is another approach to addressing the issue raised in the SAR.

If the Standards Committee is presented with a SAR that proposes developing a new Reliability Standard or definition but does not have a technical justification upon which the Reliability Standard or definition

[15] The SAR form can be downloaded from the Reliability Standards Resources web page.
[16] The *Reliability Standards Suggestions and Comments Form* can be downloaded from the Reliability Standards Resources web page.

can be developed, the Standards Committee shall direct the NERC Reliability Standards Staff to post the SAR for a 30-day comment period solely to collect stakeholder feedback on the scope of technical foundation, if any, needed to support the proposed project. If a technical foundation is determined to be necessary, the Standards Committee shall solicit assistance from NERC's technical committees or other industry experts to provide that foundation before authorizing development of the associated Reliability Standard or definition.

During the SAR comment process, the drafting team may become aware of potential regional Variances related to the proposed Reliability Standard. To the extent possible, any regional Variances or exceptions should be made a part of the SAR so that if the SAR is authorized, such variations shall be made a part of the draft new or revised Reliability Standard.

If the Standards Committee accepts a SAR, the project shall be added to the list of approved projects. The Standards Committee shall assign a priority to the project, relative to all other projects under development, and those projects already identified in the *Reliability Standards Development Plan* that are already approved for development.

The Standards Committee shall work with the NERC Reliability Standards Staff to coordinate the posting of SARs for new projects, giving consideration to each project's priority.

4.2: SAR Posting

When the Standards Committee determines it is ready to initiate a new project, the Standards Committee shall direct NERC Staff to post the project's SAR in accordance with the following:

- For SARs that are limited to addressing regulatory directives, or revisions to Reliability Standards that have had some vetting in the industry, authorize posting the SAR for a 30-day informal comment period with no requirement to provide a formal response to the comments received.
- For SARs that address the development of new projects or Reliability Standards, authorize posting the SAR for a 30-day formal comment period.

If a SAR for a new Reliability Standard is posted for a formal comment period, the Standards Committee shall appoint a drafting team to work with the NERC Staff coordinator to give prompt consideration of the written views and objections of all participants. The Standards Committee may use a public nomination process to populate the Reliability Standard drafting team, or may use another method that results in a team that collectively has the necessary technical expertise and work process skills to meet the objectives of the project. In some situations, an *ad hoc* team may already be in place with the requisite expertise, competencies, and diversity of views that are necessary to refine the SAR and develop the Reliability Standard, and additional members may not be needed. The drafting team shall address all comments submitted, which may be in the form of a summary response addressing each of the issues raised in comments received, during the public posting period. An effort to resolve all expressed objections shall be made, and each objector shall be advised of the disposition of the objection and the reasons therefore. If the drafting team concludes that there is not sufficient stakeholder support to continue to refine the SAR, the team may recommend that the Standards Committee direct curtailment of work on the SAR.

While there is no established limit on the number of times a SAR may be posted for comment, the Standards Committee retains the right to reverse its prior decision and reject a SAR if it believes continued revisions are not productive. The Standards Committee shall notify the sponsor in writing of the rejection within 10 calendar days.

If stakeholders indicate support for the project proposed with the SAR, the drafting team shall present its work to the Standards Committee with a request that the Standards Committee authorize development of the associated Reliability Standard.

The Standards Committee, once again considering the public comments received and their resolution, may then take one of the following actions:

- Authorize drafting the proposed Reliability Standard or revisions to a Reliability Standard.
- Reject the SAR with a written explanation to the sponsor and post that explanation.

4.3: Form Drafting Team

When the Standards Committee is ready to have a drafting team begin work on developing a new or revised Reliability Standard, the Standards Committee shall appoint a drafting team, if one was not already appointed to develop the SAR. If the Standards Committee appointed a drafting team to refine the SAR, the same drafting team shall work to develop the associated Reliability Standard.

If no drafting team is in place, then the Standards Committee may use a public nomination process to populate the Reliability Standard drafting team, or may use another method that results in a team that collectively has the necessary technical expertise, diversity of views and work process skills to accomplish the objectives of the project on a timely basis. In some situations, an ad hoc team may already be in place with the requisite expertise, competencies, and diversity of views that are necessary to develop the Reliability Standard, and additional members may not be needed.

The NERC Reliability Standards Staff shall provide one or more members as needed to support the team with facilitation, project management, compliance, legal, regulatory and technical writing expertise and shall provide administrative support to the team, guiding the team through the steps in completing its project. In developing the Reliability Standard, the individuals provided by the NERC Reliability Standards Staff serve as advisors to the drafting team and do not have voting rights but share accountability along with the drafting team members assigned by the Standards Committee for timely delivery of a final draft Reliability Standard that meets the quality attributes identified in NERC's Benchmarks for Excellent Standards. The drafting team members assigned by the Standards Committee shall have final authority over the technical details of the Reliability Standard, while the technical writer shall provide assistance to the drafting team in assuring that the final draft of the Reliability Standard meets the quality attributes identified in NERC's Benchmarks for Excellent Standards.

Once it is appointed by the Standards Committee, the Reliability Standard drafting team is responsible for making recommendations to the Standards Committee regarding the remaining steps in the Reliability Standards process. Consistent with the need to provide for timely standards development, the Standards Committee may decide a project is so large that it should be subdivided and either assigned to more than one drafting team or assigned to a single drafting team with clear direction on completing the project in specified phases. The normally expected timeframes for standards development within the context of this manual are applicable to individual standards and not to projects containing multiple standards. Alternatively, a single drafting team may address the entire project with a commensurate increase in the expected duration of the development work. If a SAR is subdivided and assigned to more than one drafting team, each drafting team will have a clearly defined portion of the work such that there are no overlaps and no gaps in the work to be accomplished.

The Standards Committee may supplement the membership of a Reliability Standard drafting team or provide for additional advisors, as appropriate, to ensure the necessary competencies and diversity of views are maintained throughout the Reliability Standard development effort.

4.4: Develop Preliminary Draft of Reliability Standard, Implementation Plan and VRFs and VSLs

4.4.1: Project Schedule

When a drafting team begins its work, either in refining a SAR or in developing or revising a proposed Reliability Standard, the drafting team shall develop a project schedule which shall be approved by the Standards Committee. The drafting team shall report progress to the Standards Committee, against the initial project schedule and any revised schedule as requested by the Standards Committee. Where project milestones cannot be completed on a timely basis, modifications to the project schedule must be presented to the Standards Committee for consideration along with proposed steps to minimize unplanned project delays.

4.4.2: Draft Reliability Standard

The team shall develop a Reliability Standard that is within the scope of the associated SAR that includes all required elements as described earlier in this manual with a goal of meeting the quality attributes identified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval. The team shall document its justification for the Requirements in its proposed Reliability Standard by explaining how each meets these criteria. The standard drafting team shall document its justification for selecting each reference by explaining how each Requirement fits the category chosen.

4.4.3: Implementation Plan

As a drafting team drafts its proposed revisions to a Reliability Standard, that team is also required to develop an implementation plan to identify any factors for consideration when approving the proposed effective date or dates for the associated Reliability Standard or Standards. As a minimum, the implementation plan shall include the following:

- The proposed effective date (the date entities shall be compliant) for the Requirements.
- Identification of any new or modified definitions that are proposed for approval with the associated Reliability Standard.
- Whether there are any prerequisite actions that need to be accomplished before entities are held responsible for compliance with one or more of the Requirements.
- Whether approval of the proposed Reliability Standard will necessitate any conforming changes to any already approved Reliability Standards – and identification of those Reliability Standards and Requirements.
- The Functional Entities that will be required to comply with one or more Requirements in the proposed Reliability Standard.

A single implementation plan may be used for more than one Reliability Standard. The implementation plan is posted with the associated Reliability Standard or Standards during the 45 (calendar) day formal comment period and is balloted with the associated Reliability Standard.

4.4.4: Violation Risk Factors and Violation Severity Levels

The drafting team shall work with NERC Staff in developing a set of VRFs and VSLs that meet the latest criteria established by NERC and Applicable Governmental Authorities. The drafting team shall document its justification for selecting each VRF and for setting each set of proposed VSLs by explaining how its proposed VRFs and VSLs meet these criteria. NERC Staff is responsible for ensuring that the VRFs and VSLs proposed for stakeholder review meet these criteria.

Before the drafting team has finalized its Reliability Standard, implementation plan, and VRFs and VSLs, the team should seek stakeholder feedback on its preliminary draft documents.

4.5: Informal Feedback[17]

Drafting teams may use a variety of methods to collect informal stakeholder feedback on preliminary drafts of its documents, including the use of informal comment periods,[18] webinars, industry meetings, workshops, or other mechanisms. Information gathered from informal comment forms shall be publicly posted. While drafting teams are not required to provide a written response to each individual comment received, drafting teams are encouraged, where possible, to post a summary response that identifies how it used comments submitted by stakeholders. Drafting teams are encouraged, where possible, to reach out directly to individual stakeholders in order to facilitate resolution of identified stakeholder concerns. The intent is to gather stakeholder feedback on a "working document" before the document reaches the point where it is considered the "final draft."

4.6: Conduct Quality Review

The NERC Reliability Standards Staff shall coordinate a quality review of the Reliability Standard, implementation plan, and VRFs and VSLs in parallel with the development of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated SAR, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval of Reliability Standards. The drafting team shall consider the results of the quality review, decide upon appropriate changes, and recommend to the Standards Committee whether the documents are ready for formal posting and balloting.

The Standards Committee shall authorize posting the proposed Reliability Standard, and implementation plan for a formal comment period and ballot and the VRFs and VSLs for a non-binding poll as soon as the work flow will accommodate.

If the Standards Committee finds that any of the documents do not meet the specified criteria, the Standards Committee shall remand the documents to the drafting team for additional work.

If the Reliability Standard is outside the scope of the associated SAR, the drafting team shall be directed to either revise the Reliability Standard so that it is within the approved scope, or submit a request to expand the scope of the approved SAR. If the Reliability Standard is not clear and enforceable as written, or if the Reliability Standard does not meet the specified criteria, the Reliability Standard shall be returned to the drafting team by the Standards Committee with specific identification of any Requirement that is deemed to be unclear or unenforceable as written.

4.7: Conduct Formal Comment Period and Ballot

Proposed new or modified Reliability Standards require a formal comment period where the new or modified Reliability Standard, implementation plan and associated VRFs and VSLs or the proposal to retire a Reliability Standard, implementation plan and associated VRFs and VSLs are posted.

The formal comment period shall be at least 45-days long. Formation of the ballot pool and Ballot of the Reliability Standard take place during this formal 45-day comment period. The intent of the formal

[17] While this discussion focuses on collecting stakeholder feedback on proposed Reliability Standards and implementation plans, the same process is used to collect stakeholder feedback on proposed new or modified Interpretations, definitions and Variances.

[18] The term "informal comment period" refers to a comment period conducted outside of the ballot process and where there is no requirement for a drafting team to respond in writing to submitted comments.

comment period(s) is to solicit very specific feedback on the final draft of the Reliability Standard, implementation plan and VRFs and VSLs.

Comments in written form may be submitted on a draft Reliability Standard by any interested stakeholder, including NERC Staff, FERC Staff, and other interested governmental authorities. If stakeholders disagree with some aspect of the proposed set of products, comments provided should explain the reasons for such disagreement and, where possible, suggest specific language that would make the product acceptable to the stakeholder.

4.8: Form Ballot Pool

The NERC Reliability Standards Staff shall establish a ballot pool during the first 30 calendar days of the 45-day formal comment period. The NERC Reliability Standards Staff shall post the proposed Reliability Standard, along with its implementation plan, VRFs and VSLs and shall send a notice to every entity in the Registered Ballot Body to provide notice that there is a new or revised Reliability Standard proposed for approval and to solicit participants for the associated ballot pool. All members of the Registered Ballot Body are eligible to join each ballot pool to vote on a new or revised Reliability Standard and its implementation plan and to participate in the non-binding poll of the associated VRFs and VSLs.

Any member of the Registered Ballot Body may join or withdraw from the ballot pool until the ballot window opens. No Registered Ballot Body member may join or withdraw from the ballot pool once the first ballot starts through the point in time where balloting for that Reliability Standard action has ended. The Director of Standards may authorize deviations from this rule for extraordinary circumstances such as the death, retirement, or disability of a ballot pool member that would prevent an entity that had a member in the ballot pool from eligibility to cast a vote during the ballot window. Any approved deviation shall be documented and noted to the Standards Committee.

4.9: Conduct Ballot and Non-binding Poll of VRFs and VSLs[19]

The NERC Reliability Standards Staff shall announce the opening of the Ballot window and the non-binding poll of VRFs and VSLs. The Ballot window and non-binding poll of VRFs and VSLs shall take place during the last 10 calendar days of the 45-day formal comment period and for the Final Ballot shall be no less than 10 calendar days. If the last day of the ballot window falls on a Saturday or Sunday, the period does not end until the next business day.[20]

The ballot and non-binding poll shall be conducted electronically. The voting window shall be for a period of 10 calendar days but shall be extended, if needed, until a quorum is achieved. During a ballot window, NERC shall not sponsor or facilitate public discussion of the Reliability Standard action under ballot.

There is no requirement to conduct a new non-binding poll of the revised VRFs and VSLs if no changes were made to the associated standard, however if the requirements are modified and conforming changes are made to the associated VRFs and VSLs, another non-binding poll of the revised VRFs and VSLs shall be conducted.

[19] While RSAWs are not part of the Reliability Standard, they are developed through collaboration of the SDT and NERC Compliance Staff. A non-binding poll, similar to what is done for VRFs and VSLs may be conducted for the RSAW developed through this process to gauge industry support for the companion RSAW to be provided for informational purposes to the NERC Board of Trustees.

[20] Closing dates may be extended as deemed appropriate by NERC Staff.

4.10: Criteria for Ballot Pool Approval

Ballot pool approval of a Reliability Standard requires:

A quorum, which is established by at least 75% of the members of the ballot pool submitting a response; and

A two-thirds majority of the weighted Segment votes cast shall be affirmative. The number of votes cast is the sum of affirmative votes and negative votes with comments. This calculation of votes for the purpose of determining consensus excludes (i) abstentions, (ii) non-responses, and (iii) negative votes without comments.

The following process[21] is used to determine if there are sufficient affirmative votes.

- For each Segment with ten or more voters, the following process shall be used: The number of affirmative votes cast shall be divided by the sum of affirmative and negative votes with comments cast to determine the fractional affirmative vote for that Segment. Abstentions, non-responses, and negative votes without comments shall not be counted for the purposes of determining the fractional affirmative vote for a Segment.
- For each Segment with less than ten voters, the vote weight of that Segment shall be proportionally reduced. Each voter within that Segment voting affirmative or negative with comments shall receive a weight of 10% of the Segment vote.
- The sum of the fractional affirmative votes from all Segments divided by the number of Segments voting[22] shall be used to determine if a two-thirds majority has been achieved. (A Segment shall be considered as "voting" if any member of the Segment in the ballot pool casts either an affirmative vote or a negative vote with comments.)
- A Reliability Standard shall be approved if the sum of fractional affirmative votes from all Segments divided by the number of voting Segments is at least two thirds.

4.11: Voting Positions

Each member of the ballot pool may **only** vote one of the following positions on the Ballot and Additional Ballot(s):

- Affirmative;
- Affirmative, with comment;
- Negative with comments;
- Abstain.

Given that there is no formal comment period concurrent with the Final Ballot, each member of the ballot pool may **only** vote one of the following positions on the Final Ballot:

- Affirmative;
- Negative;[23]
- Abstain.

[21] Examples of weighted segment voting calculation are posted on the Reliability Standards Resources web page.

[22] When less than ten entities vote in a Segment, the total weight for that Segment shall be determined as one tenth per entity voting, up to ten.

[23] The Final Ballot is used to confirm consensus achieved during the Formal Comment and Ballot stage. Ballot Pool members voting negative on the Final Ballot will be deemed to have expressed the reason for their negative ballot in their own comments or the comments of others during prior Formal Comment periods.

4.12: Consideration of Comments
If a stakeholder or balloter proposes a significant revision to a Reliability Standard during the formal comment period or concurrent Ballot that will improve the quality, clarity, or enforceability of that Reliability Standard, then the drafting team may choose to make such revisions and post the revised Reliability Standard for another 45 calendar day public comment period and ballot. Prior to posting the revised Reliability Standard for an additional comment period, the drafting team must communicate this decision to stakeholders. This communication is intended to inform stakeholders that the drafting team has identified that significant revisions to the Reliability Standard are necessary and should note that the drafting team is not required to respond in writing to comments from the previous ballot. The drafting team will respond to comments received in the last Additional Ballot prior to conducting a Final Ballot.

There is no formal comment period concurrent with the Final Ballot and no obligation for the drafting team to respond to any comments submitted during the Final Ballot.

4.13: Additional Ballots
A drafting team must respond in writing to every stakeholder written comment submitted in response to a ballot prior to conducting a Final Ballot. These responses may be provided in summary form, but all comments and objections must be responded to by the drafting team. All comments received and all responses shall be publicly posted.

However, a drafting team is not required to respond in writing to comments to the previous ballot when it determines that significant changes are needed and an Additional Ballot will be conducted.

4.14: **Conduct Final Ballot**
When the drafting team has reached a point where it has made a good faith effort at resolving applicable objections and is not making any substantive changes from the previous ballot, the team shall conduct a "Final Ballot." A non-substantive revision is a revision that does not change the scope, applicability, or intent of any Requirement and includes but is not limited to things such as correcting the numbering of a Requirement, correcting the spelling of a word, adding an obviously missing word, or rephrasing a Requirement for improved clarity. Where there is a question as to whether a proposed modification is "substantive," the Standards Committee shall make the final determination.

In the Final Ballot, members of the ballot pool shall again be presented the proposed Reliability Standard along with the reasons for negative votes from the previous ballot, the responses of the drafting team to those concerns, and any resolution of the differences.

All members of the ballot pool shall be permitted to reconsider and change their vote from the prior ballot. Members of the ballot pool who did not respond to the prior ballot shall be permitted to vote in the Final Ballot. In the Final Ballot, votes shall be counted by exception only — members on the Final Ballot may indicate a revision to their original vote; otherwise their vote shall remain the same as in their prior ballot.

4.15: Final Ballot Results
There are no limits to the number of public comment periods and ballots that can be conducted to result in a Reliability Standard or interpretation that is clear and enforceable, and achieves a quorum and sufficient affirmative votes for approval. The Standards Committee has the authority to conclude this process for a particular Reliability Standards action if it becomes obvious that the drafting team cannot develop a Reliability Standard that is within the scope of the associated SAR, is sufficiently clear to be enforceable, and achieves the requisite weighted Segment approval percentage.

The NERC Reliability Standards Staff shall post the final outcome of the ballot process. If the Reliability Standard is rejected, the Standards Committee may decide whether to end all further work on the

proposed standard, return the project to informal development, or continue holding ballots to attempt to reach consensus on the proposed standard. If the Reliability Standard is approved, the Reliability Standard shall be posted and presented to the Board of Trustees by NERC management for adoption and subsequently filed with Applicable Governmental Authorities for approval.

4.16: Board of Trustees Adoption of Reliability Standards, Implementation Plan and VRFs and VSLs

If a Reliability Standard and its associated implementation plan are approved by its ballot pool, the Board of Trustees shall consider adoption of that Reliability Standard and its associated implementation plan and shall direct the standard to be filed with Applicable Governmental Authorities for approval. In making its decision, the Board shall consider the results of the balloting and unresolved dissenting opinions. The Board shall adopt or reject a Reliability Standard and its implementation plan, but shall not modify a proposed Reliability Standard. If the Board chooses not to adopt a Reliability Standard, it shall provide its reasons for not doing so.

The board shall consider approval of the VRFs and VSLs associated with a reliability standard. In making its determination, the board shall consider the following:

- The Standards Committee shall present the results of the non-binding poll conducted and a summary of industry comments received on the final posting of the proposed VRFs and VSLs.
- NERC Staff shall present a set of recommended VRFs and VSLs that considers the views of the standard drafting team, stakeholder comments received on the draft VRFs and VSLs during the posting for comment process, the non-binding poll results, appropriate governmental agency rules and directives, and VRF and VSL assignments for other Reliability Standards to ensure consistency and relevance across the entire spectrum of Reliability Standards.

4.17: Compliance

For a Reliability Standard to be enforceable, it shall be approved by its ballot pool, adopted by the NERC Board of Trustees, and approved by Applicable Governmental Authorities, unless otherwise approved by the NERC Board of Trustees pursuant to the NERC Rules of Procedure (*e.g*, Section 321) and approved by Applicable Governmental Authorities. Once a Reliability Standard is approved or otherwise made mandatory by Applicable Governmental Authorities, all persons and organizations subject to jurisdiction of the ERO will be required to comply with the Reliability Standard in accordance with applicable statutes, regulations, and agreements.

4.18: Withdrawal of a Reliability Standard, Interpretation, or Definition

The term "withdrawal" as used herein, refers to the discontinuation of a Reliability Standard, Interpretation, Variance or definition that has been approved by the Board of Trustees and (1) has not been filed with Applicable Governmental Authorities, or (2) has been filed with, but not yet approved by, Applicable Governmental Authorities. The Standards Committee may withdraw a Reliability Standard, Interpretation or definition for good cause upon approval by the Board of Trustees. Upon approval by the Board of Trustees, NERC Staff will petition the Applicable Governmental Authorities, as needed, to allow for withdrawal. The Board of Trustees also has an independent right of withdrawal that is unaffected by the terms and conditions of this Section.

4.19: Retirement of a Reliability Standard, Interpretation, or Definition

The term "retirement" refers to the discontinuation of a Reliability Standard, Interpretation or definition that has been approved by Applicable Governmental Authorities. A Reliability Standard, Variance or Definition may be retired when it is superseded by a revised version, and in such cases the retirement of

the earlier version is to be noted in the implementation plan presented to the ballot pool for approval and the retirement shall be considered approved by the ballot pool upon ballot pool approval of the revised version.

Upon identification of a need to retire a Reliability Standard, Variance, Interpretation or definition, where the item will not be superseded by a new or revised version, a SAR containing the proposal to retire a Reliability Standard, Variance, Interpretation or definition will be posted for a comment period and ballot in the same manner as a Reliability Standard. The proposal shall include the rationale for the retirement and a statement regarding the impact of retirement on the reliability of the Bulk Power System. Upon approval by the Board of Trustees, NERC Staff will petition the Applicable Governmental Authorities to allow for retirement.

Section 5.0: Process for Developing a Defined Term

NERC maintains a glossary of approved terms, entitled the *Glossary of Terms Used in NERC Reliability Standards*[24] ("Glossary of Terms"). The Glossary of Terms includes terms that have been through the formal approval process and are used in one or more NERC Reliability Standards. Definitions shall not contain statements of performance Requirements. The Glossary of Terms is intended to provide consistency throughout the Reliability Standards.

There are several methods that can be used to add, modify or retire a defined term used in a continent-wide Reliability Standard.

- Anyone can use a Standard Authorization Request ("SAR") to submit a request to add, modify, or retire a defined term.
- Anyone can submit a Standards Comments and Suggestions Form recommending the addition, modification, or retirement of a defined term. (The suggestion would be added to a project and incorporated into a SAR.)
- A drafting team may propose to add, modify, or retire a defined term in conjunction with the work it is already performing.

5.1: Proposals to Develop a New or Revised Definition

The following considerations should be made when considering proposals for new or revised definitions:

- Some NERC Regional Entities have defined terms that have been approved for use in Regional Reliability Standards, and where the drafting team agrees with a term already defined by a Regional Entity, the same definition should be adopted if needed to support a NERC Reliability Standard.
- If a term is used in a Reliability Standard according to its common meaning (as found in a collegiate dictionary), the term shall not be proposed for addition to the Glossary of Terms.
- If a term has already been defined, any proposal to modify or delete that term shall consider all uses of the definition in approved Reliability Standards, with a goal of determining whether the proposed modification is acceptable, and whether the proposed modification would change the scope or intent of any approved Reliability Standards.
- When practical, where NAESB has a definition for a term, the drafting team shall use the same definition to support a NERC Reliability Standard.

Any definition that is balloted separately from a proposed new or modified Reliability Standard or from a proposal for retirement of a Reliability Standard shall be accompanied by an implementation plan.

If a SAR is submitted to the NERC Reliability Standards Staff with a proposal for a new or revised definition, the Standards Committee shall consider the urgency of developing the new or revised definition and may direct NERC Staff to post the SAR immediately, or may defer posting the SAR until a later time based on its priority relative to other projects already underway or already approved for future development. If the SAR identifies a term that is used in a Reliability Standard already under revision by a drafting team, the Standards Committee may direct the drafting team to add the term to the scope of the existing project. Each time the Standards Committee accepts a SAR for a project that was not identified in the *Reliability Standards Development Plan*, the project shall be added to the list of approved projects.

[24] The latest approved version of the Glossary of Terms is posted on the NERC website on the Standards web page.

5.2: Stakeholder Comments and Approvals

Any proposal for a new or revised definition shall be processed in the same manner as a Reliability Standard and quality review shall be conducted in parallel with this process. Once authorized by the Standards Committee, the proposed definition and its implementation plan shall be posted for at least one formal stakeholder comment period and shall be balloted in the same manner as a Reliability Standard. If a new or revised definition is proposed by a drafting team, that definition may be balloted separately from the associated Reliability Standard.

Each definition that is approved by its ballot pool shall be submitted to the NERC Board of Trustees for adoption and then filed with Applicable Governmental Authorities for approval in the same manner as a Reliability Standard.

Section 6.0: Processes for Conducting Field Tests and Collecting and Analyzing Data

While most drafting teams can develop their Reliability Standards without the need to conduct any field tests and without the need to collect and analyze data, some Reliability Standard development efforts may require field tests to analyze data and validate concepts in the development of Reliability Standards.

There are two types of field tests – tests of concepts and tests of requirements.

6.1: Field Tests and Data Analysis for Validation of Concepts

Field tests or collection and analysis of data to validate concepts that support the development of Requirements should be conducted before the SAR for a project is finalized. If an entity wants to test a technical concept in support of a proposal for a new or revised Reliability Standard, the entity should either work with one of NERC's technical committees in collecting and analyzing the data or in conducting the field test, or the entity should submit a SAR with a request to collect and analyze data or conduct a field test to validate the concept prior to developing a new or revised Reliability Standard. The request to collect and analyze data or conduct a field test should include, at a minimum, either the data collection and analysis or field test plan, the implementation schedule, and an expectation for periodic updates of the analysis of the results. If the SAR sponsor has not collected and analyzed the data or conducted the field test, the Standards Committee may solicit support from NERC's technical committees or others in the industry. The results of the data collection and analysis or field test shall then be used to determine whether to add the SAR to the list of projects in the Reliability Standard Development Plan.

If a drafting team finds that it needs to collect and analyze data or conduct a field test of a concept that was not identified when the SAR was accepted, then the Standards Committee may direct the team to withdraw the SAR until the data has been collected and analyzed or until the field test has been conducted and the industry has had an opportunity to review the results for the impact on the scope of the proposed project.

6.2: Field Tests and Data Analysis for Validation of Requirements

If a drafting team wants to conduct a field test or collect and analyze data to validate its proposed Requirements in a Reliability Standard, the team shall first obtain approval from the Standards Committee.[25] Drafting teams are not required to collect and analyze data or to conduct a field test to validate a Reliability Standard.

The request should include at a minimum the data collection and analysis or field test plan, the implementation schedule, and an expectation for periodic updates of the results. When authorizing a drafting team to collect and analyze data or to conduct a field test of one or more Requirements, the Standards Committee may request inputs on technical matters related from NERC's technical committees or industry experts, and may request the assistance of the Compliance Monitoring and Enforcement Program. All data collection and analysis and all field tests shall be concluded and the results incorporated into the Reliability Standard Requirements as necessary before proceeding to the formal comment period and subsequent balloting.

[25] The Process for Approving Data Collection and Analysis and Field Tests Associated with a Reliability Standard is posted on the Reliability Standards Resources web page.

6.3: Communication and Coordination for All Types of Field Tests and Data Analyses

If the conduct of a field test (concepts or Requirements) or data collection and analysis could render Registered Entities incapable of complying with the current Requirements of an approved Reliability Standard that is undergoing revision, the drafting team shall request a temporary waiver from compliance to those Requirements for entities participating in the field test. Upon request, the Standards Committee shall seek approval for the waiver from the Compliance Monitoring and Enforcement Program prior to the approval of the field test or data collection and analysis.

Once a plan for a field test or a plan for data collection and analysis is approved, the NERC Reliability Standards Staff shall, under the direction of the Standards Committee, coordinate the implementation of the field test or data collection and analysis and shall provide official notice to the participants in the field test or data collection of any applicable temporary waiver to compliance with specific noted Requirements. The drafting team conducting the field test shall provide periodic updates on the progress of the field tests or data collection and analysis to the Standards Committee. The Standards Committee has the right to curtail a field test or data collection and analysis that is not implemented in accordance with the approved plan.

The field test plan or data collection and analysis plan, its approval, its participants, and all reports and results shall be publicly posted for stakeholder review on the Reliability Standards web page.

If a drafting team conducts or participates in a field test or in data collection and analysis (of concepts or Requirements), it shall provide a final report that identifies the results and how those results will be used.

Section 7.0: Process for Developing an Interpretation

A valid Interpretation request is one that requests additional clarity about one or more Requirements in approved NERC Reliability Standards, but does not request approval as to how to comply with one or more Requirements. A valid Interpretation response provides additional clarity about one or more Requirements, but does not expand on any Requirement and does not explain how to comply with any Requirement. Any entity that is directly and materially affected by the reliability of the North American Bulk Power Systems may request an Interpretation of any Requirement in any continent-wide Reliability Standard that has been adopted by the NERC Board of Trustees. Interpretations will only be provided for Board of Trustees-approved Reliability Standards *i.e.* (i) the current effective version of a Reliability Standard; or (ii) a version of a Reliability Standard with a future effective date.

An Interpretation may only clarify or interpret the Requirements of an approved Reliability Standard, including, if applicable, any attachment referenced in the Requirement being clarified. No other elements of an approved Reliability Standard are subject to Interpretation.

The entity requesting the Interpretation shall submit a *Request for Interpretation* form[26] to the NERC Reliability Standards Staff explaining the clarification required, the specific circumstances surrounding the request, and the impact of not having the Interpretation provided. The NERC Reliability Standards and Legal Staffs shall review the request for interpretation to determine whether it meets the requirements for a valid interpretation. Based on this review, the NERC Standards and Legal Staffs shall make a recommendation to the Standards Committee whether to accept the request for Interpretation and move forward in responding to the Interpretation request.

For example, an Interpretation request may be rejected where it:

(1) Requests approval of a particular compliance approach;
(2) Identifies a gap or perceived weakness in the approved Reliability Standard;
(3) Where an issue can be addressed by an active standard drafting team;
(4) Where it requests clarification of any element of a Reliability Standard other than a Requirement;
(5) Where a question has already been addressed in the record;
(6) Where the Interpretation identifies an issue and proposes the development of a new or modified Reliability Standard, (such issues should be addressed via submission of a SAR);
(7) Where an Interpretation seeks to expand the scope of a Reliability Standard; or
(8) Where the meaning of a Reliability Standard is plain on its face.

If the Standards Committee rejects the Interpretation request, it shall provide a written explanation for rejecting the Interpretation to the entity requesting the Interpretation within 10 business days of the decision to reject. If the Standards Committee accepts the Interpretation request, the NERC Standards Staff shall (i) form a ballot pool and (ii) assemble an Interpretation drafting team with the relevant expertise to address the interpretation for approval by the Standards Committee. As soon as practical, the team shall develop a "final draft" Interpretation providing the requested clarity.

Interpretations will be balloted in the same manner as Reliability Standards.

[26] The *Request for Interpretation* form is posted on the NERC Standards web page.

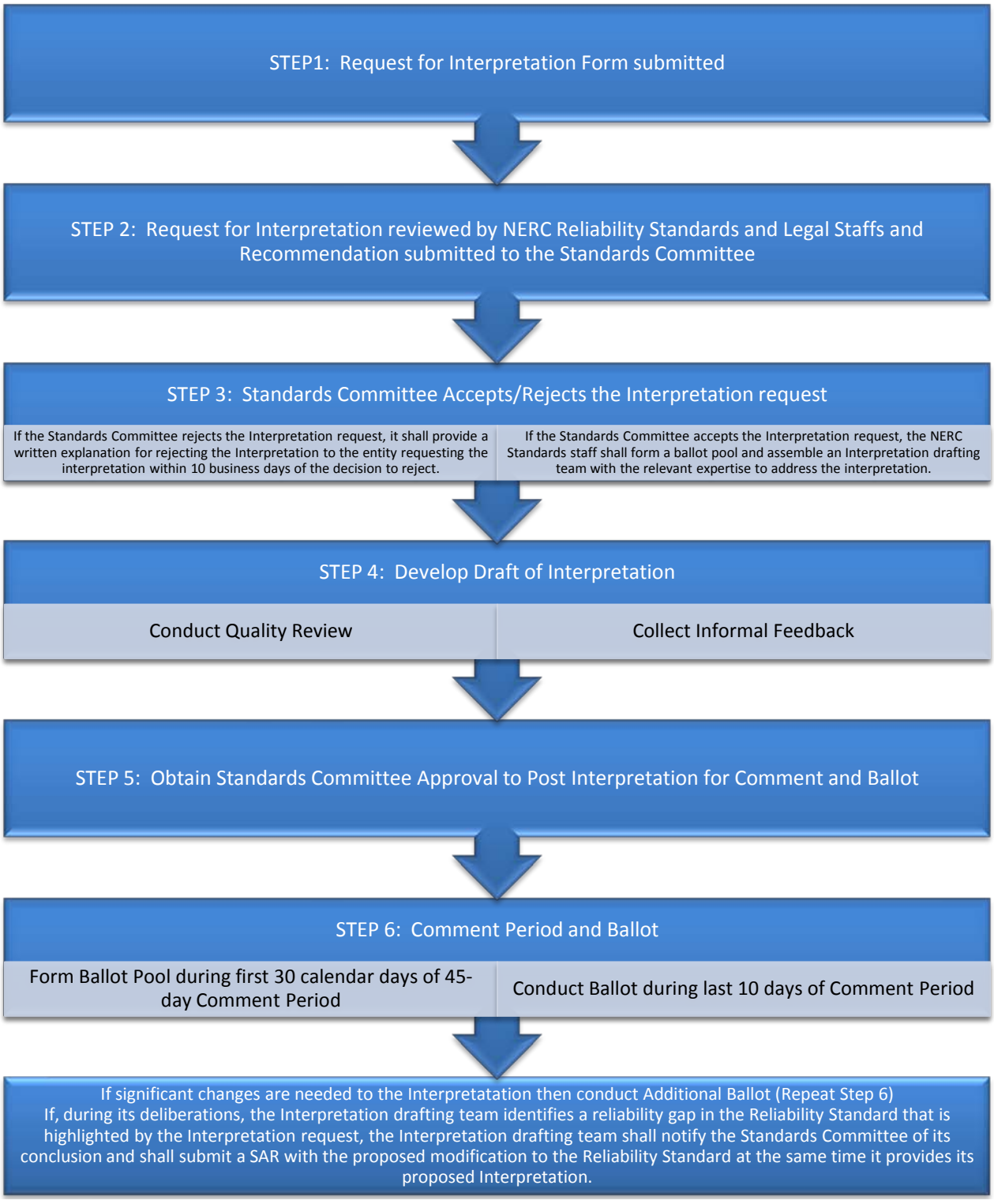
If stakeholder comments indicate that there is not a consensus for the Interpretation, and the Interpretation drafting team cannot revise the Interpretation without violating the basic expectations outlined above, the Interpretation drafting team shall notify the Standards Committee of its conclusion and may submit a SAR with the proposed modification to the Reliability Standard. The entity that requested the Interpretation shall be notified and the disposition of the Interpretation shall be posted.

If, during its deliberations, the Interpretation drafting team identifies a reliability gap in the Reliability Standard that is highlighted by the Interpretation request, the Interpretation drafting team shall notify the Standards Committee of its conclusion and may submit a SAR with the proposed modification to the Reliability Standard at the same time it provides its proposed Interpretation.

The NERC Reliability Standards and Legal Staffs shall review the final Interpretation to determine whether it has met the requirements for a valid Interpretation. Based on this review, the NERC Standards and Legal Staffs shall make a recommendation to the NERC Board of Trustees regarding adoption.

If approved by its ballot pool, the Interpretation shall be forwarded to the NERC Board of Trustees for adoption.[27] If an Interpretation drafting team proposes a modification to a Reliability Standard as part of its work in developing an Interpretation, the Board of Trustees shall be notified of this proposal at the time the Interpretation is submitted for adoption. Following adoption by the Board of Trustees, NERC Staff shall file the Interpretation for approval by Applicable Governmental Authorities and the Interpretation shall become effective when approved by those Applicable Governmental Authorities. The Interpretation shall stand until such time as the Interpretation can be incorporated into a future revision of the Reliability Standard or the Interpretation is retired due to a future modification of the applicable Requirement.

[27] NERC will maintain a record of all interpretations associated with each standard on the Reliability Standards page of the NERC website.


STEP1: Request for Interpretation Form submitted
STEP 2: Request for Interpretation reviewed by NERC Reliability Standards and Legal Staffs and Recommendation submitted to the Standards Committee
STEP 3: Standards Committee Accepts/Rejects the Interpretation request
If the Standards Committee rejects the Interpretation request, it shall provide a written explanation for rejecting the Interpretation to the entity requesting the interpretation within 10 business days of the decision to reject.
If the Standards Committee accepts the Interpretation request, the NERC Standards staff shall form a ballot pool and assemble an Interpretation drafting team with the relevant expertise to address the interpretation.
STEP 4: Develop Draft of Interpretation
Conduct Quality Review
Collect Informal Feedback
STEP 5: Obtain Standards Committee Approval to Post Interpretation for Comment and Ballot
STEP 6: Comment Period and Ballot
Form Ballot Pool during first 30 calendar days of 45-day Comment Period
Conduct Ballot during last 10 days of Comment Period
If significant changes are needed to the Interpretatation then conduct Additional Ballot (Repeat Step 6)
If, during its deliberations, the Interpretation drafting team identifies a reliability gap in the Reliability Standard that is highlighted by the Interpretation request, the Interpretation drafting team shall notify the Standards Committee of its conclusion and shall submit a SAR with the proposed modification to the Reliability Standard at the same time it provides its proposed Interpretation.

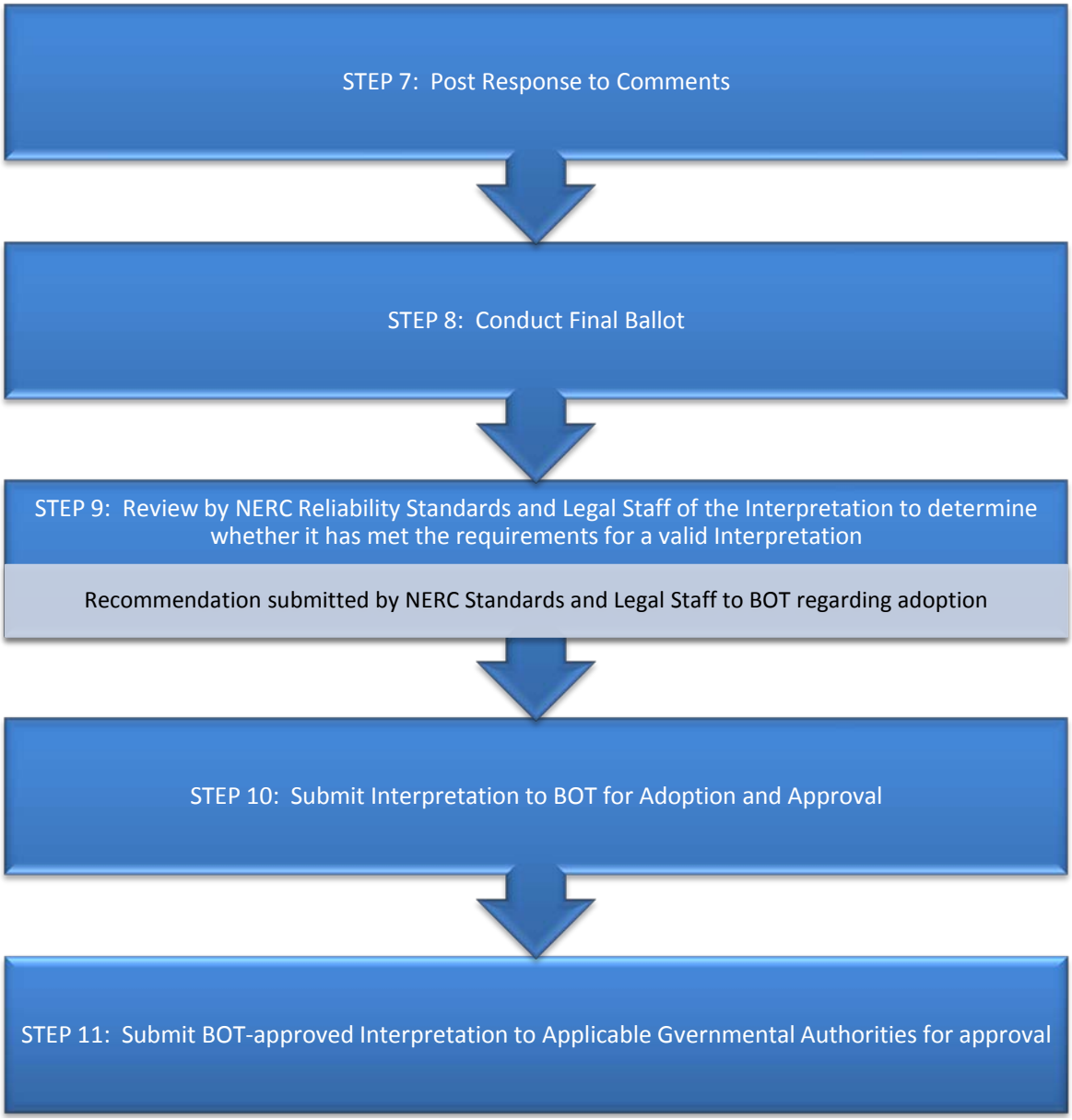


FIGURE 2: Process for Developing an Interpretation

Section 8.0: Process for Appealing an Action or Inaction

Any entity that has directly and materially affected interests and that has been or will be adversely affected by any procedural action or inaction related to the development, approval, revision, reaffirmation, retirement or withdrawal of a Reliability Standard, definition, Variance, associated implementation plan, or Interpretation shall have the right to appeal. This appeals process applies only to the NERC Reliability Standards processes as defined in this manual, not to the technical content of the Reliability Standards action.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made in writing within 30 days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants.

8.1: Level 1 Appeal

Level 1 is the required first step in the appeals process. The appellant shall submit (to the Director of Standards) a complaint in writing that describes the procedural action or inaction associated with the Reliability Standards process. The appellant shall describe in the complaint the actual or potential adverse impact to the appellant. Assisted by NERC Staff and industry resources as needed, the Director of Standards shall prepare a written response addressed to the appellant as soon as practical but not more than 45 days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response shall be made a part of the public record associated with the Reliability Standard.

8.2: Level 2 Appeal

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the Director of Standards, the Director of Standards shall convene a Level 2 Appeals Panel. This panel shall consist of five members appointed by the Board of Trustees. In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The NERC Reliability Standards Staff shall post the complaint and other relevant materials and provide at least 30 days notice of the meeting of the Level 2 Appeals Panel. In addition to the appellant, any entity that is directly and materially affected by the procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may, in its decision, find for the appellant and remand the issue to the Standards Committee with a statement of the issues and facts in regard to which fair and equitable action was not taken. The panel may find against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise, approve, disapprove, or adopt a Reliability Standard, definition, Variance or Interpretation or implementation plan as these responsibilities remain with the ballot pool and Board of Trustees respectively. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the Board of Trustees for consideration at the time the Board decides whether to adopt a particular Reliability Standard, definition, Variance or Interpretation. The objection shall be in writing, signed by an officer of

the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection shall be filed no later than 30 days after the announcement of the vote by the ballot pool on the Reliability Standard in question.

Section 9.0: Process for Developing a Variance

A Variance is an approved, alternative method of achieving the reliability intent of one or more Requirements in a Reliability Standard. 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 Reliability 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.

NERC's drafting teams shall aim to develop Reliability Standards with Requirements that apply on a continent-wide basis, minimizing the need for Variances while still achieving the Reliability Standard's reliability objectives. If one or more Requirements cannot be met or complied with as written because of a physical difference in the Bulk Power System or because of an operational difference (such as a conflict with a federally or provincially approved tariff), but the Requirement's reliability objective can be achieved in a different fashion, an entity or a group of entities may pursue a Variance from one or more Requirements in a continent-wide Reliability Standard. It is the responsibility of the entity that needs a Variance to identify that need and initiate the processing of that Variance through the submittal of a SAR[28] that includes a clear definition of the basis for the Variance.

There are two types of Variances – those that apply on an Interconnection-wide basis, and those that apply to one or more entities on less than an Interconnection-wide basis.

9.1: Interconnection-wide Variances

Any Variance from a NERC Reliability Standard Requirement that is proposed to apply to Registered Entities within a Regional Entity organized on an Interconnection-wide basis shall be considered an Interconnection-wide Variance and shall be developed through that Regional Entity's NERC-approved Regional Reliability Standards development procedure.

While an Interconnection-wide Variance may be developed through the associated Regional Reliability Standards development process, Regional Entities are encouraged to work collaboratively with existing continent-wide drafting teams to reduce potential conflicts between the two efforts.

An Interconnection-wide Variance from a NERC 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 other applicable standards of governmental authorities shall be made part of the associated NERC Reliability Standard. NERC shall rebuttably presume that an Interconnection-wide Variance from a NERC Reliability Standard that is developed, in accordance with a Regional Reliability Standards development procedure 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.

9.2: Variances that Apply on Less than an Interconnection-wide Basis

Any Variance from a NERC Reliability Standard Requirement that is proposed to apply to one or more entities but less than an entire Interconnection (*e.g.*, 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), shall be considered a Variance. A Variance may be requested while a Reliability Standard is under development or a Variance may be requested at any time after a Reliability Standard is approved. Each request for a Variance shall be initiated through a SAR, and processed and approved in the same

[28] A sample of a SAR that identifies the need for a Variance and a sample Variance are posted as resources on the Reliability Standards Resources web page.

manner as a continent-wide Reliability Standard, using the Reliability Standards development process defined in this manual.

Section 10.0: Processes for Developing a Reliability Standard Related to a Confidential Issue

While it is NERC's intent to use its ANSI-accredited Reliability Standards development process for developing its Reliability Standards, NERC has an obligation as the ERO to ensure that there are Reliability Standards in place to preserve the reliability of the interconnected Bulk Power Systems throughout North America. When faced with a national security emergency situation, NERC may use one of the following special processes to develop a Reliability Standard that addresses an issue that is confidential. Reliability Standards developed using one of the following processes shall be called, "special Reliability Standards" and shall not be filed with ANSI for approval as American National Standards.

The NERC Board of Trustees may direct the development of a new or revised Reliability Standard to address a national security situation that involves confidential issues. These situations may involve imminent or long-term threats. In general, these Board directives will be driven by information from the President of the United States of America or the Prime Minister of Canada or a national security agency or national intelligence agency of either or both governments indicating (to the ERO) that there is a national security threat to the reliability of the Bulk Power System.[29]

There are two special processes for developing Reliability Standards responsive to confidential issues – one process where the confidential issue is "imminent," and one process where the confidential issue is "not imminent."

10.1: Process for Developing Reliability Standards Responsive to Imminent, Confidential Issues
If the NERC Board of Trustees directs the immediate development of a new or revised Reliability Standard to address a confidential national security emergency situation, the NERC Reliability Standards Staff shall develop a SAR, form a ballot pool (to vote on the Reliability Standard and its implementation plan) and assemble a slate of pre-defined subject matter experts as a proposed drafting team for approval by the Standards Committee's officers. All members of the Registered Ballot Body shall have the opportunity to join the ballot pool.

10.2: Drafting Team Selection
The Reliability Standard drafting team selection process shall be limited to just those candidates who have already been identified as having the appropriate security clearance, the requisite technical expertise, and either have signed or are willing to sign a strict confidentiality agreement.

10.3: Work of Drafting Team
The Reliability Standard drafting team shall perform all its work under strict security and confidential rules. The Reliability Standard drafting team shall develop the new or revised Reliability Standard and its implementation plan.

The Reliability Standard drafting team shall review its work, to the extent practical, as it is being developed with officials from the appropriate governmental agencies in the U.S. and Canada, under strict security and confidentiality rules.

[29] The NERC Board may direct the immediate development and issuance of a Level 3 (Essential Action) alert and then may also direct the immediate development of a new or revised Reliability Standard.

10.4: Formal Stakeholder Comment & Ballot Window
The draft Reliability Standard and its implementation plan shall be distributed for a formal comment period, under strict confidentiality rules, only to those entities that are listed in the NERC Compliance Registry to perform one of the functions identified in the applicability section of the Reliability Standard and have identified individuals from their organizations that have signed confidentiality agreements with NERC.[30] At the same time, the Reliability Standard shall be distributed to the members of the ballot pool for review and ballot. The NERC Reliability Standards Staff shall not post or provide the ballot pool with any confidential background information.

The drafting team, working with the NERC Reliability Standards Staff, shall consider and respond to all comments, make any necessary conforming changes to the Reliability Standard and its implementation plan, and shall distribute the comments, responses and any revision to the same population as received the initial set of documents for formal comment and ballot.

10.5: Board of Trustee Actions
Each Reliability Standard and implementation plan developed through this process shall be submitted to the NERC Board of Trustees for adoption.

10.6: Governmental Approvals
All approved documents shall be filed for approval with Applicable Governmental Authorities.

[30] In this phase of the process, only the proposed Reliability Standard shall be distributed to those entities expected to comply, not the rationale and justification for the Reliability Standard. Only the special drafting team members, who have the appropriate security credentials, shall have access to this rationale and justification.

10.7: Developing a Reliability Standard Responsive to an Imminent, Confidential Issue

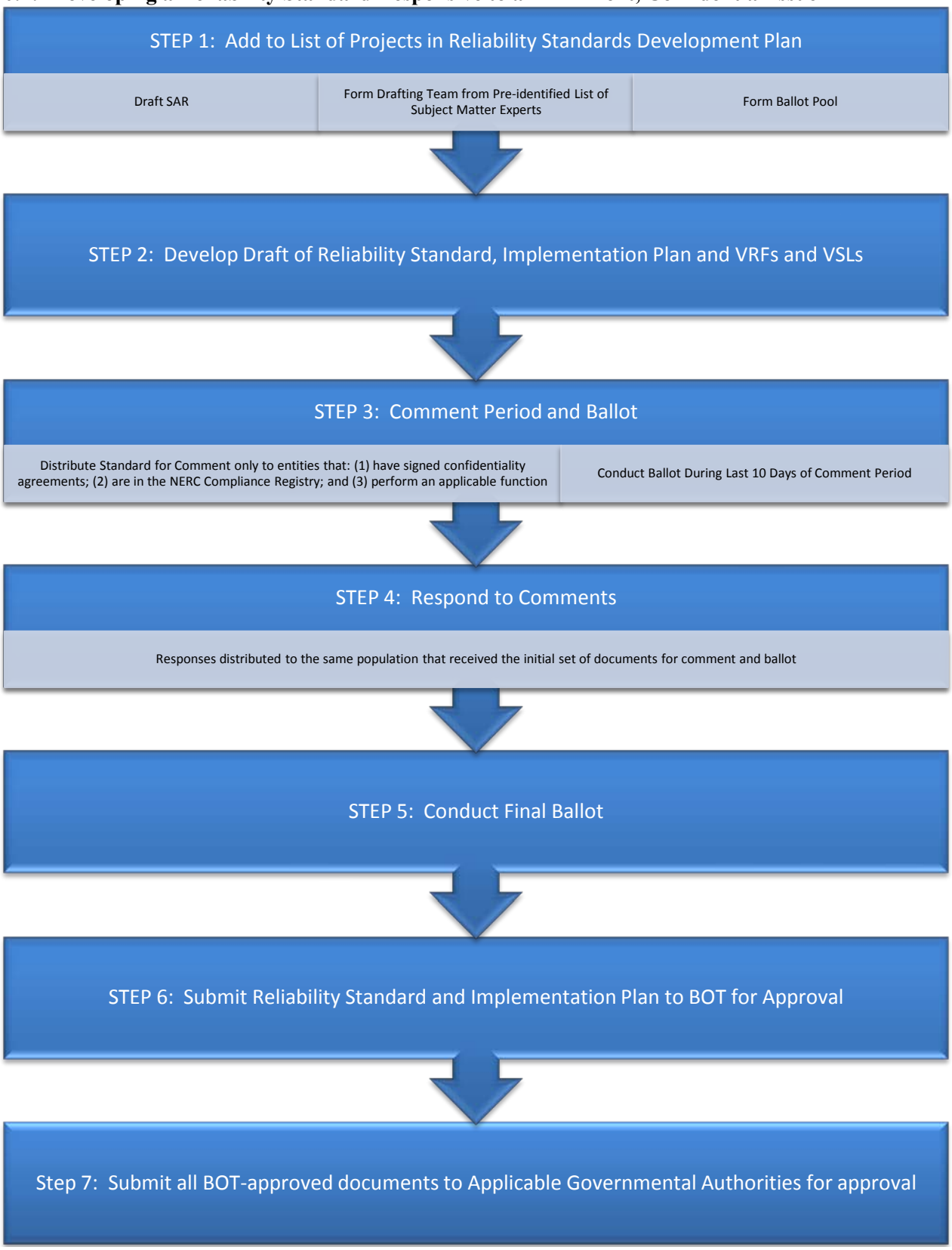


FIGURE 3: Process for Developing a Standard Responsive to an Imminent, Confidential Issue

10.8: Process for Developing Reliability Standards Responsive to Non-imminent, Confidential Issues

If the NERC Board of Trustees directs the immediate development of a new or revised Reliability Standard to address a confidential national security emergency situation, the NERC Reliability Standards Staff shall develop a SAR, form a ballot pool (to vote on the Reliability Standard and its implementation plan) and assemble a slate of pre-defined subject matter experts as a proposed drafting team for approval by the Standards Committee's officers. All members of the Registered Ballot Body shall have the opportunity to join the ballot pool.

10.9: Drafting Team Selection

The drafting team selection process shall be limited to just those candidates who have already been identified as having the appropriate security clearance, the requisite technical expertise, and either have signed or are willing to sign a strict confidentiality agreement.

10.10: Work of Drafting Team

The drafting team shall perform all its work under strict security and confidential rules. The Reliability Standard drafting team shall develop the new or revised Reliability Standard and its implementation plan.

The drafting team shall review its work, to the extent practical, as it is being developed with officials from the Applicable Governmental Authorities, under strict security and confidentiality rules.

10.11: Formal Stakeholder Comment & Ballot Window

The draft Reliability Standard and its implementation plan shall be distributed for a formal comment period, under strict confidentiality rules, only to those entities that are listed in the NERC Compliance Registry to perform one of the functions identified in the applicability section of the Reliability Standard and have identified individuals from their organizations that have signed confidentiality agreements with NERC.[31] At the same time, the Reliability Standard shall be distributed to the members of the ballot pool for review and ballot. The NERC Reliability Standards Staff shall not post or provide the ballot pool with any confidential background information.

10.12: Revisions to Reliability Standard, Implementation Plan and VRFs and VSLs

The drafting team, working with the NERC Reliability Standards Staff, shall work to refine the Reliability Standard, implementation plan and VRFs and VSLs in the same manner as for a new Reliability Standard following the "normal" Reliability Standards development process described earlier in this manual with the exception that distribution of the comments, responses, and new drafts shall be limited to those entities that are in the ballot pool and those entities that are listed in the NERC Compliance Registry to perform one of the functions identified in the applicability section of the Reliability Standard and have identified individuals from their organizations that have signed confidentiality agreements with NERC.

10.13: Board of Trustee Action

Each Reliability Standard, implementation plan, and the associated VRFs and VSLs developed through this process shall be submitted to the NERC Board of Trustees for adoption.

10.14: Governmental Approvals

All BOT-approved documents shall be filed for approval with Applicable Governmental Authorities.

[31] In this phase of the process, only the proposed Reliability Standard shall be distributed to those entities expected to comply, not the rationale and justification for the Reliability Standard. Only the special drafting team members, who have the appropriate security credentials, shall have access to this rationale and justification.

Developing a Reliability Standard Responsive to a Non-imminent, Confidential Issue

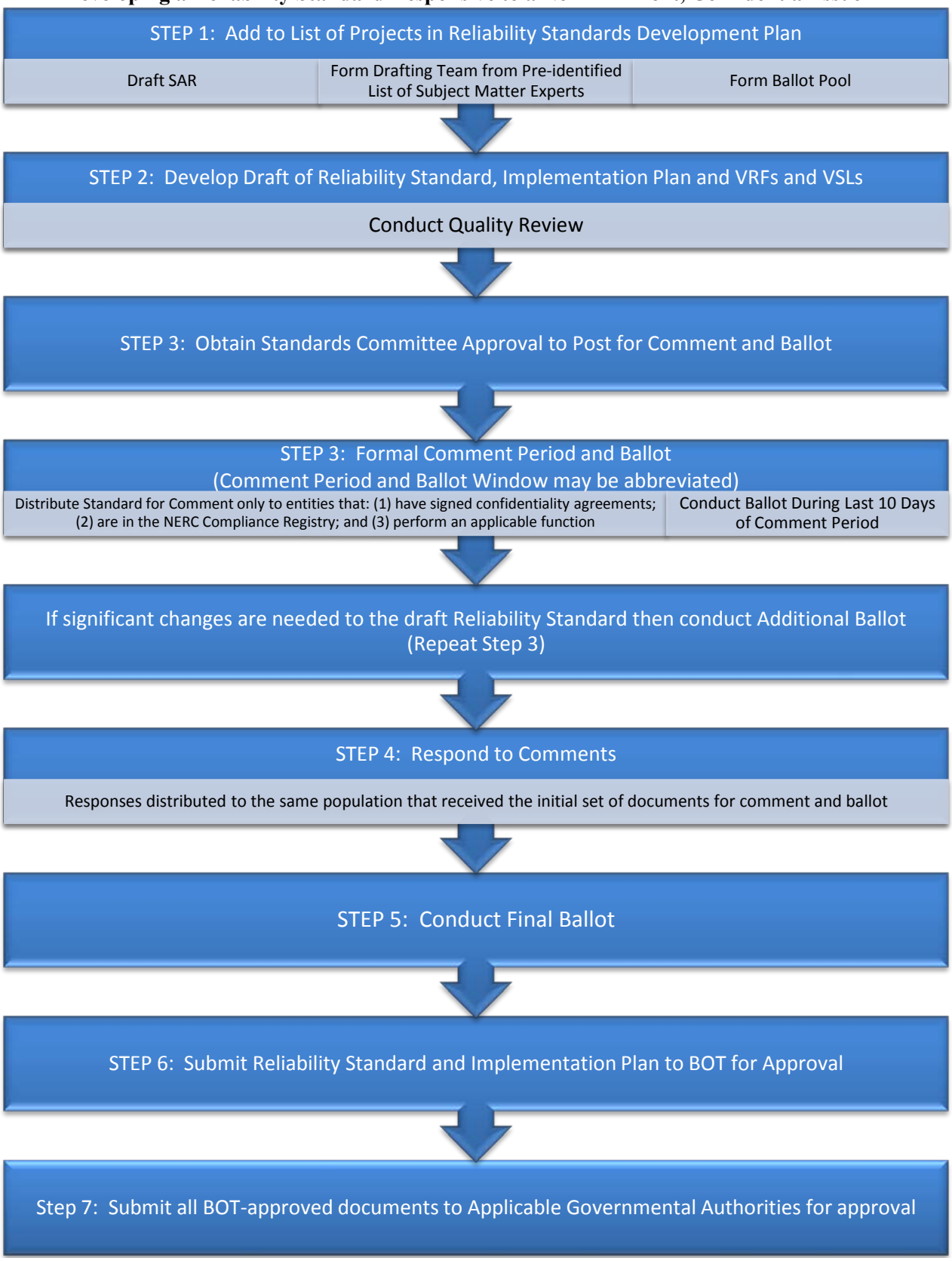


FIGURE 4: Developing a Standard Responsive to a Non-Imminent, Confidential Issue

Section 11.0: Process for Approving Supporting Documents

The following types of documents are samples of the types of supporting documents that may be developed to enhance stakeholder understanding and implementation of a Reliability Standard. These documents may explain or facilitate implementation of Reliability Standards but do not themselves contain mandatory Requirements subject to compliance review. Any Requirements that are mandatory shall be incorporated into the Reliability Standard in the Reliability Standard development process.

While most supporting documents are developed by the standard drafting team working to develop the associated Reliability Standard, any entity may develop a supporting document associated with a Reliability Standard.

The Standards Committee shall authorize the posting of all supporting references[32] that are linked to an approved Reliability Standard. Prior to granting approval to post a supporting reference with a link to the associated Reliability Standard, the Standards Committee shall verify that the document has had stakeholder review to verify the accuracy of the technical content. While the Standards Committee has the authority to approve the posting of each such reference, stakeholders, not the Standards Committee, verify the accuracy of the document's contents.

Type of Document	Description
Reference	Descriptive, technical information or analysis or explanatory information to support the understanding and interpretation of a Reliability Standard. A standard reference may support the implementation of a Reliability Standard or satisfy another purpose consistent with the reliability and market interface principles.
Guideline	Recommended process that identifies a method of meeting a Requirement under specific conditions.
Supplement	Data forms, pro forma documents, and associated instructions that support the implementation of a Reliability Standard.
Training Material	Documents that support the implementation of a Reliability Standard.
Procedure	Step-wise instructions defining a particular process or operation. Procedures may support the implementation of a Reliability Standard or satisfy another purpose consistent with the reliability and market interface principles.
White Paper	An informal paper stating a position or concept. A white paper may be used to propose preliminary concepts for a Reliability Standard or one of the documents above.

[32] The Standards Committee's Procedure for Approving the Posting of Reference Documents is posted on the Reliability Standards Resources web page.

Section 12.0: Process for Correcting Errata

From time to time, an error may be discovered in a Reliability Standard. Such errors may be corrected (i) following a Final Ballot prior to Board of Trustees adoption, (ii) following Board of Trustees adoption prior to filing with Applicable Governmental Authorities; and (iii) following filing with Applicable Governmental Authorities. If the Standards Committee agrees that the correction of the error does not change the scope or intent of the associated Reliability Standard, and agrees that the correction has no material impact on the end users of the Reliability Standard, then the correction shall be filed for approval with Applicable Governmental Authorities as appropriate. The NERC Board of Trustees has resolved to concurrently approve any errata approved by the Standards Committee.

Section 13.0: Process for Conducting Periodic Reviews of Reliability Standards

All Reliability Standards shall be reviewed at least once every ten years from the effective date of the Reliability Standard or the date of the latest Board of Trustees adoption to a revision of the Reliability Standard, whichever is later. If a Reliability Standard is approved by ANSI as an American National Standard, it shall be reviewed at least once every five years from the effective date of the Reliability Standard or the date of the latest Board of Trustees adoption to a revision of the Reliability Standard, whichever is later.

The *Reliability Standards Development Plan* shall include projects that address this five or ten-year review of Reliability Standards.

- If a Reliability Standard is nearing its five or ten-year review and has issues that need resolution, then the *Reliability Standards Development Plan* shall include a project for the complete review and associated revision of that Reliability Standard that includes addressing all outstanding governmental directives, all approved Interpretations, and all unresolved issues identified by stakeholders.
- If a Reliability Standard is nearing its five or ten-year review and there are no outstanding governmental directives, Interpretations, or unresolved stakeholder issues associated with that Reliability Standard, then the Reliability *Standards Development Plan* shall include a project solely for the "five-year review" of that Reliability Standard.

For a project that is focused solely on the five-year review, the Standards Committee shall appoint a review team of subject matter experts to review the Reliability Standard and recommend whether the American National Standard Institute-approved Reliability Standard should be reaffirmed, revised, or withdrawn. Each review team shall post its recommendations for a 45 calendar day formal stakeholder comment period and shall provide those stakeholder comments to the Standards Committee for consideration.

- If a review team recommends reaffirming a Reliability Standard, the Standards Committee shall submit the reaffirmation to the Board of Trustees for adoption and then to Applicable Governmental Authorities for approval. Reaffirmation does not require approval by stakeholder ballot.
- If a review team recommends modifying, or retiring a Reliability Standard, the team shall develop a SAR with such a proposal and the SAR shall be submitted to the Standards Committee for prioritization as a new project. Each existing Reliability Standard recommended for modification, or retirement shall remain in effect in accordance with the associated implementation plan until the action to modify or withdraw the Reliability Standard is approved by its ballot pool, adopted by the Board of Trustees, and approved by Applicable Governmental Authorities.

In the case of reaffirmation of a Reliability Standard, the Reliability Standard shall remain in effect until the next five or ten-year review or until the Reliability Standard is otherwise modified or withdrawn by a separate action.

Section 14.0: Public Access to Reliability Standards Information

14.1: Online Reliability Standards Information System

The NERC Reliability Standards Staff shall maintain an electronic copy of information regarding currently proposed and currently in effect Reliability Standards. This information shall include current Reliability Standards in effect, proposed revisions to Reliability Standards, and proposed new Reliability Standards. This information shall provide a record, for at a minimum the previous five years, of the review and approval process for each Reliability Standard, including public comments received during the development and approval process.

14.2: Archived Reliability Standards Information

The NERC Staff shall maintain a historical record of Reliability Standards information that is no longer maintained online. Archived information shall be retained indefinitely as practical, but in no case less than five years or one complete standard cycle from the date on which the Reliability 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 Reliability Standards Staff of a written request.

Section 15.0: Process for Updating Standard Processes

15.1: Requests to Revise the Standard Processes Manual

Any person or entity may submit a request to modify one or more of the processes contained within this manual. The Standards Committee shall oversee the handling of each request. The Standards Committee shall prioritize all requests, merge related requests, and respond to each sponsor within 30 calendar days.

The Standards Committee shall post the proposed revisions for a 45 (calendar) day formal comment period. Based on the degree of consensus for the revisions, the Standards Committee shall:

a. Submit the revised process or processes for ballot pool approval;
b. Repeat the posting for additional inputs after making changes based on comments received;
c. Remand the proposal to the sponsor for further work; or
d. Reject the proposal.

The Registered Ballot Body shall be represented by a ballot pool. The ballot procedure shall be the same as that defined for approval of a Reliability Standard, including the use of an Additional Ballot if needed. If the proposed revision is approved by the ballot pool, the Standards Committee shall submit the revised procedure to the Board for adoption. The Standards Committee shall submit to the Board a description of the basis for the changes, a summary of the comments received, and any minority views expressed in the comment and ballot process. The proposed revisions shall not be effective until approved by the NERC Board of Trustees and Applicable Governmental Authorities.

Section 16.0: Waiver

While it is NERC's intent to use its ANSI-accredited Reliability Standards development process for developing its Reliability Standards, NERC may need to develop a new or modified Reliability Standard, definition, Variance, or implementation plan under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn't sufficient time to follow all the steps in the normal Reliability Standards development process.

The Standards Committee may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:

- In response to a national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber attack on the Bulk Electric System;
- Where necessary to meet regulatory deadlines;
- Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
- Where the Standards Committee determines that a modification to a proposed Reliability Standard or its Requirement(s), a modification to a defined term, a modification to an interpretation, or a modification to a variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

In no circumstances shall this provision be used to modify the requirements for achieving quorum or the voting requirements for approval of a standard.

A waiver request may be submitted to the Standards Committee by any entity or individual, including NERC committees or subgroups and NERC Staff. Prior to consideration of any waiver request, the Standards Committee must provide five business days notice to stakeholders.

Action on the waiver request will be included in the minutes of the Standards Committee. Following the approval of the Standards Committee to waive any provision of the Standard Process Manual, the Standards Committee will report this decision to the Standards Oversight and Technology Committee.[33] Actions taken pursuant to an approved waiver request will be posted on the Standard Project page and included in the next project announcement.

In addition, the Standards Committee shall report the exercise of this waiver provision to the Board of Trustees prior to adoption of the related Reliability Standard, Interpretation, definition or Variance.

Reliability Standards developed as a result of a waiver of any provision of the Standard Processes Manual shall not be filed with ANSI for approval as American National Standards.

[33] Any entity may appeal a waiver decision or any other procedural decision by the Standards Committee pursuant to Section 8.0 of the NERC Standard Processes Manual.

4.6: Conduct Quality Review

The NERC Reliability Standards Staff shall coordinate a quality review of the Reliability Standard, implementation plan, and VRFs and VSLs in parallel with the development of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated SAR, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval of Reliability Standards. The drafting team shall consider the results of the quality review, decide upon appropriate changes, and recommend to the Standards Committee whether the documents are ready for formal posting and balloting.

The Standards Committee shall authorize posting the proposed Reliability Standard, and implementation plan for a formal comment period and ballot and the VRFs and VSLs for a non-binding poll as soon as the work flow will accommodate.

If the Standards Committee finds that any of the documents do not meet the specified criteria, the Standards Committee shall remand the documents to the drafting team for additional work.

If the Reliability Standard is outside the scope of the associated SAR, the drafting team shall be directed to either revise the Reliability Standard so that it is within the approved scope, or submit a request to expand the scope of the approved SAR. If the Reliability Standard is not clear and enforceable as written, or if the Reliability Standard does not meet the specified criteria, the Reliability Standard shall be returned to the drafting team by the Standards Committee with specific identification of any Requirement that is deemed to be unclear or unenforceable as written.